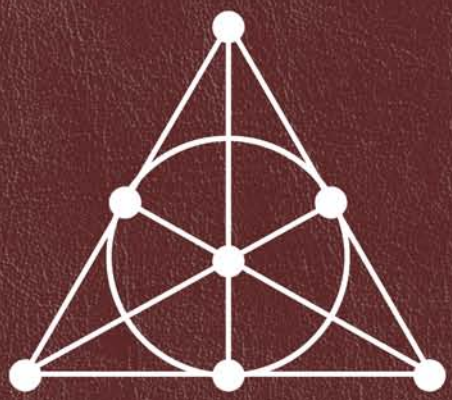
DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

EDITED BY
CHARLES J. COLBOURN
JEFFREY H. DINITZ

HANDBOOK OF



COMBINATORIAL DESIGNS

SECOND EDITION

Chapman & Hall/CRC
Taylor & Francis Group

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

HANDBOOK OF COMBINATORIAL DESIGNS

SECOND EDITION

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor
Kenneth H. Rosen, Ph.D.

Juergen Bierbrauer, Introduction to Coding Theory

Kun-Mao Chao and Bang Ye Wu, Spanning Trees and Optimization Problems

Charalambos A. Charalambides, Enumerative Combinatorics

Henri Cohen, Gerhard Frey, et al., Handbook of Elliptic and Hyperelliptic Curve Cryptography

Charles J. Colbourn and Jeffrey H. Dinitz, Handbook of Combinatorial Designs, Second Edition

Steven Furino, Ying Miao, and Jianxing Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence

Randy Goldberg and Lance Riek, A Practical Handbook of Speech Coders

Jacob E. Goodman and Joseph O'Rourke, Handbook of Discrete and Computational Geometry, Second Edition

Jonathan L. Gross and Jay Yellen, Graph Theory and Its Applications, Second Edition

Jonathan L. Gross and Jay Yellen, Handbook of Graph Theory

Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson, Introduction to Information Theory and Data Compression, Second Edition

Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt, Network Reliability: Experiments with a Symbolic Algebra Environment

Leslie Hogben, Handbook of Linear Algebra

Derek F. Holt with Bettina Eick and Eamonn A. O'Brien, Handbook of Computational Group Theory

David M. Jackson and Terry I. Visentin, An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces

Richard E. Klima, Neil P. Sigmon, and Ernest L. Stitzinger, Applications of Abstract Algebra with Maple™ and MATLAB® , Second Edition

Patrick Knupp and Kambiz Salari, Verification of Computer Codes in Computational Science and Engineering

William Kocay and Donald L. Kreher, Graphs, Algorithms, and Optimization

Donald L. Kreher and Douglas R. Stinson, Combinatorial Algorithms: Generation Enumeration and Search

Continued Titles

Charles C. Lindner and Christopher A. Rodgers, Design Theory

Hang T. Lau, A Java Library of Graph Algorithms and Optimization

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography

Richard A. Mollin, Algebraic Number Theory

Richard A. Mollin, Codes: The Guide to Secrecy from Ancient to Modern Times

Richard A. Mollin, Fundamental Number Theory with Applications

Richard A. Mollin, An Introduction to Cryptography, Second Edition

Richard A. Mollin, Quadratics

Richard A. Mollin, RSA and Public-Key Cryptography

Carlos J. Moreno and Samuel S. Wagstaff, Jr., Sums of Squares of Integers

Dingyi Pei, Authentication Codes and Combinatorial Designs

Kenneth H. Rosen, Handbook of Discrete and Combinatorial Mathematics

Douglas R. Shier and K.T. Wallenius, Applied Mathematical Modeling: A Multidisciplinary Approach

Jörn Steuding, Diophantine Analysis

Douglas R. Stinson, Cryptography: Theory and Practice, Third Edition

Roberto Togneri and Christopher J. deSilva, Fundamentals of Information Theory and Coding Design

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

HANDBOOK OF COMBINATORIAL DESIGNS

SECOND EDITION

EDITED BY
CHARLES J. COLBOURN
JEFFREY H. DINITZ

Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York

Chapman & Hall/CRC is an imprint of the
Taylor & Francis Group, an informa business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 1-58488-506-8 (Hardcover)
International Standard Book Number-13: 978-1-58488-506-1 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Handbook of combinatorial designs / edited by Charles J. Colbourn, Jeffrey H. Dinitz. -- 2nd ed.
p. cm. -- (Discrete mathematics and its applications)
ISBN 1-58488-506-8
1. Combinatorial designs and configurations. I. Colbourn, Charles J. II. Dinitz, Jeffrey H., 1952- III. Title. IV. Series.

QA166.25.H36 2007
511'.6--dc22 2006050484

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Preface

The Purpose of this Book

The *CRC Handbook of Combinatorial Designs (Second Edition)* is a reference book of combinatorial designs, including constructions of designs, existence results, properties of designs, and many applications of designs. The handbook is not a textbook introduction to combinatorial design theory, but rather a comprehensive, easy-to-access reference for facts about designs.

Organization of the Handbook

The presentation is organized into seven main parts, each divided into chapters. The first part contains a brief introduction and history. The next four parts center around four main classes of combinatorial designs: balanced incomplete block designs (II), orthogonal arrays and latin squares (III), pairwise balanced designs (IV), and Hadamard and orthogonal designs (V). Part VI then contains sixty-five shorter chapters (placed in alphabetical order) devoted to other classes of designs—naturally, many of these classes are closely connected with designs in Parts II–V. Part VII gives mathematical and computational background of particular use in design theory.

How to Use this Book

This handbook is not meant to be used in a sequential way, but rather for direct access to information about relevant topics. Each chapter makes references to other chapters for related information; in particular, the See Also listing at the end of each chapter provides useful links.

An extensive index and the table of contents provide first entry points for most material. For readers new to the area, the first chapter, *Opening the Door*, can assist in finding a suitable starting point. This handbook can be used on its own as a reference book or in conjunction with numerous excellent available texts on the subject. Although material at the research frontier is often included, the handbook emphasizes basic, useful information.

Combinatorial design theory has extensive interactions with numerous areas of mathematics: group theory, graph theory, number theory and finite fields, finite geometry, and linear algebra. It also has applications ranging from routine to complex in numerous disciplines: experimental design, coding theory, cryptography, and computer science, among others. The handbook treats all of these, providing information for design theorists to understand the applications, and for users of design theory to obtain pointers in to the rest of the handbook, and hence to the mathematics of combinatorial designs.

Notes for the User

A home page for the CRC Handbook of Combinatorial Designs is being maintained. It is located at `http://www.cems.uvm.edu/~dinitz/hcd.html`. Notes, corrections, and updates will be disseminated at that site.

Fixed numbering conventions are used. This book has seven main parts numbered using roman numerals I–VII. Each part is divided into chapters, which in turn have sections; all are numbered. So, for example, the third section in the fourth chapter of the second part is §II.4.3. This is the manner to which it is referred when referenced from any *other* chapter. When referenced from within Chapter II.4, it is referenced

simply as §4.3. Occasionally, sections contain subsections. However, to avoid four level numbers, such subsections are *not* numbered; rather, the beginning of a subsection is given by the symbol '▷' preceding the title of the subsection. Numbering of Theorems, Definitions, Remarks, Corollaries, Tables, Algorithms, and the like is consecutive within each chapter. So, for example, in §II.4.2, Theorem II.4.8 (displayed with "4.8" exdented) is followed by Definition II.4.9, which is followed by Remark II.4.10. As before, the roman numeral is omitted if both the referenced theorem and the reference to it are in the same chapter. Definitions are displayed in gray boxes.

Forward and reverse citations are given. There is a single bibliography after Part VII. However, each chapter provides a list of the reference numbers for items cited therein. In addition, the last entry of each item in the bibliography (in angle brackets) enumerates the page numbers on which the item is cited. This is often useful to uncover further relationships among the topics treated.

Original references are not, in general, given. Instead, each chapter references surveys and textbooks in which the information is readily accessible. These sources should be consulted for more complete lists of references. One exception is Chapter I.2, *Design Theory: Antiquity to 1950*, which provides original references. Each chapter covers the *basic* material, but sufficient pointers to find more specialized information are typically given.

The state of the subject is continually advancing. Each chapter presents, as far as possible, information that is current at the time of writing. Inevitably, improvements will occur! Readers aware of improvements on, or corrections to, the material presented here are invited to contact the author(s) of the chapter(s) involved and also the editors-in-chief.

Differences Between the Editions

The second edition exhibits a substantial increase in size over the first; the book is over 30% larger, with 235 additional pages! While the basic structure has been retained, a new introductory part has been added to provide a general overview and a historical perspective. Material on Hadamard and related designs has been collected together into a new part (V). On the other hand, the Applications part of the first edition has been incorporated into the remaining parts, in the belief that the effort to distinguish theory from application is no longer appropriate. Finally, the nearly 90 separate bibliographies of the first edition have been amalgamated to form a single bibliography for the *Handbook*, to provide yet another means to find the right "starting point" on a search for desired information. This bibliography contains roughly 2200 references and in itself provides an excellent resource.

Often material that is closely related has been combined into a single chapter; in the process, virtually all of the content of the first edition is preserved, but the reader may find small changes in its location. The material is completely updated, and generally enlarged, in the second. The major tables from the first edition (BIBDs, MOLS, PBDs, Hadamard matrices) have been definitive sources for the current knowledge, and all are updated in the second edition. We do not believe that designs whose heyday seems to have passed deserve less attention than the topics of most active current research. The basics of yesteryear continue to be important. Nevertheless, because the discipline continues to evolve, many new topics have been incorporated. Particular emphasis is on topics that bridge with many areas of application, as well as with other areas of mathematics.

In the second edition, the new chapters are: Opening the Door (I.1), Design Theory: Antiquity to 1950 (I.2), Triple Systems (II.2), Group Divisible Designs (IV.4), Optical Orthogonal Codes (V.9), Bent Functions (VI.4), Block-Transitive Designs (VI.5), Covering Arrays (VI.10), Deletion-Correcting Codes (VI.14), Graph Embed-

dings and Designs (VI.25), Grooming (VI.27), Infinite Designs (VI.30), Low Density Parity Check Codes (VI.33), Magic Squares (VI.34), Nested Designs (VI.36), Perfect Hash Families (VI.43), Permutation Codes and Arrays (VI.44), Permutation Polynomials (VI.45), Pooling Designs (VI.46), Quasi-3 Designs (VI.47), Supersimple Designs (VI.57), Turán Systems (VI.61), Divisible Semiplanes (VII.3), Linear Algebra and Designs (VII.7), Designs and Matroids (VII.10), and Directed Strongly Regular Graphs (VII.12). We are pleased to have been able to add much new material to the *Handbook*.

A Note of Appreciation

We must begin by acknowledging the excellent work done by the 110 contributors. Each kindly agreed to write a chapter on a specific topic, their job made difficult by the style and length restrictions placed upon them. Many had written hundreds of pages on their topic, yet were asked to summarize in a few pages. They also were asked to do this within the fairly rigid stylistic framework that is relatively consistent throughout the book. The editors were merciless in their attempt to uphold this style, and offer a special thanks to the copyeditor, Carole Gustafson, for assistance. Many chapters were edited extensively. We thank the contributors for their cooperation.

Many chapters have profited from comments from a wide variety of readers, in addition to the contributors and editors. A compilation of this size can only be accomplished with the help of a small army of people. The concept developed and realized in the first edition from 1996 was the cumulative effort of approximately one hundred people. Many have extensively updated their earlier chapters, and some generously agreed to contribute new material. Many chapters in the second edition employ a conceptual design and/or material first written by others. We thank again authors from both editions for worrying less about whose name is on the byline for the material than the fact that it is a good reflection on our discipline. The concept of the Handbook owes much to those who compiled extensive tables prior to the first edition, such as the BIBD tables of Rudi Mathon and Alex Rosa, and the MOLS table of Andries Brouwer. For the first edition, Ron Mullin coordinated a substantial effort to make the first tables of PBDs, and Don Kreher generated extensive tables of t-designs; in the process, both developed new and useful ways to present these tables, updated in the second edition. We thank Ron and Don again for their great contributions.

As in the first edition, we again thank Debbie Street and Vladimir Tonchev for their extensive help in organizing the material in statistical designs and coding theory, respectively. For the second edition, we especially thank Hadi Kharaghani for organizing (and writing much of) the material in Part V. Special thanks too to Leo Storme for the complete rewrite and reorganization of the chapter on finite geometry. For going above and beyond with their help on the second edition, we also thank Julian Abel, Dan Archdeacon, Frank Bennett, Ian Blake, Warwick de Launey, Peter Dukes, Gennian Ge, Malcolm Greig, Jonathan Jedwab, Teresa Jin, Esther Lamken, Bill Martin, Gary McGuire, Patric Östergård, David Pike, Donald Preece, Alex Rosa, Joe Rushanan, Doug Stinson, Anne Street, Tran van Trung, Ian Wanless, and Zhu Lie. Thanks also to the excellent logistical support from the publisher, particularly to Nora Konopka and Wayne Yuhasz for the first edition, and to Helena Redshaw, Judith Simon, and Bob Stern for the second.

Finally, we thank Sue Dinitz and Violet Syrotiuk for their love and support. Putting together this extensive volume has taken countless hours; we thank them for their patience during it all.

Charles J. Colbourn
Jeffrey H. Dinitz

To Violet, Sarah, and Susie, with love.

CJC

To my father, Simon Dinitz, who has inspired me in all that I have done. Happy 80th birthday!

JHD

Editors-in-Chief

Charles J. Colbourn
Computer Science and Engineering
Arizona State University
U.S.A.

Jeffrey H. Dinitz
Mathematics and Statistics
University of Vermont
U.S.A

Contributors

R. Julian R. Abel
University of New South Wales
Australia

Lars D. Andersen
University of Aalborg
Denmark

Ian Anderson
University of Glasgow
U.K.

Lynn Margaret Batten
Deakin University
Australia

Lucien Bénéteau
INSA
France

Frank E. Bennett
Mount Saint Vincent University
Canada

Jean-Claude Bermond
INRIA Sophia-Antipolis
France

Anton Betten
Colorado State University
U.S.A.

Jürgen Bierbrauer
Michigan Technological University
U.S.A.

Ian F. Blake
University of Toronto
Canada

Andries E. Brouwer
Technical University of Eindhoven
Netherlands

Darryn Bryant
University of Queensland
Australia

Marco Buratti
Università di Perugia
Italy

Peter J. Cameron
University of London
U.K.

Yeow Meng Chee
Card View Pte Ltd.
Singapore

Leo G. Chouinard II
University of Nebraska
U.S.A.

Wensong Chu
Arizona State University
U.S.A.

Charles J. Colbourn
Arizona State University
U.S.A.

David Coudert
INRIA Sophia-Antipolis
France

Robert Craigen
University of Manitoba
Canada

Anne Delandtsheer
Université Libre de Bruxelles
Belgium

Warwick de Launey
Center for Communications Research
U.S.A.

Michel M. Deza
École Normale Supérieure
France

Jeffrey H. Dinitz
University of Vermont
U.S.A.

Peter J. Dukes
University of Victoria
Canada

Saad El-Zanati
Illinois State University
U.S.A.

Anthony B. Evans
Wright State University
U.S.A.

Norman J. Finizio
University of Rhode Island
U.S.A.

Dalibor Froncek
University of Minnesota Duluth
U.S.A.

Gennian Ge
Zhejiang University
P.R. China

Peter B. Gibbons
University of Auckland
New Zealand

Chistopher D. Godsil
University of Waterloo
Canada

Solomon W. Golomb
University of Southern California
U.S.A.

K. Gopalakrishnan
East Carolina University
U.S.A.

Daniel M. Gordon
Center for Communications Research
U.S.A.

Ken Gray
The University of Queensland
Australia

Malcolm Greig
Greig Consulting
Canada

Terry S. Griggs
The Open University
U.K.

Hans-Dietrich O. F. Gronau
Universität Rostock
Germany

Harald Gropp
Universität Heidelberg
Germany

A. S. Hedayat
University of Illinois at Chicago
U.S.A.

Tor Helleseth
University of Bergen
Norway

Sylvia A. Hobart
University of Wyoming
U.S.A.

Spencer P. Hurd
The Citadel
U.S.A.

Frank K. Hwang
National Chiao Tung University
Taiwan

Yury J. Ionin
Central Michigan University
U.S.A.

Robert Jajcay
Indiana State University
U.S.A.

Dieter Jungnickel
Universität Augsburg
Germany

Hadi Kharaghani
University of Lethbridge
Canada

Gholamreza B. Khosrovshahi
IPM
Iran

Christos Koukouvinos
National Technical University of Athens
Greece

Earl S. Kramer
University of Nebraska–Lincoln
U.S.A.

Donald L. Kreher
Michigan Technological University
U.S.A.

Joseph M. Kudrle
University of Vermont
U.S.A.

Esther R. Lamken
San Francisco
U.S.A.

Reinhard Laue
Universität Bayreuth
Germany

Charles F. Laywine
Brock University
Canada

Vladimir I. Levenshtein
Keldysh Inst. Applied Mathematics
Russia

P. C. Li
University of Manitoba
Canada

Charles C. Lindner
Auburn University
U.S.A.

Spyros S. Magliveras
Florida Atlantic University
U.S.A.

Alireza Mahmoodi
York University
Canada

William J. Martin
Worcester Polytechnic Institute
U.S.A.

Rudolf Mathon
University of Toronto
Canada

Gary McGuire
National University of Ireland
Ireland

Sarah B. Menard
University of Vermont
U.S.A.

Eric Mendelsohn
University of Toronto
Canada

Ying Miao
University of Tsukuba
Japan

J. P. Morgan
Virginia Tech
U.S.A.

Gary L. Mullen
The Pennsylvania State University
U.S.A.

Ronald C. Mullin
Florida Atlantic University
U.S.A.

Akihiro Munemasa
Tohoku University
Japan

William Orrick
Indiana University
U.S.A.

Patric R. J. Östergård
Helsinki University of Technology
Finland

Stanley E. Payne
University of Colorado at Denver
U.S.A.

Alexander Pott
Universität Magdeberg
Germany

Donald A. Preece
University of London
U.K.

Chris Rodger
Auburn University
U.S.A.

Alexander Rosa
McMaster University
Canada

Gordon F. Royle
University of Western Australia
Australia

Miklós Ruszinkó
Hungarian Academy of Sciences
Hungary

Dinesh G. Sarvate
College of Charleston
U.S.A.

Nabil Shalaby
Memorial University of Newfoundland
Canada

James B. Shearer
IBM
U.S.A.

Mohan S. Shrikhande
Central Michigan University
U.S.A.

Jozef Širáň
University of Auckland
New Zealand

Ken W. Smith
Central Michigan University
U.S.A.

Hong-Yeop Song
Yonsei University
Korea

Sung Y. Song
Iowa State University
U. S. A.

Edward Spence
University of Glasgow
U.K.

Douglas R. Stinson
University of Waterloo
Canada

Leo Storme
Ghent University
Belgium

Anne Penfold Street
The University of Queensland
Australia

Deborah J. Street
University of Technology, Sydney
Australia

Herbert Taylor
University of Southern California
U.S.A.

Joseph A. Thas
Ghent University
Belgium

Vladimir D. Tonchev
Michigan Technological University
U.S.A.

David C. Torney
Los Alamos National Laboratory
U.S.A.

G. H. John van Rees
University of Manitoba
Canada

Tran van Trung
University of Duisburg–Essen
Germany

Robert A. Walker II
Arizona State University
U.S.A.

Walter D. Wallis
Southern Illinois University
U.S.A.

Ian M. Wanless
Monash University
Australia

Bridget S. Webb
The Open University
U.K.

Ruizhong Wei
Lakehead University
Canada

Hugh Williams
University of Calgary
Canada

Richard M. Wilson
California Institute of Technology
U.S.A.

Jianxing Yin
Suzhou University
China

L. Zhu
Suzhou University
China

Contents

VI Other Combinatorial Designs

VII Related Mathematics

Part I

Introduction

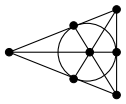
It seems to me that whatever else is beautiful apart from absolute beauty is beautiful because it partakes of that absolute beauty, and for no other reason. Do you accept this kind of causality? Yes, I do.

Well, now, that is as far as my mind goes; I cannot understand these other ingenious theories of causation. If someone tells me that the reason why a given object is beautiful is that it has a gorgeous color or shape or any other such attribute, I disregard all these other explanations—I find them all confusing—and I cling simply and straightforwardly and no doubt foolishly to the explanation that the one thing that makes the object beautiful is the presence in it or association with it, in whatever way the relation comes about, of absolute beauty. I do not go so far as to insist upon the precise details—only upon the fact that it is by beauty that beautiful things are beautiful. This, I feel, is the safest answer for me or anyone else to give, and I believe that while I hold fast to this I cannot fall; it is safe for me or for anyone else to answer that it is by beauty that beautiful things are beautiful. Don't you agree? (Plato, *Phaedo*, 100c-e)

1 Opening the Door

Charles J. Colbourn

1.1 Example The Fano plane.

Seven points		Seven lines
Three points on a line		Three lines through a point
Every two points define a line		Every two lines meet at a point

1.2 Remarks Opening the door into the world of combinatorial designs, and stepping through that door, is familiar to some and mysterious to many. What lies on the other side? And where is the map to guide us?

There is territory both charted and uncharted; the guide map is at best known only in part. Meandering through this world without fixed direction can be both enjoyable and instructive; yet most have a goal, a question whose answer is sought. This introduction explores, with the simplest examples, the landmarks of the world of combinatorial designs. While not prescribing a path, it provides some direction.

Perhaps the most vexing problem is to recognize the object sought when it is encountered; the disguises are often ingenious, but the many faces of one simple object often reveal its importance. Example 1.1 is recast in many different ways, to acquaint the reader with correspondences that are useful in recognizing an object when its representation changes. This exercise provides a first view of the large body of material in the rest of the handbook, to which pointers are provided for the reader to follow.

1.1 Balance

▷ **Sets and Blocks**

1.3 Example The Fano plane as a set system.

{0,1,2}, {0,3,4}, {0,5,6}, {1,3,5}, {1,4,6}, {2,3,6}, {2,4,5}	Using elements $\{0, 1, 2, 3, 4, 5, 6\}$, label the points in Example 1.1. For each line, form a set that contains the elements corresponding to the points on that line. The result is a collection of sets, a *set system*.

1.4 **Remark** The set system of Example 1.3 exhibits in many ways a desideratum that is central to the understanding of combinatorial designs, the desire for *balance*. Some of the ways are considered here.

- *All sets have the same size $k = 3$.* The set system is *k-uniform*.
- *All elements occur in precisely $r = 3$ of the sets.* The set system is *r-regular* or *equireplicate with replication r*.
- *Every pair of distinct elements occurs as a subset of exactly $\lambda = 1$ of the sets.* The set system is 2-*balanced* with *index* $\lambda = 1$.
- *Every pair of distinct sets intersects in exactly $\mu = 1$ elements.* Equivalently, the symmetric difference of every two distinct sets contains exactly four elements; the set system is 4-*equidistant*.

Balance is a key to understanding combinatorial designs, not just a serendipitous feature of one small example.

1.5 Consider a general finite set system. It has a (finite) ground set V of size v whose members are *elements* (or *points* or *varieties*), equipped with a (finite) collection $\mathcal{B}$ of b subsets of V whose members are *blocks* (or *lines* or *treatments*). Then

- $K = \{|B| : B \in \mathcal{B}\}$ is the set of *block sizes*;
- $R = \{|\{B : x \in B \in \mathcal{B}\}| : x \in V\}$ is the set of *replication numbers*,
- for $t \geq 0$ integer, $\Lambda_t = \{|\{B : T \subseteq B \in \mathcal{B}\}| : T \subseteq V, |T| = t\}$ is the set of *t-indices*. Indeed, $\Lambda_0 = \{b\}$, and $\Lambda_1 = R$.
- $M = \{|B \cap B'| : B, B' \in \mathcal{B}, B \neq B'\}$, the set of *intersection numbers*.

1.6 **Remark** Restricting any or all of K, R, M, or the $\{\Lambda_t\}$s imposes structure on the set system; restrictions to a single element balance that structure in some regard. Table 1.7 considers the effect of restricting one or more of these sets to be singletons, providing pointers into the remainder of the handbook. Indeed, set systems so defined are among the most central objects in all of design theory and are studied extensively. The language with which they are discussed in this chapter varies from set systems to hypergraphs, matrices, geometries of points and lines, graph decompositions, codes, and the like; the balance of the underlying set system permeates all.

1.7 **Table** Some of the set systems that result when at least one of the balance sets K, R, M, or the $\{\Lambda_t\}$ is a singleton.

K	R	Λ_2	Λ_t	M	Other	Name	Section
$\{k\}$	$\{r\}$	$\{\lambda_2\}$	$\{\lambda_t\}$			t-design	II.4
$\{k\}$	$\{r\}$	$\{\lambda_2\}$	$\{\lambda_t\}$		$\lambda_t = 1$	Steiner system	II.5
$\{k\}$	$\{r\}$	$\{\lambda\}$				balanced incomplete block design (BIBD)	II.1, II.3
$\{k\}$	$\{r\}$	$\{\lambda\}$		$\{\mu\}$	$k = r$	symmetric design (SBIBD)	II.6
$\{k\}$	$\{r\}$	$\{\lambda\}$		$\{\mu\}$	$\lambda = \mu = 1$	projective plane	II.6, VII.2.1
	$\{r\}$	$\{\lambda\}$				(r, λ)-design	VI.49
		$\{\lambda\}$				pairwise balanced design (PBD)	IV.1
		$\{\lambda\}$			$\lambda = 1$	linear space	IV.1, IV.6
			$\{\lambda_t\}$			t-wise balanced design	VI.63

1.8 **Remarks** A natural relaxation is obtained by specifying an upper or a lower bound on values arising in the set, or by specifying a small number of permitted values; the short form $\{\underline{x}\}$ is adopted to permit all values greater than or equal to x, and $\{\overline{x}\}$ to indicate all values less than or equal to x. Then certain generalizations have been well studied; see Table 1.9.

1.9 Table Some set systems that result when K is a singleton and M or $\{\Lambda_t\}$ is bounded.

K	R	Λ_2	Λ_t	M	Other	Name	Section
$\{k\}$			$\{\underline{\lambda_t}\}$			t-covering	VI.11
$\{k\}$				$\{\overline{\mu}\}$		constant weight code	VII.1
$\{k\}$			$\{\overline{\lambda_t}\}$			t-packing	VI.40

▷ **Algebras and Arrays**

1.10 Example A quasigroup and a latin square.

$\otimes$	0	1	2	3	4	5	6
0	0	2	1	4	3	6	5
1	2	1	0	5	6	3	4
2	1	0	2	6	5	4	3
3	4	5	6	3	0	1	2
4	3	6	5	0	4	2	1
5	6	3	4	1	2	5	0
6	5	4	3	2	1	0	6

Use the blocks of Example 1.3 to define the binary operation $\otimes$ at left, as follows. When $\{x, y, z\}$ is a block, define $x \otimes y = z$; then define $x \otimes x = x$.
Delete the headline and sideline, reorder rows and columns, and rename symbols to get the array on the right.

1	7	2	6	5	4	3
4	5	6	3	7	1	2
3	6	5	7	4	2	1
5	4	3	2	1	7	6
2	1	7	5	6	3	4
7	2	1	4	3	6	5
6	3	4	1	2	5	7

1.11 Remarks Example 1.10 introduces another kind of balance. The operation $\otimes$ defined has a simple property: the equation $a \otimes b = c$ always has a unique solution for the third variable given the other two. This is reminiscent of groups, yet the algebra defined has no identity element and hence no notion of inverses. It weakens the properties of finite groups, and is a *quasigroup*. As an $n \times n$ array, it is equivalent to say that every symbol occurs in every row once, and also in every column once; the array is a *latin square*. Part III focuses on latin squares and their generalizations; see particularly §III.1 for latin squares, §III.2 for quasigroups, and §VI.22 for generalizations to balanced squares in which every cell contains a fixed number of elements greater than one.

1.12 Example For the square at left in Example 1.10, form a set $\{x, y+7, z+14\}$ whenever $x \otimes y = z$. The resulting sets are:

$\{0,7,14\}$, $\{0,8,16\}$, $\{0,9,15\}$, $\{0,10,18\}$, $\{0,11,17\}$, $\{0,12,20\}$, $\{0,13,19\}$,
$\{1,7,16\}$, $\{1,8,15\}$, $\{1,9,14\}$, $\{1,10,19\}$, $\{1,11,20\}$, $\{1,12,17\}$, $\{1,13,18\}$,
$\{2,7,15\}$, $\{2,8,14\}$, $\{2,9,16\}$, $\{2,10,20\}$, $\{2,11,19\}$, $\{2,12,18\}$, $\{2,13,17\}$,
$\{3,7,18\}$, $\{3,8,19\}$, $\{3,9,20\}$, $\{3,10,17\}$, $\{3,11,14\}$, $\{3,12,15\}$, $\{3,13,16\}$,
$\{4,7,17\}$, $\{4,8,20\}$, $\{4,9,19\}$, $\{4,10,14\}$, $\{4,11,18\}$, $\{4,12,16\}$, $\{4,13,15\}$,
$\{5,7,20\}$, $\{5,8,17\}$, $\{5,9,18\}$, $\{5,10,15\}$, $\{5,11,16\}$, $\{5,12,19\}$, $\{5,13,14\}$,
$\{6,7,19\}$, $\{6,8,18\}$, $\{6,9,17\}$, $\{6,10,16\}$, $\{6,11,15\}$, $\{6,12,14\}$, $\{6,13,20\}$.

1.13 Remarks Example 1.12 gives a representation of the quasigroup in Example 1.10 once again as blocks. In this set system with 49 blocks on 21 points, every point occurs in 7 blocks, every block has three points; yet some pairs occur once while others occur not at all, in the blocks. Indeed pairs inside the *groups* $\{0,1,2,3,4,5,6\}$, $\{7,8,9,10,11,12,13\}$, and $\{14,15,16,17,18,19,20\}$ are precisely those that do not appear. This is a *group divisible design* (see §IV.1). Balance with respect to occurrence of pairs could be recovered by adjoining the three groups as blocks; the result exhibits pair balance but loses equality of block sizes because blocks of size 3 and 7 are present; this is a *pairwise balanced design* (see §IV.1). Instead, placing a copy of the 7 point design on each of the groups balances both pair occurrences and block sizes, and, indeed, provides a larger balanced incomplete block design, this one on 21 points having 70 ($= 49 + 3 \times 7$) blocks.

Returning to the group divisible design, yet another balance property is found; every block meets every group in exactly one point. This defines a *transversal design*; see §III.3.

1.14 **Example** Two mutually orthogonal latin squares of side 7.

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\odot$	0	1	2	3	4	5	6
0	0	2	4	6	1	3	5
1	1	3	5	0	2	4	6
2	2	4	6	1	3	5	0
3	3	5	0	2	4	6	1
4	4	6	1	3	5	0	2
5	5	0	2	4	6	1	3
6	6	1	3	5	0	2	4

$+,\odot$	0	1	2	3	4	5	6
0	0,0	1,2	2,4	3,6	4,1	5,3	6,5
1	1,1	2,3	3,5	4,0	5,2	6,4	0,6
2	2,2	3,4	4,6	5,1	6,3	0,5	1,0
3	3,3	4,5	5,0	6,2	0,4	1,6	2,1
4	4,4	5,6	6,1	0,3	1,5	2,0	3,2
5	5,5	6,0	0,2	1,4	2,6	3,1	4,3
6	6,6	0,1	1,3	2,5	3,0	4,2	5,4

1.15 **Remark** The operation $\otimes$ in Example 1.10 is by no means the only way to define a quasigroup on 7 symbols. In Example 1.14, two more are shown, with operations $+$ and $\odot$. A natural question is whether they are different from each other in an essential manner, or different from $\otimes$. The definition of $+$ has the same columns as that of $\odot$, but in a different order. While different as algebras, they are nonetheless quite similar. They are introduced here to note yet another kind of balance. When superimposing two $n \times n$ latin squares, one could expect every ordered pair of symbols to arise any number of times between 0 and n; but the average number of times is precisely one. This example demonstrates that perfect balance can be achieved: every pair arises exactly once in the superposition. As latin squares, these are *mutually orthogonal*. Section III.3 explores these, in their various disguises as quasigroups, as squares, and as transversal designs.

1.16 **Example** For the square at left in Example 1.10, form an array whose columns are precisely the triples $(x, y, z)^T$ for which $x \otimes y = z$.

$$\begin{array}{l} 00000001111111222222233333334444444555555566666666 \\ 01234560123456012345601234560123456012345601234560123456 \\ 02143652105634102654345630123650421634125054321 06 \end{array}$$

1.17 **Remark** Example 1.16 gives yet another view of the same structure. In the 3×49 array, each of the 7 symbols occurs 7 times in each row. However, much more is true. Choosing *any* two rows, there are $49 = 7 \cdot 7$ pairs of entries possible, and 49 occurring. As one might expect, the case of interest is that of balance, when every pair occurs the same number of times (here, once). This is an *orthogonal array*; see §III.6 and §III.7. While playing a prominent role in combinatorial design theory, they play a larger role yet in experimental design in statistics; see §VI.21.

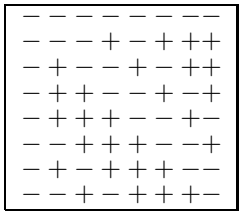
▷ Matrices, Vectors, and Codes

1.18 **Example** Begin with the set system representation of the Fano plane in Example 1.3 and construct the 7×7 matrix of 0s and 1s on the right by placing a 1 in cell (a, b) if the element a is in set b; place a 0 otherwise.

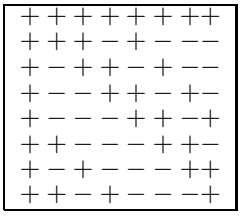
1	1	1	0	0	0	0
1	0	0	1	1	0	0
1	0	0	0	0	1	1
0	1	0	1	0	1	0
0	1	0	0	1	0	1
0	0	1	1	0	0	1
0	0	1	0	1	1	0

1.19 **Remark** The matrix in Example 1.18 is the *incidence matrix* of the Fano plane. Generally, the rows are indexed by the points of the design and the columns by the blocks. Important properties of designs can be determined by matrix properties of these incidence matrices; see §VII.7.

1.20 **Example** Apply the permutation (0)(1)(2 5 3)(4)(6) to the symbols in Example 1.3. Form a 7×7 matrix with columns indexed by blocks and rows indexed by symbols.



Place a $-$ in the cell of row x and column y when symbol x appears in block y, and a $+$ otherwise. Finally add an initial row and an initial column consisting entirely of $-$ to get the array at the left. Invert $+$ and $-$ to get the array on the right.



1.21 **Remark** Of course, the balance observed previously repeats in the matrix on the left in Example 1.20. In this presentation, however, the balance is seen in a new light. Taking $+$ to be $+1$ and $-$ to be -1, it is possible for two rows to have inner product between -8 and $+8$; yet here every pair of distinct rows have inner product exactly equal to 0 (and indeed, so do any two distinct columns). This property over $\{\pm 1\}$ defines a *Hadamard matrix*; see §V.1. Such matrices have the remarkable property that they maximize the matrix determinant over all $n \times n$ $\{\pm 1\}$-matrices; see §V.3. Generalizing to arithmetic over algebras other than $(\{\pm 1\}, \cdot)$ yields classes of orthogonal matrices and designs (§V.2).

The matrix on the right shares the same properties, being the negative of the one on the left. But a surprise is in store. Juxtapose the two horizontally, and delete the two constant columns to form an 8×14 matrix. Every two distinct columns of the result have either 0 or 4 identical entries. For each column form a set that contains the indices of the $+$ entries in that column; this yields 14 blocks each of size 4, on a set of 8 elements. Every element occurs in 7 blocks, every 2-subset of elements in 6 blocks, and every 3-subset of elements in exactly one block. This is a Steiner system and a 3-design (a Hadamard 3-design).

1.22 **Example** In Example 1.20, delete the constant row and constant column, and treat the remaining 7 rows as $\{\pm 1\}$-vectors. These vectors are:

```
[--+-+++] [+--+-++] [++--+-+] [+++--+-] [-+++--+] [+-+++--] [-+-+++-]
```

1.23 **Remark** In communicating between a sender and a receiver, synchronization is a major issue, as demonstrated by the message `...EATEATEATEATEATEATEA...`, which might say `EAT`, `ATE`, or `TEA` depending on your timing. Knowing the message, however, enables one to determine the timing. Suppose then that a sender repeatedly sent `[+-+++--]`. If the receiver is "in phase," it multiplies the expected vector with the received one, and computes 7. If "out of phase," it instead computes -1 no matter what the nonzero phase shift is. This *autocorrelation* can be used to synchronize, and the balance plays a practical purpose; see §V.9 and §V.7.

1.24 **Example** An error-correcting code.

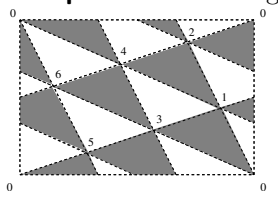
Replace $+$ by `1` and $-$ by `0` in the two Hadamard matrices of Example 1.20, and treat the 16 rows of the resulting matrices as binary vectors of length 8.

```
[00000000] [00010111]
[01001011] [01100101]
[01110010] [00111001]
[01011100] [00101110]
[11111111] [11101000]
[10110100] [10011010]
[10001101] [11000110]
[10100011] [11010001]
```

1.25 **Remark** The sixteen binary vectors of Example 1.24 have the property that every two distinct vectors differ in exactly 4 or in all 8 positions. A sender and receiver can agree that in order to communicate sixteen information symbols, they are to use these 16 "codewords." If a single bit error is made in transmission, there is exactly one codeword that could have been intended; if two bit errors are made, the receiver knows that an error occurred but does not know which two bit errors account for the incorrect received word. This is a 1-error-correcting code and a 2-error-detecting code; see §VII.1.

▷ **Graphs**

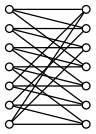
1.26 **Example** An embedding of the Fano plane on the torus.



Draw the complete graph on 7 vertices (K_7) on the torus (identify the left and right borders, and the top and bottom borders, to form the torus—you may need to purchase a second *Handbook* to do this). The number of vertices is 7 and the number of edges is 21, so the number of faces (by Euler's formula) is 14.

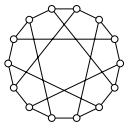
1.27 **Remark** The triangular faces in the drawing of Example 1.26 have the property that they can be colored with two colors, so that every edge belongs to one face of each color. Consider then the faces of one color; every edge (2-subset of vertices) appears in exactly one of the chosen faces (3-subset of vertices). Seven vertices, seven faces, three vertices on every face, three faces at every vertex, and for each edge exactly one face that contains it. See §VI.25 for embeddings of graphs in surfaces that correspond to designs.

1.28 **Example** In the graph shown, label points on the left by seven different symbols, and each point on the right by the 3-subset of symbols for its adjacent vertices. The seven 3-subsets thereby chosen form the blocks of a balanced incomplete block design, and this *incidence graph* shows the element-block incidence structure.

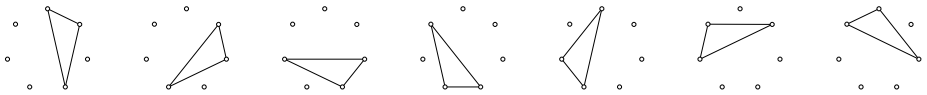


1.29 **Remark** Example 1.28 gives a purely graph-theoretic representation of the running example; see §VII.4. Again a surprise is in store. Consider Example 1.26 further. Surface duality implies that, by interchanging the roles of faces and vertices in the drawing, the embedding of a dual graph is obtained. What is the structure of the dual graph in this case? It is shown in Example 1.28.

1.30 **Example** The graph in Example 1.28 has a hamiltonian cycle. Redraw the graph with the hamiltonian cycle on the exterior. This is the *Heawood graph*, the smallest 3-regular graph whose shortest cycle has length six (also called a *cage*); see §VII.4.



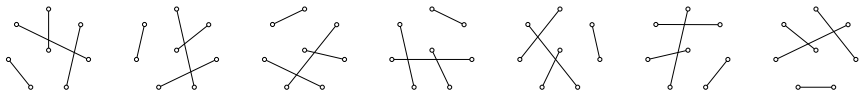
1.31 **Example** A decomposition of the complete graph into triangles.



1.32 **Remark** In another vernacular, Example 1.26 shows that K_7 can be decomposed into edge-disjoint copies of K_3 (the triangle). The toroidal embedding is not needed to see this, however. Example 1.31 explicitly shows seven K_3s that edge-partition K_7. Another line of investigation opens: When can one edge-partition a graph G into copies of a graph H? Combinatorial design theory concentrates on cases when G is a complete graph. When H is also complete, another view of balanced incomplete block designs is obtained. But when H is a cycle, a different generalization is encountered, *cycle systems*; see §VI.12. Further, when H is arbitrary, a *graph design* is obtained; see §VI.24.

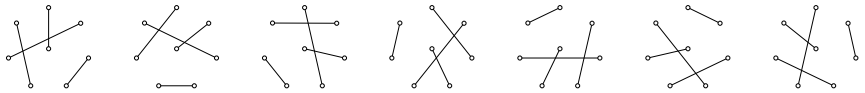
Imagine that the set of all possible edges is to be partitioned into subgraphs, so that no subgraph has too many edges; in addition, every vertex in a subgraph that has one or more edges at it incurs a cost. The goal is to minimize cost. This is achieved by choosing subgraphs that are complete whenever possible, and hence block designs provide solutions. Exactly such a problem arises in "grooming" traffic in optical networks; see §VI.27.

1.33 Example Start with blocks $\{0,1,3\}$, $\{0,4,5\}$, $\{0,2,6\}$, $\{1,2,4\}$, $\{1,5,6\}$, $\{2,3,5\}$, and $\{3,4,6\}$. Arrange the points $0,\ldots,6$ on the perimeter of a circle consecutively, and place an additional point, ∞, at the center of the circle. Now form seven graphs numbered also $0,\ldots,6$. In the ith, place the edge $\{\infty,i\}$, and for all $x \in \{0,\ldots,6\}\setminus\{i\}$ place the edge $\{x,y\}$ if and only if $\{i,x,y\}$ is a block.



1.34 Remark In Example 1.33, each of the seven graphs is a *perfect matching* or *1-factor* on the eight points. The seven 1-factors share no edges; they partition the edges of K_8 into 1-factors. This is a *1-factorization*; see §VII.5. Playing a *round-robin tournament* with 8 players over 7 time-periods can be accomplished using the matches shown here; see §VII.51.

1.35 Example An orthogonal 1-factorization and a Room square.



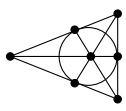
$\infty 0$	26	45		13		
	$\infty 1$	03	56		24	
		$\infty 2$	14	06		35
46			$\infty 3$	25	01	
	05			$\infty 4$	36	12
23		16			$\infty 5$	04
15	34		02			$\infty 6$

Above is shown another 1-factorization, obtained from Example 1.33 by reflecting the first picture through the vertical axis. Remarkably it has the property that every 1-factor of this factorization shares at most one edge with that of Example 1.33, such one factorizations are *orthogonal*. Form a 7×7 square (at left) with rows indexed by the factors of Example 1.33 and columns by the factors in its reflection. In each cell, place the edge (if any) that the factors share.

1.36 Remark Example 1.35 gives a square in which every cell is either empty or contains an unordered pair (edge); every unordered pair occurs in exactly one cell; and every row and every column contains every symbol exactly once. This is a *Room square*; see §VI.50. Generalizing to factorizations of regular graphs other than complete ones leads to *Howell designs*; see §VI.29.

▷ Finite Geometry

1.37 Example In the picture at right, label the three corner points by binary vectors (0,0,1), (0,1,0), and (1,0,0). When (a,b,c) and (x,y,z) are points, so also is $(a \oplus x, b \oplus y, c \oplus z) = (a,b,c) \oplus (x,y,z)$; the operation $\oplus$ is addition modulo 2. Then (1,1,0), (1,0,1), (0,1,1), and (1,1,1) are also points—but (0,0,0) is not. Lines are defined by all sets of three distinct points whose sum under $\oplus$ is (0,0,0).



1.38 Remark This is a *geometry* of points and lines that is finite; as with plane geometry, any two points define a line, and two lines meet in at most one point. Unlike usual geometry in the plane, however, there are no two lines parallel; every two lines meet in exactly one point. This is a *finite projective geometry*, one of a number of finite geometries (§VII.2). Geometries in which lines can have different sizes generalize this notion to *linear spaces*; see §VI.31.

1.2 Symmetry

1.39 Remark That the one simple structure in Example 1.1 can demonstrate balance in so many different settings is remarkable, and its vast generalizations through these different representations underpin many topics in combinatorial design theory. But the example leads to much more. It exhibits symmetry as well as balance. As a first step, note that permuting the three coordinate positions in Example 1.37 relabels the points. Yet the picture remains unchanged! This describes a sixfold *symmetry*.

1.40 Example In $\mathbb{Z}_7$ form the 3-set $\{1, 2, 4\}$ consisting of the three nonzero squares (the *quadratic residues*). Form seven sets by adding each element of $\mathbb{Z}_7$ in turn to this *base block*. These seven sets give the set system representation of the Fano plane.

1.41 Remark Example 1.40 gives another representation of the recurring example, as translates of the quadratic residues modulo 7; this opens the door into number theory (§VII.8). More than that, there is a sevenfold symmetry by translation through $\mathbb{Z}_7$. Example 1.31 depicted this symmetry already, but in Example 1.40 a more compact representation is given.

1.42 Example The automorphism group of the Fano plane.

(0 1 2 3 4 5 6)
(0 3) (1) (2 6 4 5)
(0 3 1) (2) (4 5 6)
(0) (1 3) (2) (6) (4 5)

The four permutations on the left generate a permutation group Γ of order 168. Under the action of Γ, the orbit of $\{0, 1, 3\}$ contains 7 triples; that of $\{0, 1, 5\}$ contains seven (different) triples; and that of $\{0, 1, 2\}$ contains the remaining 21 triples.

1.43 Remark Example 1.42 constructs the recurring example via the action of a group; indeed the orbit of $\{0, 1, 3\}$ under Γ provides the seven triples. As there are no other group actions that preserve this orbit, Γ is the *full automorphism group* of the design. See §VII.9 for relevant descriptions of groups. In this representation, many symmetries are provided, not all of which are easily seen geometrically. One particular symmetry of interest is that the seven points lie in a single orbit (*point transitivity*); a second is that all blocks lie in the same orbit (*block transitivity*). See §VII.5.

1.44 Example Begin again with the 3-set $\{1, 2, 4\}$ in $\mathbb{Z}_7$ from Example 1.40. Calculate differences modulo 7 among these three elements to obtain ±1, ±2, and ±3, all nonzero differences in $\mathbb{Z}_7$.

1.45 Remark In Example 1.42, not only is there a transitive action on the seven points, the action is a single 7-cycle. In Example 1.44, this is seen by the occurrence of every nonzero *difference* among the points once. Such *cyclic* designs have received particular attention. See §II.18 for cyclic and transitive symmetric designs (*difference sets*) and §VI.16 for cyclic block designs (*difference families*); also see §V.5 and §VI.17 for generalizations of orthogonal arrays defined by group actions.

1.3 Parallelism

1.46 Example On $\{0, 1, 2, 3, 4, 5, 6\} \times \{0, 1, 2\}$, form the 70 sets

$$\begin{aligned}\mathcal{B} = \quad & \{\{(i, 0), (i, 1), (i, 2)\} : i = 0, \ldots, 6\} \\ \cup \ & \{\{(i+1, j), (i+2, j), (i+4, j)\} : i = 0, \ldots, 6, j = 0, 1, 2\} \\ \cup \ & \{\{(i+3, a), (i+5, b), (i+6, c)\} : i = 0, \ldots, 6, \{a, b, c\} = \{0, 1, 2\}\}.\end{aligned}$$

Arithmetic in the first component is done modulo 7, and in the second modulo 3.

1.47 Remark Example 1.46 contains three copies of Example 1.31 within it; they lie on the points $\{0, 1, 2, 3, 4, 5, 6\} \times \{j\}$ for $j \in \{0, 1, 2\}$. Every two of the 21 points occur

together in exactly one of the 70 sets. This is a *recursive construction* of a larger design from a smaller one. Now rewrite Example 1.46.

1.48 Example For $i \in \{0,1,2,3,4,5,6\}$ let

$$\begin{aligned}\mathcal{P}_i = \quad & \{\{(i,0),(i,1),(i,2)\},\\ & \{(i+1,0),(i+2,0),(i+4,0)\}, \quad \{(i+3,0),(i+5,1),(i+6,2)\},\\ & \{(i+1,1),(i+2,1),(i+4,1)\}, \quad \{(i+3,1),(i+5,2),(i+6,0)\},\\ & \{(i+1,2),(i+2,2),(i+4,2)\}, \quad \{(i+3,2),(i+5,0),(i+6,1)\}\}.\end{aligned}$$

For $j \in \{0,1,2\}$ let $\mathcal{Q}_j = \{\{(i+3,j),(i+5,j+2),(i+6,j+1)\} : i = 0,\ldots,6\}$. The 70 sets in $\mathcal{B}$ are partitioned into ten classes $(\mathcal{P}_0,\mathcal{P}_1,\ldots,\mathcal{P}_6,\mathcal{Q}_1,\mathcal{Q}_2,\mathcal{Q}_3)$ of seven sets each in this manner.

1.49 Remark In Example 1.48, consider one of the classes in the partition. It contains seven sets each of size 3, chosen from a set system on 21 points. Asking again for "balance," one would hope that every point occurs in exactly one set of the class. And indeed it does! Each class contains every point exactly once; it is a *parallel class* or a *resolution class*. The whole design is partitioned into resolution classes; it is *resolvable*. The partition into classes is a *resolution*. Geometrically, one might think of the sets as lines, and a resolution class as a spanning set of parallel lines. Then resolvability is interpreted as a "parallelism." Resolvability is a key concept in combinatorial design theory. See §II.7 and §IV.5. Indeed resolvability also arises extensively in tournament scheduling (§VI.3,§VI.51).

1.4 Closing

1.50 Remark This short introduction has afforded only a cursory glance at the many ways in which such simple objects are generated, classified, enumerated, generalized, and applied. The main themes of combinatorial design theory, balance and symmetry, recur throughout the handbook. Nevertheless, there is more to learn from the initial tour. Often the representation chosen dictates the questions asked; one seemingly simple object appears in a myriad of disguises. To explore this world further, one piece of advice is in order. Be mindful of the ease with which any combinatorial design can arise in an equivalent formulation, with different vernacular and different lines of research. The intricate web of connections among designs may not be a blessing to those entering the area, but it is nonetheless a strength.

2 Design Theory: Antiquity to 1950

Ian Anderson
Charles J. Colbourn
Jeffrey H. Dinitz
Terry S. Griggs

Those who do not read and understand history are doomed to repeat it. (Harry Truman)

At the time of writing, every passing year sees the addition of more than five hundred new published papers on combinatorial designs and likely thousands more employing the results and techniques of combinatorial design theory. The roots of modern design theory are diverse and often unexpected. Here a brief history is given. It is intended to provide first steps in tracing the evolution of ideas in the field.

The literature on latin squares goes back at least 300 years to the monograph *Koo-Soo-Ryak* by Choi Seok-Jeong (1646–1715); he uses orthogonal latin squares of order 9 to construct a magic square and notes that he cannot find orthogonal latin squares of order 10. It is unlikely that this was the first appearance of latin squares. Ahrens [68] remarks that latin square amulets go back to medieval Islam (c1200), and a magic square of al-Buni, c 1200, indicates knowledge of two 4×4 orthogonal latin squares. In 1723, a new edition of Ozanam's four-volume treatise [1712] presented a card puzzle that is equivalent to finding two orthogonal latin squares of order 4. Then in 1776, Euler presented a paper (*De Quadratis Magicis*) to the Academy of Sciences in St. Petersburg in which he again constructed magic squares of orders 3, 4, and 5 from orthogonal latin squares. He posed the question for order 6, now known as *Euler's 36 Officers Problem*. Euler was unable to find a solution and wrote a more extensive paper [798] in 1779/1782. He conjectured that no solution exists for order 6. Indeed he conjectured further that there exist orthogonal latin squares of all orders n except when $n \equiv 2 \pmod 4$:

> et je n'ai pas hésité d'en conclure qu'on ne saurait produire aucun quarré complet de 36 cases, et que la même impossibilité s'étende aux cas de $n = 10$, $n = 14$ et en général à tous les nombres impairement pairs.

No progress was to be made on this problem for over a century, although it was not neglected by mathematicians of the day. Indeed, Gauss and Schumacher (see [862]) corresponded in 1842 about work of Clausen establishing the impossibility when $n = 6$ and conjecturing (independently of Euler) the impossibility when $n \equiv 2 \pmod 4$, which work was apparently not published. In 1900, by an exhaustive search, Tarry [2004] showed that none exists for $n = 6$, and in 1934 the statisticians Fisher and Yates [820] gave a simpler proof. Petersen [1731] in 1901 and Wernicke [2129] in 1910 published fallacious proofs of Euler's conjecture for $n \equiv 2 \pmod 4$. Then in 1922 MacNeish [1499] published another, after pointing out the error in Wernicke's approach! In 1942 Mann [1520] described the construction of orthogonal latin squares using orthomorphisms. The falsity of the general Euler conjecture was finally established in 1958 when Bose and Shrikhande [308] constructed two orthogonal squares of order 22; and then in 1960 Bose, Shrikhande, and Parker [309] established that two orthogonal latin squares of order n exist for all $n \equiv 2 \pmod 4$, other than 2 and 6.

The study of block designs can be traced back to 1835, when Plücker [1754], in a study of algebraic curves, encountered a Steiner triple system of order 9, and claimed that an STS(m) could exist only when $m \equiv 3 \pmod 6$. In 1839 he correctly revised this condition to $m \equiv 1, 3 \pmod 6$ [1755]. Plücker's discovery that every nonsingular cubic has 9 points of inflection, defining 12 lines each of 3 points, and with each pair of points on a line, illustrates the early connection between designs and geometry. Another discovery of Plücker concerned the double tangents of fourth order curves, namely, a design of 819 4-element subsets of a 28-element set such that every 3-element subset is in exactly one of the 4-element subsets, a 3-$(28, 4, 1)$ design. Plücker raised the question of constructing in general a t-$(m, t + 1, 1)$ design.

In England, a prize question of Woolhouse [2167] in the Lady's and Gentleman's Diary of 1844 asked:

> determine the number of combinations that can be made out of n symbols, p symbols in each; with this limitation, that no combination of q symbols, which may appear in any one of them shall be repeated in any other.

In 1847 Kirkman [1300] dealt with the existence of such a system in the case $p = 3$ and $q = 2$, constructing STS(m) for all $m \equiv 1, 3 \pmod 6$. The next case to be solved, $p = 4$ and $q = 3$, was done more than a century later by Hanani [1035] in 1960. The reason the *triad systems* (as Kirkman called them) are not now called Kirkman triple

systems but rather Steiner triple systems lies in the fact that Steiner [1956], apparently unaware of Kirkman's work, asked about their existence in 1853; subsequently Reiss [1799] (again) settled their existence, and later Witt [2159] named the systems after Steiner. A particular irony is that Steiner had actually asked a related but different question, which was taken up by Bussey in 1914 [407]. The name Kirkman has instead come to be attached to resolvable Steiner systems, on account of Kirkman's famous 15 schoolgirls problem [1303]: fifteen young ladies in a school walk out three abreast for seven days in succession; it is required to arrange them daily, so that no two shall walk twice abreast.

The first solution to the schoolgirls problem to appear in print was by Cayley [442] in 1850 followed in the same year by another by Kirkman [1302] himself. Kirkman's solution involved an ingenious combination of an STS(7) and a (noncyclic) Room square of side 7. In 1863, Cayley [443] pointed out that his solution could also be presented in this way. Cayley's and Kirkman's solutions are nonisomorphic as Kirkman triple systems but isomorphic as Steiner triple systems, being the two different resolutions into parallel classes of the point-line design of the projective geometry $PG(3, 2)$. In 1860 Peirce [1726] found all three solutions of the 15 schoolgirls problem having an automorphism of order 7, and in 1897 Davis [634] published an elegant geometric solution based on representing the girls as the 8 corners, the 6 midpoints of the faces, and the centre of a cube. In 1912, Eckenstein [769] published a bibliography of Kirkman's schoolgirl problem, consisting of 48 papers. The 7 nonisomorphic solutions of the 15 schoolgirls problem were enumerated by Mulder [1644] and Cole [593]. The first published solution of the existence of a Kirkman triple system of order m, KTS(m), for all $m \equiv 3 \pmod 6$ was by Ray-Chaudhuri and Wilson [1781] in 1971. The problem had in fact already been solved by the Chinese mathematician Lu Jiaxi at least eight years previously, but the solution had remained unpublished because of the political upheavals of the time. Lu also solved the corresponding problem for blocks of size 4; these results were eventually published in his collected works [1484] in 1990.

Prior claim to the authorship of the 15 schoolgirls problem was made by Sylvester [1996] in 1861, hotly refuted by both Kirkman [1305] and Woolhouse [2168]. But Sylvester raised further questions about such systems, for example: can all 455 triples from a 15-element set be arranged into 13 disjoint KTS(15)s, thereby allowing a walk for each of the 13 weeks of a school term, without any three girls walking together twice? The problem was finally solved in 1974 by Denniston [690] although both Kirkman and Sylvester had solutions for the corresponding problem with 9 instead of 15 (indeed they had the first example of a large set of designs). Surely neither Sylvester nor Denniston would have anticipated that Denniston's solution would form the basis in 2005 of a musical score, *Kirkman's Ladies* [1212], about which the composer states:

> The music seems to come from some point where precise organization meets near chaos.

The problem of the existence of large sets of KTS(n) in the general case of $n \equiv 3 \pmod 6$ is still unsolved. Sylvester also asked about the existence of a large set of 13 disjoint STS(15)s. In this case, the general problem of large sets of STS(n) is solved for all $n \equiv 1, 3 \pmod 6$, $n \neq 7$, mainly by work of Lu [1482, 1483] but also Teirlinck [2015]. Cayley [442] had shown that the maximum number of disjoint STS(7)s on the same set is 2. In 1917, Bays [169] determined that there are precisely 2 nonisomorphic large sets of STS(9).

Kirkman's solution of the 15 schoolgirls problem was extended brilliantly in 1852–3 by Anstice [103, 104]; he generalised the case where $n = 15$ to any integer of the form $n = 2p + 1$, where p is prime, $p \equiv 1 \pmod 6$. For the first time making use of primitive roots in the construction of designs (a method basic to Bose's 1939 paper) and introducing the method of difference families, Anstice constructed an infinite class

of cyclic Room squares, cyclic Steiner triple systems, and 2-rotational Kirkman triple systems. His starter-adder approach to the construction of Room squares includes the Mullin–Nemeth starters [1653] as a special case.

In 1857 Kirkman [1304] used difference sets (in the equivalent formulation of perfect partitions) to construct cyclic finite projective planes of orders 2, 3, 4, 5, and 8, introducing at the same time the concept of a multiplier of a difference set. He also wrote that he thought that a solution for 6 is "improbable," for 7 is "very likely" (because 7 is prime) and that he did not see why one should not be discovered for 9. He did not comment on order 10. A few years earlier, Kirkman [1301] had shown how to construct affine planes of prime order, and, hence, essentially by adding points at infinity, finite projective planes of all prime orders (although he did not use the geometric terminology). This paper also showed how to construct certain families of pairwise balanced designs. Such designs were to prove invaluable in later combinatorial constructions; indeed, in the same paper Kirkman himself used them to solve the schoolgirls problem for $5 \cdot 3^{m+1}$ symbols. Kirkman's work on combinatorial designs is indeed seminal. To quote Biggs [269]:

> Kirkman has established an incontestable claim to be regarded as the founding father of the theory of designs. Among his contemporaries, only Sylvester attempted anything comparable, and his papers on Tactic seem to be more concerned with advancing his claims to have discovered the subject than with advancing the subject itself. Not until the *Tactical Memoranda* of E. H. Moore in 1896 is there another contribution to rival Kirkman's.

In 1867, Sylvester [1997] investigated a tiling problem and constructed what he called *anallagmatic pavements*, which are equivalent to Hadamard matrices. He showed how to construct such of order $2n$ from a solution of order n; twenty-six years later Hadamard [1003] showed that Hadamard matrices give the largest possible determinant for a matrix whose entries are bounded by 1. Hadamard showed that the order of such a matrix had to be 1, 2, or a multiple of 4, and he constructed matrices of orders 12 and 20. In 1898 Scarpis [1846] showed how to construct Hadamard matrices of order $2^k \cdot p(p+1)$ whenever p is a prime for which a Hadamard matrix of order $p+1$ exists. In 1933 Paley [1713] used squares in $\mathbb{F}_q$ to construct Hadamard matrices of order $q+1$ when $q \equiv 3 \pmod 4$ and of order $2(q+1)$ when $q \equiv 1 \pmod 4$. He also showed that if $m = 2^n$, then the 2^m (± 1)-sequences of length m can be partitioned in such a way as to form the rows of 2^{m-n} Hadamard matrices. In a footnote Paley acknowledged that some of his results had been announced by Gilman in the 1931 *Bulletin of the AMS*, but without proof. In the same journal issue in 1933, Todd [2036] pointed out the connection between Hadamard matrices and Hadamard designs; designs with these parameters were relevant to work of Coxeter (also in the same journal issue) on regular compound polytopes! At this time the matrices were not yet called Hadamard matrices; Paley called them U-matrices. Williamson [2142] first called them Hadamard matrices in 1944. The existence of Hadamard matrices for all admissible orders remains open.

Cayley introduced the word *tactic* for the general area of designs. The word *configuration*, used nowadays more generally, was given a specific meaning in 1876 by Reye [1800] in terms of geometrical structures. Essentially, a configuration was defined to be a system of v points and b lines with k points on each line and r lines through each point, with at most one line through any two points (and hence any two lines intersecting in at most one point). If $v = b$ (and therefore $k = r$), the configuration is symmetric and denoted by v_k; thus, for example, the Fano plane is 7_3, the Pappus configuration is 9_3, and the Desargues configuration is 10_3. In fact, the first appearance of the Petersen graph is not in Petersen's paper of 1891 but in 1886 by Kempe [1277] as the graph of the Desargues configuration. In 1881, Kantor [1250] showed that there exist one 8_3, three 9_3, and ten 10_3 configurations. Six years later, Martinetti [1528]

showed there were thirty-one 11_3 configurations. In the following years, Martinetti constructed symmetric 2-configurations (two points are connected by at most 2 lines), with parameters $(7_4)_2$, $(8_4)_2$, and $(9_4)_2$ as well as the biplanes $(11_5)_2$ and $(16_6)_2$. The biplane $(11_5)_2$, also a Hadamard design 2-$(11, 5, 2)$, had previously been constructed by Kirkman [1305] in 1862. Symmetric configurations v_4 were first studied in 1913 by Merlin [1593]. In 1942, Levi [1442] unified the treatment of configurations with questions in algebra, geometry, and design theory.

Interest in counting configurations is reflected in the enumerative work on Steiner systems. It was known early on that there are unique STS(7) and STS(9). In 1897, Zulauf [2219] showed that the known STS(13)s fall into two isomorphism classes. Using the connection between STS(13)s and symmetric configurations 10_3, in 1899 De Pasquale [659] determined that only two isomorphism classes are possible. The same result was also obtained two years later by Brunel. The enumeration of nonisomorphic STS(15)s was first done by Cole, Cummings, and White. In 1913, both Cole and White published papers introducing ideas for enumeration and a year later Cummings classified all 23 STS(15)s which have a subsystem of order 7. Then in 1919, White, Cole, and Cummings [2135] in a remarkable memoir, succeeded in determining that there are precisely 80 nonisomorphic STS(15)s. In 1940, Fisher [819], unaware of this catalogue, also generated STS(15)s; he used trades on Pasch configurations to find 79 of the 80 systems. The veracity of White, Cole, and Cummings' work was confirmed in 1955 by Hall and Swift [1020] in one of the first cases in which digital computers were used to catalogue combinatorial designs. The number of nonisomorphic STS(19)s was published only in 2004 [1268], perhaps understandably as it is 11,084,874,829. Enumeration of latin squares has a more complex history (see [1573]); early results are by Euler [798] in 1782, Cayley [446] and Frolov [834] in 1890, Tarry [2004] in 1900, MacMahon [1498] in 1915, Schönhardt [1853] in 1930, Fisher and Yates [820] in 1934, and Sade [1836] and Saxena [1844] in 1951.

By the end of the 19th century there was no formal body of work called graph theory, but some graph theoretic results were in existence in the language of configurations or designs. One-factorizations of K_{2n} are resolvable 2-$(2n, 2, 1)$ designs, and the "classical" method of construction appeared in Lucas' 1883 book [1488]; the construction was credited to Walecki and can be described in terms of chords of a circle or in terms of a difference family now known as a patterned starter. Remarkably, in 1847 Kirkman [1300] already gave a construction based on a lexicographic method (in fact the greedy algorithm), which gives a schedule isomorphic to that of Lucas–Walecki. Lucas' book also describes the construction of round-dances (or hamiltonian decompositions of the complete graph) by means of what we now call a *terrace*. Enumeration results for nonisomorphic 1-factorizations of K_{2n} span nearly a century. In 1896, Moore [1626] reported that there are 6 distinct 1-factorizations of K_6 that fall into a single isomorphism class. The 6 nonisomorphic 1-factorizations of K_8 appear in Dickson and Safford [703]. Gelling [887] showed that the number of nonisomorphic 1-factorizations of K_{10} is 396, and Dinitz, Garnick, and McKay [715] showed that there are 526,915,620 nonisomorphic 1-factorizations of K_{12}.

In 1891, Netto [1670], unaware of Kirkman's work, gave four constructions for Steiner triple systems: (i) an STS$(2n+1)$ from an STS(n), (already used by Kirkman), (ii) an STS(mn) from an STS(m) and an STS(n), (iii) an STS(p) where p is a prime of the form $6m+1$, and (iv) an STS$(3p)$ where p is of the form $6m+5$. The construction given by Netto for (iii) involves primitive roots, but is not the construction usually associated with his name. These constructions enabled Netto to construct STS(n) for all admissible $n < 100$ except for $n \in \{25, 85\}$. In 1893 Moore [1624] completed Netto's proof, giving a construction of an STS$(w + u(v - w))$ from an STS(u) and an STS(v) with an STS(w) subsystem. In [1624] he also proved that for all admissible

$v > 13$, there exist at least two nonisomorphic STS(v). In 1895 and 1899, Moore [1625, 1627] determined the automorphism groups of the unique STS(7) and 3-$(8, 4, 1)$ designs and studied the intersection properties of the 30 realizations on the same base set of both systems.

Undoubtedly the most far-reaching paper by Moore is his "Tactical Memoranda I–III" [1626]. This was published in 1896 in the *American Journal of Mathematics* (founded in 1878 by Sylvester during his seven-year stay in the U.S. as professor at Johns Hopkins University). It contains many jewels hidden in 40 pages of difficult and often bewildering terminology and notation. After a brief introductory section (memorandum I), memorandum II introduces a plethora of different types of designs, including with order and/or with repeated block elements, the first occurrence of both of these concepts. Here we find the construction using finite fields of a complete set of $q - 1$ mutually orthogonal latin squares (MOLS) of order q whenever q is a prime power (a result rediscovered much later by Bose [300] in 1938 and by Stevens [1961] in 1939 independently). One also finds the theorem, later rediscovered by MacNeish [1499], that if there exist t MOLS of order m and of order n, then there exist t MOLS of order mn. Further, it contains the construction of many 1-rotational designs including Kirkman triple systems and work on orthogonal arrays. Memorandum III contains the first general results on whist tournaments and triple-whist tournaments. Whist tournaments $Wh(4n)$ had been presented by Mitchell [1618] in 1891 for several small values of n; Moore showed how to construct several infinite families of such designs. These are resolvable 2-$(4n, 4, 3)$ designs with extra properties, and are the first examples of nested designs to appear in the literature. Further in this section, Moore points out the relationship between whist tournaments $Wh(4n)$ and resolvable 2-$(4n, 4, 1)$ designs and gives a cyclic construction of such designs in the case where $4n = 3p + 1$, where p is a prime of the form $4m + 1$. At this time much work was being done on finite geometries and tactical configurations. For example, Fano [807] described a number of finite geometries in 1892, and in 1906 Veblen and Bussey [2097] used finite projective geometries to construct many designs, in particular finite projective planes of all prime power orders.

Triple systems were also studied by Heffter whose approach to the subject stemmed from his study of triangulations of complete graphs on orientable surfaces, relating these to twofold triple systems. In 1891 he gave a particularly simple construction for twofold triple systems of order $12s + 7$ [1076]. Although Kirkman, nearly 40 years earlier, had pointed to the existence of an indecomposable 2-$(7, 3, 3)$ design without repeated blocks, this seems to be the first known infinite class of designs with $\lambda > 1$. In 1896, Heffter [1077] introduced his famous first difference problem, in relation to the construction of cyclic STS($6s + 1$), and a year later both the first and second difference problems appeared [1078].

Heffter's difference problems were eventually solved in 1939 by Peltesohn [1727], and later a particularly elegant approach by Skolem [1924, 1925] was given in 1957–58. Skolem's interest in Steiner triple systems was longstanding. In 1927 he wrote notes for the second edition of Netto's book [1671], whose first edition appeared in 1901; there he constructed STS(v) for all products of primes of the form $6n + 1$ and showed that if $v = 6s + 1$ then there are at least $2s$ such STS(v). Then in [1924], he introduced the idea of a pure Skolem sequence of order n and proved that these exist if and only if $n \equiv 0, 1 \pmod 4$. In [1925] he extended this idea to that of a hooked Skolem sequence, the existence of which for all admissible n, along with that of pure Skolem sequences, would constitute a complete solution to Heffter's first difference problem. O'Keefe [1695] proved that a hooked Skolem sequence exists if and only if $n \equiv 2, 3 \pmod 4$.

In 1923–34, Bays [170, 171] undertook a systematic study of group actions on

cyclic STS, and also in [172] on SQS; this culminated in a remarkable theorem, the Bays–Lambossy theorem [1382] demonstrating that isomorphism of cyclic structures of prime orders is the same as multiplier equivalence.

The period between the two world wars saw a major step forward in the study of statistical experimental design. Already by 1788, de Palluel [618] had used a 4×4 latin square to define an experimental layout for wintering sheep (see [1985] for a modern treatment of his work). In 1924 Knut Vik [2100] described the use of certain latin squares in field experiments. But in 1926 [818], Fisher, at Rothamsted Experimental Station, indicated how orthogonal latin squares could be used in the construction of experiments. This led to detailed work in listing and enumerating all latin squares of small orders; in particular, in 1934 Fisher and Yates [820] (Fisher's successor at Rothamsted when he left to take up a chair in London) enumerated all 6×6 latin squares and established that no two were orthogonal. Then, in a 1935 paper delivered to the Royal Statistical Society, Yates [2180] drew attention to the importance of balanced block designs for statistical design. In [2181] Yates called them symmetrical incomplete randomized blocks, the present terminology of balanced incomplete block designs being introduced by Bose in 1939; but the present use of v, b, r, k, and λ goes back to Yates (except that Yates originally used t for treatment instead of v for variety). It was also in 1935 that Yates [2179] gave the first formal treatment of the factorial designs proposed by Fisher in 1926. In 1938, Fisher and Yates [821] published their important book *Statistical Tables for Biological, Agricultural and Medical Research* which, along with much statistical data, presented what was known about latin squares of small order, including complete sets of orthogonal latin squares of orders 3, 4, 5, 7, 8, and 9, as well as tables of balanced incomplete block designs with replication number r up to 10. Some gaps would be filled by Bose the following year, and some gaps would be ruled out by Fisher's inequality.

The years 1938–39 saw the publication of several important papers. Peltesohn [1727] gave a complete solution to Heffter's difference problems and hence established the existence of cyclic Steiner triple systems for all admissible orders with the exception of $v = 9$. Singer [1920] used hyperplanes in $PG(2, q)$ to construct cyclic difference sets, thereby establishing the existence of cyclic finite projective planes (a few of which had been found by Kirkman) for all prime power orders. Singer's cyclic difference sets gave the first important family of difference sets apart from those implicitly in the work of Paley, although many examples of difference families had been used by Anstice and Netto. In 1942 Bose [302] gave an affine analogue of Singer's theorem. Here he gave the first examples of relative difference sets and suggested the notion of a group divisible design (GDD). Chowla [501] constructed difference sets using biquadratic residues in 1944. In 1947, Hall [1012] published an important paper on cyclic projective planes. Difference sets were studied in depth after World War II; the important multiplier theorem of Hall and Ryser [1019] dates from 1951.

In 1938, there was also the remarkable paper by Witt [2159] on Steiner systems, detailing the existence of several Steiner systems with $t = 3$, including various families obtained geometrically and the Steiner systems $S(3, 4, 26)$ and $S(3, 4, 34)$ constructed by Fitting [822] in 1914. But of greater interest, the paper also includes the systems $S(5, 8, 24)$ and $S(5, 6, 12)$ with the Mathieu groups M_{24} and M_{12}, respectively, as their automorphism groups. Witt gives a construction of these systems as a single orbit of a starter block under the action of the groups $PSL_2(23)$ and $PSL_2(11)$, respectively, and proofs of the uniqueness of the designs as well as of their derived subsystems. He also gives a proof of the uniqueness of the system $S(3, 5, 17)$ and of the nonexistence of a system $S(4, 6, 18)$.

The results on the Mathieu systems had already appeared in 1931 by Carmichael [437, 438]. However in 1868 in the *Educational Times*, Lea [1418] both proposed the

problem and gave a solution to constructing the system $S(4, 5, 11)$. The next year another solution appeared, this time by none other than Kirkman [1306], who went on to try to construct a system $S(4, 5, 15)$. The fact that this system does not exist was not shown until 1972 by Mendelsohn and Hung [1588]. Because it is relatively easy to construct the system $S(5, 6, 12)$ from the $S(4, 5, 11)$, it is perhaps a surprise that Kirkman did not do so. Instead, this was left to Barrau [161] in 1908 who, using purely combinatorial methods, proved the existence and uniqueness of both the systems $S(4, 5, 11)$ and $S(5, 6, 12)$.

The work of Fisher and Yates created growing interest in designs among statisticians, and in 1939 Bose [301], in Calcutta, published a major paper on the subject. To quote Colbourn and Rosa [578]:

> Sixty years on, the paper of Bose forms a watershed. Before then, while combinatorial design theory arose with some frequency in other researches, it was an area without a basic theme, and without substantial application. After the paper of Bose, the themes of the area that recur today were clarified, and the importance of constructing designs went far beyond either recreational interest, or as a secondary tactical problem in a larger algebraic or geometric study.

Bose presents the study of balanced incomplete block designs as a coherent theory, using finite fields, finite projective geometries, and difference methods to create many families of designs that contain many old and many new examples. There is much material on designs with $\lambda > 1$. The use of difference families, both pure and mixed, carried on the work of Anstice of which he was unaware. Bose's paper appeared in volume 9 of the *Annals of Eugenics*. It is remarkable what combinatorial design theory appeared in that volume of 1939. Stevens [1961] discusses the existence of complete sets of orthogonal latin squares; Savur [1843] gives (yet) another construction of STSs; and Norton [1686] discusses 7×7 latin and graeco-latin squares. Stevens and Norton had presented their work at the 1938 meeting of the British Association in Cambridge, where Youden [2195] introduced the experimental designs subsequently known as Youden squares. These arrays are equivalent to latin rectangles whose columns are the blocks of a symmetric balanced design. That this representation is always possible is a consequence of Philip Hall's 1935 theorem on systems of distinct representatives (or, equivalently, König's theorem), widely known as the Marriage Problem, which has had many applications in the study of designs.

In 1938, Bose [300] proved that the existence of a complete set of $n - 1$ MOLS of order n is equivalent to the existence of a finite projective plane of order n. Then in 1938, Bose and Nair [306] introduced the ideas of association schemes and partially balanced incomplete block designs. In 1942, Bose [303] gave nontrivial examples of balanced incomplete block designs with repeated blocks. The term *association scheme* was introduced by Bose and Shimamoto [307] in 1952. Bose moved to the US in 1949, and later with Shrikhande and Parker established the falsity of the Euler conjecture, as mentioned above. This work showed clearly the usefulness of pairwise balanced designs.

While Bose's 1939 paper exploits the algebra of finite fields, the connection with algebra explored at the time was much broader. In 1877, Cayley [444, 445] discussed the structure of the multiplication table of a group (its Cayley table). Schröder, from 1890 through 1905, published a two-thousand page treatise [1857] on algebras with a binary operation, and extensively discussed quasigroups with various restrictions. Frolov [834] and Schönhardt [1853] exploited the connection between latin squares and quasigroups. However, only in the 1930s and 1940s did the area take form. In 1935, Moufang [1640] studied a specific class of quasigroups, introducing in the process the Moufang loops. In 1937, Ore and Hausmann [1701] first used the term *quasigroup* in

the sense that we do today, which left a need for a term that conveyed the additional structure of the algebras studied by Moufang. The distinction between quasigroups and loops was made explicit by Albert in 1943 [73, 74], and a general theory of quasigroups was laid by Bruck in 1944 [354, 355]. The field of universal algebra builds on these threads. The important work of Baer [133, 134] in 1939 adopted a geometric view of quasigroups as nets, and the essential connections between orthogonal latin squares and nets ensured that universal algebra and combinatorial designs were on converging paths.

Experimental design continued to generate much of the impetus for the design theory that we know today. Fisher's inequality [819] that $b \geq v$ in a block design dates from 1940. Orthogonal arrays of strength two were introduced by Plackett and Burman [1748] in 1943, and for general strength by Plackett [1747] and Rao [1775] in 1946. Weighing designs were introduced in 1944 by Hotelling [1135] and in 1945 by Kishen [1307]. Also in 1945, Finney [817] introduced fractional replication of factorial arrangements.

The applications in experimental design were, as it turned out, indicative of many more applications to come. In 1950, Belevitch [181] considered a problem in conference telephony, and in the process introduced *conference matrices*. The connection to digital communication is much more extensive.

In 1948, the new subject of information and coding theory intervened as if from nowhere. However, as MacWilliams [1502] wrote in 1968:

> Our history, of course, begins with Shannon. However, in the pre-Shannon era there was a fairly abundant growth of primeval flora and fauna, resulting in deposits of valuable fuel which we are now beginning to discover.

The fuels are perhaps not the expected ones. In 1949, Shannon and Weaver [1893] cite earlier work in statistical physics on entropy, and in the complexity of biological systems, as influential sources. However it came about, Shannon [1891] in 1948 created a new field, information theory, in a single stroke. In this seminal paper, Shannon gives a perfect error-correcting code provided to him by Hamming. As well explained in [2030], Hamming had made substantial advances in a theory of error-correcting codes but his discovery was to be tied up in patent disclosure for nearly three years. Meanwhile Golay saw Hamming's example in Shannon's paper, and in 1949 he published perfect error-correcting codes for p symbols, p a prime [923]. In 1950, the patent issue resolved, Hamming [1031] published a much fuller exposition. In 1954, Reed [1786] developed linear codes. It may appear that this work evolved in isolation, but quickly connections with experimental design and finite geometry set much of experimental design theory, combinatorial design theory, and coding theory on paths that share much to the current day.

Shannon's paper on information theory in 1948 launched coding theory into a burst of incredible growth. But Shannon's next work [1892], in 1949, was to be appreciated only much later. He developed a mathematical theory of secrecy systems, a precursor to deep connections between design theory and cryptography that have been extensively developed in the past 20 years. Indeed, many applications in communications, cryptography, and networking that continue to drive the field today were all anticipated in the literature of the middle of the last century.

The important theorems of Bruck–Ryser [356], Chowla–Ryser [503], and Bose–Connor [305] on the existence of symmetric designs and configurations appeared in 1949, 1950, and 1952, respectively. Of course, many topics in the *Handbook* were not developed until after 1950, where this history ends. However, it may be appropriate to record the first occurrence of some of these.

In 1943, Bhattacharya [249] showed that 2-$(v, 3, 2)$ designs exist for all $v \equiv 0, 1$

(mod 3), and in 1961, Hanani [1036] proved that the admissible conditions for the existence of 2-$(v, 3, \lambda)$ designs are sufficient for all λ. Necessary and sufficient conditions for the existence of directed triple systems were given by Hung and Mendelsohn [1154] in 1973 and for Mendelsohn triple systems by Mendelsohn [1586] in 1969. Also in [1036], Hanani determined the necessary and sufficient conditions for the existence of BIBDs with block size 4 and any value of λ. In 1972, Hanani [1039] did the same for BIBDs with block size 5 with the exception of the nonexistent 2-$(15, 5, 2)$ design, a fact previously discovered by Nandi [1664] in 1945. Three years later, Hanani [1042] published a survey paper over 100 pages long, containing all of his previous existence results for block sizes 3, 4 and 5; there he extended the results to block size 6 and any $\lambda \geq 2$, showing sufficiency of the basic necessary conditions for existence except for the nonexistent 2-$(21, 6, 2)$ design. The existence spectrum for block size 6 and $\lambda = 1$ remains open.

Notwithstanding the earlier examples, particularly by Anstice, Room squares are so-named after their introduction by Room [1817] in 1955. In 1968, Stanton and Mullin [1953] reintroduced the starter-adder method of construction, and the existence problem for Room squares of side $2n + 1$ for all $n \neq 3$ was finally completed in 1973 [1656]. Room squares of sides up to 29 were known by Howell in the 1890s in the context of bridge tournaments where use was also made of a generalization of Room squares, now known as Howell designs. The mathematical study of Howell designs dates from Hung and Mendelsohn [1155] in 1974. The first paper on self-orthogonal latin squares (SOLS) was by Stein [1955] in 1957. Spouse avoiding mixed doubles round robin tournaments (SAMDRR) were introduced by Brayton, Coppersmith, and Hoffman [322] in 1974 and were shown to be closely related to SOLS. Balanced tournament designs were introduced by Haselgrove and Leech [1066] in 1977. Early results on lotto designs were given by Hanani, Ornstein, and Sós [1046] in 1964. Generalized polygons were introduced by Tits [2034] in 1959 and partial geometries by Bose [304] in 1963. Golay sequences were introduced by Golay in 1961 [924]. Block's theorem [283] that under the action of an automorphism group, the number of block orbits is at least as large as the number of point orbits, dates from 1967.

In 1973, Wilson [2147] proved that given t, k, and v, there exist t-(v, k, λ) designs whenever the admissibility conditions for the design are satisfied and provided λ is sufficiently large. But the designs may have repeated blocks. In 1987, Teirlinck [2012] proved that t-designs without repeated blocks exist for all t.

The landmark contributions of Euler in 1782, Kirkman in 1847, Moore in 1896, and Bose in 1939 are central to the development of combinatorial design theory; each in its own way charted a new course for the field. With the comfort of a long historical perspective, these landmarks are easily seen; we leave it to others to write the history of the last five decades with the same benefit of historical perspective. Among the results of more modern times, however, the contributions of Wilson [2145, 2146, 2151] in demonstrating that the elementary necessary conditions for the existence of pairwise balanced designs (and block designs) are asymptotically sufficient stands out. Indeed, the techniques developed by Wilson [2149] have placed pairwise balanced designs and their close relatives among the cornerstones of modern design theory.

Many threads are interwoven to form the fabric of the area of combinatorial designs explored in this handbook. Combinatorial design theory continues to develop as a subject that is at once pure mathematics, applicable mathematics, and applied mathematics.

2.1 A Timeline

A very brief list of biographical data about the main contributors mentioned is given; only name, year and place of birth, and year and place of death, are given.

Name	Years	Birthplace	Place of Death
Ozanam, Jacques	1640–1717	Bouligneux	Paris
Choi Seok-Jeong	1646–1715	Korea	Korea
Euler, Leonhard	1707–1783	Basel	St Petersburg
Cretté de Palluel, Francois	1741–1798	Drancy-les-Noues	Dugny, France
Steiner, Jakob	1796–1863	Utzenstorf	Bern
Plücker, Julius	1801–1868	Elberfeld	Bonn
Kirkman, Thomas Penyngton	1806–1895	Bolton	Bowden, UK
Peirce, Benjamin	1809–1880	Salem MA	Cambridge MA
Woolhouse, Wesley Stoker Barker	1809–1893	North Shields	London
Anstice, Robert Richard	1813–1853	Madeley	Wigginton, UK
Sylvester, James Joseph	1814–1897	London	London
Cayley, Arthur	1821–1895	Richmond	Cambridge
Reye, Theodor	1838–1919	Ritzebüttell	Würzburg
Petersen, Julius Peter Christian	1839–1910	Sorø	Copenhagen
Schröder, Ernst	1841–1902	Mannheim	Karlsruhe
Lucas, Francois Eduard Anatole	1842–1891	Amiens	Paris
Tarry, Gaston	1843–1913	Villefranche	Le Havre
Netto, Eugen	1848–1919	Halle	Giessen
Mitchell, John Templeton	1854–1914	Glasgow	Chicago, IL
Martinetti, Vittorio	1859–1936	Scorzalo	Milan
Eckenstein, Oscar Johannes Ludwig	1859–1921	London	Aylesbury
Howell, Edwin Cull	1860–1907	Nantucket MA	Washington DC
Scarpis, Umberto	1861–1921	Padova	Bologna
Cole, Frank Nelson	1861–1926	Ashland MA	New York NY
White, Henry Seely	1861–1943	Cazenovia NY	Poughkeepsie NY
Heffter, Lothar	1862–1962	Köslin	Freiburg
Moore, Eliakim Hastings	1862–1932	Marietta OH	Chicago IL
Hadamard, Jacques	1865–1963	Versailles	Paris
Wernicke, August Ludwig Paul	1866–?	Leipzig	St. Louis MO
Cummings, Louise Duffield	1870–1947	Hamilton ON	?
Fano, Gino	1871–1952	Mantua	Verona
Barrau, Johan Anthony	1873–1953	Oisterwijk	Utrecht
Carmichael, Robert Daniel	1879–1967	Goodwater AL	Urbana IL?
Veblen, Oswald	1880–1960	Decorah IA	Brooklin ME
Bays, Severin	1885–1972	La Joux, Fribourg	Fribourg
Skolem, Thoralf Albert	1887–1963	Sandsvaer	Oslo
Fisher, Ronald Aylmer	1890–1962	London	Adelaide
Youden, William John	1900–1971	Townsville, Aus.	Washington DC
Bose, Raj Chandra	1901–1987	Hoshangabad, India	Fort Collins CO
Yates, Frank	1902–1994	Manchester	Harpenden
Golay, Marcel J E	1902–1989	Neuchâtel	Lausanne
Baer, Reinhold	1902–1979	Berlin	Zurich
Hall, Philip	1904–1982	London	Cambridge
Moufang, Ruth	1905–1977	Darmstadt	Frankfurt
Mann, Henry Berthold	1905–2000	Vienna	Tucson AZ

Name	Years	Birthplace	Place of Death
Paley, Raymond Edward Alan Christopher	1907–1933	Bournemouth	Banff AB
Chowla, Sarvadaman	1907–1995	London	Laramie WY
Todd, John Arthur	1908–1994	Liverpool	Croydon
Hall, Marshall	1910–1990	St. Louis MO	London
Witt, Ernst	1911–1991	Alsen	Hamburg
Hanani, Haim	1912–1991	Slupca, Poland	Haifa
Bruck, Richard Hubert	1914–1991	Pembroke ON	Madison WI
Hamming, Richard Wesley	1915–1998	Chicago IL	Monterey CA
Shannon, Claude Elwood	1916–2001	Gaylord MI	Medford MA
Mendelsohn, Nathan Saul	1917–2006	New York NY	Toronto ON
Ryser, Herbert John	1923–1985	Milwaukee WI	Pasadena CA
Parker, Ernest Tilden	1926–1991	Oakland MI	Urbana IL
Leech, John	1926–1992	Weybridge, UK	Firth of Clyde
Lu, Jiaxi	1935–1983	Shanghai	Baotou, China

See Also

§VI.34	History of magic squares.
[153, 154]	Kirkman triple systems.
[578]	A history for triple systems.
[1493]	Biographies of Cayley, Kirkman, Sylvester from 1916.
[1734]	The history of loops and quasigroups.
[2081]	Orthogonal latin squares, early history.

References Cited: [68, 73, 74, 103, 104, 133, 134, 153, 154, 161, 169, 170, 171, 172, 181, 249, 269, 283, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 322, 354, 355, 356, 407, 437, 438, 442, 443, 444, 445, 446, 501, 503, 578, 593, 618, 634, 659, 690, 703, 715, 769, 798, 807, 817, 818, 819, 820, 821, 822, 834, 862, 887, 923, 924, 1003, 1012, 1019, 1020, 1031, 1035, 1036, 1039, 1042, 1046, 1066, 1076, 1077, 1078, 1135, 1154, 1155, 1212, 1250, 1268, 1277, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1382, 1418, 1442, 1482, 1483, 1484, 1488, 1493, 1498, 1499, 1502, 1520, 1528, 1573, 1586, 1588, 1593, 1618, 1624, 1625, 1626, 1627, 1640, 1644, 1653, 1656, 1664, 1670, 1671, 1686, 1695, 1701, 1712, 1713, 1726, 1727, 1731, 1734, 1747, 1748, 1754, 1755, 1775, 1781, 1786, 1799, 1800, 1817, 1836, 1843, 1844, 1846, 1853, 1857, 1891, 1892, 1893, 1920, 1924, 1925, 1953, 1955, 1956, 1961, 1985, 1996, 1997, 2004, 2012, 2015, 2030, 2034, 2036, 2081, 2097, 2100, 2129, 2135, 2142, 2145, 2146, 2147, 2149, 2151, 2159, 2167, 2168, 2179, 2180, 2181, 2195, 2219]

Part II

Block Designs

1 2-(v, k, λ) Designs of Small Order

Rudolf Mathon
Alexander Rosa

1.1 Definition and Basics

1.1 A *balanced incomplete block design* (BIBD) is a pair $(V, \mathcal{B})$ where V is a v-set and $\mathcal{B}$ is a collection of b k-subsets of V (*blocks*) such that each element of V is contained in exactly r blocks and any 2-subset of V is contained in exactly λ blocks. The numbers v, b, r, k, and λ are *parameters* of the BIBD.

1.2 **Proposition** Trivial necessary conditions for the existence of a BIBD(v, b, r, k, λ) are (1) $vr = bk$, and (2) $r(k-1) = \lambda(v-1)$. Parameter sets that satisfy (1) and (2) are *admissible*.

1.3 A BIBD $(X, \mathcal{D})$ is a *subdesign* of a BIBD $(V, \mathcal{B})$ if $X \subseteq V$ and $\mathcal{D} \subseteq \mathcal{B}$. The subdesign is *proper* if $X \subset V$.

1.4 **Proposition** If a (v, k, λ) design has a proper (w, k, λ) subdesign, then $w \leq \frac{v-1}{k-1}$.

1.5 **Remark** The three parameters v, k, and λ determine the remaining two as $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{vr}{k}$. Hence one often writes (v, k, λ) *design* to denote a BIBD(v, b, r, k, λ). The notation 2-(v, k, λ) *design* is also used, because BIBDs are t-designs with $t = 2$. See §II.4. When $\lambda = 1$, the notation $S(2, k, v)$ is also employed in the literature, because such BIBDs are Steiner systems. See §II.5. The notations $S_\lambda(2, k, v)$ or (v, k, λ) BIBD for a (v, k, λ) design are also in common use.

1.6 A BIBD $(V, \mathcal{B})$ with parameters v, b, r, k, λ is

complete	or *full* if it is simple and contains $\binom{v}{k}$ blocks.
decomposable	if $\mathcal{B}$ can be partitioned into two nonempty collections $\mathcal{B}_1$ and $\mathcal{B}_2$ so that $(V, \mathcal{B}_i)$ is a (v, k, λ_i) design for $i = 1, 2$.
derived	(from a symmetric design) $(X, \mathcal{D})$ if for some $D \in \mathcal{D}$, the collection of blocks $\{D' \cap D : D' \in \mathcal{D}, D \neq D'\} = \mathcal{B}$.
Hadamard	if $v = 4n-1$, $k = 2n-1$, and $\lambda = n-1$ for some integer $n \geq 2$. See §V.1.
m-multiple	if $v, \frac{b}{m}, \frac{r}{m}, k, \frac{\lambda}{m}$ are the parameters of a BIBD.
nontrivial	if $3 \leq k < v$.
quasi-symmetric	if every two distinct blocks intersect in either μ_1 or μ_2 elements; the block intersection graph is strongly regular. See §VI.48 and §VI.11.
residual	(of a symmetric design) $(X, \mathcal{D})$ if for some $D \in \mathcal{D}$, the collection of blocks $\{D' \setminus D : D' \in \mathcal{D}, D \neq D'\} = \mathcal{B}$.
resolvable	(an *RBIBD*) if there exists a partition R of its set of blocks B into *parallel classes*, each of which in turn partitions the set V; R is a *resolution*. See §II.7
simple	if it has no repeated blocks.
symmetric	if $v = b$, or equivalently $k = r$. See §II.6.

1.7 The *incidence matrix* of a BIBD $(V, \mathcal{B})$ with parameters v, b, r, k, λ is a $v \times b$ matrix $A = (a_{ij})$, in which $a_{ij} = 1$ when the ith element of V occurs in the jth block of $\mathcal{B}$, and $a_{ij} = 0$ otherwise.

1.8 **Theorem** If A is the incidence matrix of a (v, k, λ)-design, then $AA^T = (r - \lambda)I + \lambda J$ and $JA = k\hat{J}$, where I is a $v \times v$ identity matrix, J is a $v \times v$ all ones matrix, and $\hat{J}$ is a $v \times b$ all ones matrix. Moreover, any matrix A satisfying these conditions also satisfies $\lambda(v - 1) = r(k - 1)$ and $bk = vr$; when $k < v$, it is the incidence matrix of a (v, k, λ) design. (See §VII.7.3)

1.9 **Theorem** (*Fisher's inequality*) If a BIBD(v, b, r, k, λ) exists with $2 \leq k < v$, then $b \geq v$.

1.10 **Proposition** An additional trivial necessary condition for the existence of an RBIBD is (3) $k|v$. A nontrivial condition is that $b \geq v + r - 1$, a result that extends the inequality in Theorem 1.9. See §II.7.3.

1.11 Two BIBDs (V_1, B_1), (V_2, B_2) are *isomorphic* if there exists a bijection $\alpha : V_1 \to V_2$ such that $B_1\alpha = B_2$. Isomorphism of resolutions of BIBDs is defined similarly. An *automorphism* is an isomorphism of a design with itself. The set of all automorphisms of a design forms a group, the *(full) automorphism group*. An *automorphism group* of the design is any subgroup of the full automorphism group.

1.12 **Remark** If $(V, \mathcal{B})$ is a BIBD(v, b, r, k, λ) with automorphism group G, the action of G partitions $\mathcal{B}$ into classes (*orbits*). A set of orbit representatives is a set of *starter blocks* or *base blocks*. Together with the group G, a set of base blocks can be used to define a design.

1.13 A BIBD $(V, \mathcal{B})$ with parameters v, b, r, k, λ and automorphism group G is

cyclic	if G contains a cycle of length v.
regular	if G contains a subgroup G' of order v that acts transitively on the elements.
k-rotational	if some automorphism has one fixed point and k cycles each of length $(v - 1)/k$.
transitive	if for any two elements x and y, there is an automorphism mapping x to y.

1.14 The *complement* of a design $(V, \mathcal{B})$ is $(V, \overline{\mathcal{B}})$, where $\overline{\mathcal{B}} = \{V \backslash B : B \in \mathcal{B}\}$.

1.15 **Proposition** The complement of a design with parameters (v, b, r, k, λ) is a design with parameters $(v, b, b - r, v - k, b - 2r + \lambda)$.

1.16 **Remarks**

1. In view of Proposition 1.15, one usually considers designs with $v \geq 2k$ and obtains the rest by taking the complement.
2. *Complement* has also been used, when $(V, \mathcal{B})$ is a simple 2-(v, b, r, k, λ) design, to denote the 2-$(v, \binom{v}{k} - b, \binom{v-1}{k-1} - r, k, \binom{v-2}{k-2} - \lambda)$ design obtained by taking all k-subsets *not* in $\mathcal{B}$ as blocks. The term *supplement* is used here for this second kind of complementation.

1.2 Small Examples

1.17 **Remark** To conserve space, designs are displayed in a $k \times b$ array in which each column contains the elements (taken from the decimal digits and roman letters) forming a

block. For a discussion of how to find the automorphism group of each of these designs, see Remarks VII.6.107.

1.18 **Example** The unique $(6, 3, 2)$ design and the unique $(7, 3, 1)$ design (see also Example II.6.4).

0000011122
1123423433
2345554545

0001123
1242534
3654656

1.19 **Table** The four nonisomorphic $(7, 3, 2)$ designs.

1:
00000011112222
11335533443344
22446655666655

2:
00000011112222
11335533443344
22446656565656

3:
00000011112222
11334533453344
22456646565656

4:
00000011112223
11234523453344
23456664565656

1.20 **Table** The 10 nonisomorphic $(7, 3, 3)$ designs.

1:
000000000111111222222
111333555333444333444
222444666555666666555

2:
000000000111111222222
111333555333444333444
222444666556566566556

3:
000000000111111222222
111333455333445333444
222445666456566566556

4:
000000000111111222222
111333455333445333444
222445666466556556566

5:
000000000111111222222
111333445333445333445
222456566456566456566

6:
000000000111111222223
111233455233445333444
223445666546566566565

7:
000000000111111222223
111233455233445333444
223445666645566566556

8:
000000000111111222223
111233445233455333444
223455666644566566556

9:
000000000111111222223
111233445233445333454
223456566546566456665

10:
000000000111111222233
111223445223345334544
234356566465656456656

1.21 **Table** The four nonisomorphic $(8, 4, 3)$ designs.

1:
00000001111222
11123342334334
22554666455455
34675777677766

2:
00000001111222
11123342334334
22554666455455
34675777767676

3:
00000001111222
11123342334334
22554566465455
34677677577676

4:
00000001111224
11122332233335
24645454545466
35767767667577

1.22 **Example** The unique $(9, 3, 1)$ design.

000011122236
134534534547
268787676858

1.23 **Table** The 36 nonisomorphic $(9, 3, 2)$ designs.

1:
```
000000001111112222223344
113355773344663344556655
224466885577888866777788
```
2:
```
000000001111112222223344
113355773344663344556655
224466885578787866787878
```
3:
```
000000001111112222223344
113355673344673344556655
224467885568787867687878
```
4:
```
000000001111112222223344
113355773344663344555656
224466885758786768788877
```
5:
```
000000001111112222223344
113355773344663344555656
224466885758786867787887
```
6:
```
000000001111112222223344
113355673344673344555656
224467885657887868678787
```
7:
```
000000001111112222223344
113355673344673344555656
224467885658787867687887
```
8:
```
000000001111112222223344
113355673344673344555656
224467885658787867688778
```
9:
```
000000001111112222223344
113355673344663344555756
224467885858776767886878
```
10:
```
000000001111112222223344
113355773344563344565656
224466885768786857877887
```
11:
```
000000001111112222223344
113355673344573344565656
224467885678687856788787
```
12:
```
000000001111112222223344
113355673344573344565656
224467885678687856877887
```
13:
```
000000001111112222223344
113355673344573344565656
224467885867686758788787
```
14:
```
000000001111112222223344
113355673344573344565656
224467885867686758877887
```
15:
```
000000001111112222223344
113346673345573344555656
224557884676887868677887
```
16:
```
000000001111112222223344
113345673345673344556655
224567884586787867687878
```
17:
```
000000001111112222223344
113345673345673344555656
224567884856786778687887
```
18:
```
000000001111112222223344
113345673345663344555756
224567884857786778686887
```
19:
```
000000001111112222223344
113345673345663344555657
224567884857787867686788
```
20:
```
000000001111112222223344
113345673345563344566755
224567884876785678877868
```
21:
```
000000001111112222223344
113345673345563344576655
224567884876785867687788
```
22:
```
000000001111112222223344
113345673345563344575656
224567884786876857687887
```
23:
```
000000001111112222223344
113345673345563344565756
224567884876786758876887
```
24:
```
000000001111112222233333
112445672445674455644556
233567883567887868778687
```
25:
```
000000001111112222233333
112445672445674455644556
233567883568787867878687
```
26:
```
000000001111112222233334
112445672345673455644565
233567884567888768778678
```
27:
```
000000001111112222233334
112445672345673455644565
233567884568787868778687
```
28:
```
000000001111112222233334
112445672345673455644565
233567884568788767878678
```
29:
```
000000001111112222233334
112445672345673455644565
233567884576886878778876
```
30:
```
000000001111112222233334
112445672345673455644565
233567884576888678778678
```
31:
```
000000001111112222233334
112445672345673455644565
233567884586787768868877
```
32:
```
000000001111112222233334
112445672345673455644565
233567884586788768767788
```
33:
```
000000001111112222233344
112355672344673345645655
234467885568787868776878
```
34:
```
000000001111112222233344
112355672344673345645556
234467885658786778887867
```
35:
```
000000001111112222233344
112345672345673345645655
234567885468787876886778
```
36:
```
000000001111112222233344
112345672345673345645655
234567885468787886776878
```

1.24 Table The 11 nonisomorphic $(9, 4, 3)$ designs.

1:
```
000000001111122223
111233562334433444
225544777556666555
346678888787878786
```
2:
```
000000001111122223
111233562334433444
225544777565656565
346678888788787786
```
3:
```
000000001111122223
111233462334533444
225545777456666555
346768888788778687
```
4:
```
000000001111122223
111233462334533444
225545777456666555
346768888877878687
```
5:
```
000000001111122223
111233462334533444
225545677457666555
346778888688778687
```
6:
```
000000001111122223
111233462334533444
225545677457666555
346778878678878687
```
7:
```
000000001111122223
111233462334533444
225545777465656565
346768888788787687
```
8:
```
000000001111122223
111233462334533444
225545676465757565
346778888877868876
```
9:
```
000000001111122223
111233462334533444
225545676465757565
346788788778868786
```
10:
```
000000001111122223
111233452334533444
225546677467656565
346787888578888677
```
11:
```
000000001111122234
111223352233533446
246454674745656557
357867886887887768
```

1.25 Table The three nonisomorphic $(10, 4, 2)$ designs.

1:
```
0000000111122233
1123562345345 44
2447787676586 56
3568998998997 87
```
2:
```
0000000111122233
1123562345345 44
2447787676586 56
3568999988897 97
```
3:
```
0000000111122233
1123452345345 45
2468678676476 67
3579899798589 98
```

1.26 Table The unique $(11, 5, 2)$ design and the unique $(13, 4, 1)$ design.

```
00000111223
11234236354
24567457465
35889898677
769aaaa99a8
```
```
0000111223345
1246257364789
385a46b57689a
9c7ba8cb9cabc
```

1.27 Table The two nonisomorphic $(13, 3, 1)$ designs.

1:
```
000000111112222233344455 56
13579b3469a3467867868a7897
2468ac578bc95acbbacc9bbac9
```
2:
```
000000111112222233344455 56
13579b3469a3467867868a7897
2468ac578bc95abcbcac9babc9
```

1.28 **Table** The 80 nonisomorphic $(15, 3, 1)$ designs.

1:
```
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbcdecbeddebcedcb
```

2:
```
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbcdecbededcbdebc
```

3:
```
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbcdedebcedcbcbed
```

4:
```
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbcdedbecedcbcebd
```

5:
```
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbceddecbcbdeedbc
```

6:
```
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbceddecbcdbeebdc
```

7:
```
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbdececbdcedbdbce
```

8:
```
000000011111122222233334444555566666
13579bd3478bc34789c78ab789a789a789a
2468ace569ade65abedc9deedcbdebcbcde
```

9:
```
000000011111122222233334444555566666
13579bd3478bc34789c78ab789a789a789a
2468ace569ade65abedc9deedbcdecbbcde
```

10:
```
000000011111122222233334444555566666
13579bd3478bc34789c78ab789a789a789a
2468ace569ade65abedc9deedcbdcbebedc
```

11:
```
000000011111122222233334444555566666
13579bd3478bc34789c789a789a78ab789a
2468ace569ade65abedcdbeecdbd9cebecd
```

12:
```
000000011111122222233334444555566666
13579bd3478bc34789c789a789a789a78ab
2468ace569ade65abedcdbeecdbbecdd9ce
```

13:
```
000000011111122222233334444555566666
13579bd3478bc34789c789a789a78ab789a
2468ace569ade65abedcebdedcbd9cebcde
```

14:
```
000000011111122222233334444555566666
13579bd3478bc34789c789a78ab789a789a
2468ace569ade65abedcebdd9ceedcbbcde
```

15:
```
000000011111122222233334444555566666
13579bd3478bc34789a78ac789a789b789a
2468ace569ade65bcdee9bddbecadcecebd
```

16:
```
000000011111122222233334444555566666
13579bd3478bc34789a789a78bc789a789a
2468ace569ade65bcdeedcba9eddebccbed
```

17:
```
000000011111122222233334444555566666
13579bd3478bc34789a789a789c78ab789a
2468ace569ade65bcdeedcbabedd9cecebd
```

18:
```
000000011111122222233334444555566666
13579bd3478bc34789a78ac789b789a789a
2468ace569ade65bcede9bdadcedebccbde
```

19:
```
000000011111122222233334444555566666
13579bd3478bc34789a789a78ab789c789a
2468ace569ade65bdceebdcc9deaebddceb
```

20:
```
000000011111122222233334444555566666
13579bd3478bc34789a78ac789b789a789a
2468ace569ade65bdece9bdacdedbcecebd
```

21:
```
000000011111122222233334444555566666
13579bd3478ac34789b789a789a78ab789c
2468ace569bde65acedbdcecedbd9ceeabd
```

22:
```
000000011111122222233334444555566666
13579bd3478ac34789b789a789c789a78ab
2468ace569bde65acedbdceeabdcedbd9ce
```

23:
```
000000011111122222233334444555566667
13579bd3478bc34589c789a58ab789789aa
2468ace569ade67abedcdbed9cebececdbd
```

24:
```
000000011111122222233334444555566667
13579bd3478bc34589c789a589a78978aba
2468ace569ade67abedcdbebecdecdd9ceb
```

25:
```
000000011111122222233334444555566667
13579bd3478bc34589c789a589a78978aba
2468ace569ade67abedcedbecbdbdcd9cee
```

26:
```
000000011111122222233334444555566667
13579bd3478bc3458ac789a589a789789ab
2468ace569ade67b9edcbededbcacddecbe
```

27:
```
000000011111122222233334444555566667
13579bd3478bc34589a78ab589c789789aa
2468ace569ade67bcded9ceaebdcdeebcdb
```

28:
```
000000011111122222233334444555566667
13579bd3478bc34589a78ab589c789789aa
2468ace569ade67bcedd9ceaebdedccbdeb
```

29:
```
000000011111122222233334444555566667
13579bd3478bc34589a789a58bc789789aa
2468ace569ade67bcedebdca9eddeccdbeb
```

30:
```
000000011111122222233334444555566667
13579bd3478bc34589a78ab589c789789aa
2468ace569ade67bdced9ceabedcedecbdb
```

31:
```
000000011111122222233334444555566667
13579bd3478bc34589a789a58bc789789aa
2468ace569ade67bdcedbeca9edcedecbdb
```

32:
```
000000011111122222233334444555566667
13579bd3478bc34589a78ab589c789789aa
2468ace569ade67bdcec9deaebddceebdcb
```

33:
```
000000011111122222233334444555566667
13579bd3478bc34589a78ab589c789789aa
2468ace569ade67bdecc9deaebdecddbceb
```

34:
```
000000011111122222233334444555566667
13579bd3478bc34589a789a589c78978baa
2468ace569ade67bdecdbceaebdecdc9edb
```

35:
```
000000011111122222233334444555566678
13579bd3478bc34569a689a579a78a789bc
2468ace569ade78bcdedbecedcbc9daebed
```

36:
```
000000011111122222233334444555566678
13579bd3478bc34569a689a579a78a789bc
2468ace569ade78bceddbceecdbd9caebed
```

37: 00000001111112222223333444455566678
13579bd3478bc34569a68ab579c78978aa9
2468ace569ade78bced9dceaebdceddbebc

38: 00000001111112222223333444455566678
13579bd3478bc34569a68ab579a78978ac9
2468ace569ade78bdce9cdecedbadebecdb

39: 00000001111112222223333444455566678
13579bd3478bc34569a68ab579c78978aa9
2468ace569ade78bdce9dceabedecdcebdb

40: 00000001111112222223333444455566678
13579bd3478bc34569a689a579a78a789bc
2468ace569ade78bdcecbedecdbd9caebed

41: 00000001111112222223333444455566678
13579bd3478bc34569a689c57ab78a789a9
2468ace569ade78bdceabed9dceecdcebbd

42: 00000001111112222223333444455566678
13579bd3478bc34569a68ab579c78978aa9
2468ace569ade78bdec9cdeaebddeccbebd

43: 00000001111112222223333444455566678
13579bd3478bc34569a68ac579b78978aa9
2468ace569ade78bdec9ebdacdeedcbcedb

44: 00000001111112222223333444455566678
13579bd3478bc34569a689a579a78a789bc
2468ace569ade78bdeccbdeedcbc9daebed

45: 00000001111112222223333444455566678
13579bd3478bc34569a68ac579a78978ab9
2468ace569ade78becd9bededbcacdcdbee

46: 00000001111112222223333444455566678
13579bd3478bc34569a68ab579c78978aa9
2468ace569ade78becd9dceabedceddcbeb

47: 00000001111112222223333444455566678
13579bd3478bc34569a68ab579c78978aa9
2468ace569ade78bedc9cdeabeddeccdbeb

48: 00000001111112222223333444455566678
13579bd3478bc34568a69ab578c78979aa9
2468ace569ade79becd8dceabedcdedcbeb

49: 00000001111112222223333444455566679
13579bd3478bc34568a689a578a78978abc
2468ace569ade79becddebccdbeadec9bed

50: 00000001111112222223333444455566678
13579bd3478bc34568a69ac578a78979ab9
2468ace569ade79becd8bededbcadccdbee

51: 00000001111112222223333444455566678
13579bd3478bc34568968ab579c79a78aa9
2468ace569ade7abecd9dce8ebddcecbdbe

52: 00000001111112222223333444455566678
13579bd3478bc345689689a579c79a78aab
2468ace569ade7abecdcdeb8ebddceb9dce

53: 00000001111112222223333444455566678
13579bd3478bc345689689a579c79a78aab
2468ace569ade7abecdbdec8ebddcec9dbe

54: 00000001111112222223333444455566679
13579bd3478bc345689689a578c78a78aab
2468ace569ade7abecdbecd9ebdcded9cbe

55: 00000001111112222223333444455566678
13579bd3478bc34568969ab578c78a79aa9
2468ace569ade7abecd8cde9ebdcdedbcbe

56: 00000001111112222223333444455566678
13579bd3478bc345689689a579c79a78aab
2468ace569ade7abedcdceb8ebdcdeb9cde

57: 00000001111112222223333444455566678
13579bd3478bc34568968ab579c79a78aa9
2468ace569ade7abedc9cde8ebdcdedbcbe

58: 00000001111112222223333444455566678
13579bd3478bc345689689a579c79a78aab
2468ace569ade7abedcbced8ebdcded9cbe

59: 00000001111112222223333444455566679
13579bd3478bc345689689a578a789789cb
2468ace569ade7ebacdcbeddb9caecedbde

60: 00000001111112222223333444455566679
13579bd3478bc34568968a9578a789789cb
2468ace569ade7ebacddecbcb9dadeebcde

61: 00000001111112222223333444455556666
13579bd3478ac34789b789c789a78ab789a
2468ace569bde65aecdbaedecdbd9cecdbe

62: 00000001111112222223333444455566667
13579bd3478ac34589b78ab589a789789ca
2468ace569bde67adcec9edbedcdceeabdb

63: 00000001111112222223333444455566667
13579bd3478ac34589b78ab589a789789ca
2468ace569bde67aecdd9cebcdecdeeabdb

64: 00000001111112222223333444455566667
13579bd3478ac34589a789a589b78b789ca
2468ace569bde67cdbeecdbaecdd9ebaedc

65: 00000001111112222223333444455566678
13579bd3478ac34569b68ac579a789789ba
2468ace569bde78dacee9bdbedcacecdbde

66: 00000001111112222223333444455566678
13579bd3478ac34568968ac579a79b789ba
2468ace569bde7bdacee9bd8edcacecdbde

67: 00000001111112222223333444455566679
13579bd3478ac34568a68ac578b789789ab
2468ace569bde79cbdee9bdaecdbeddacce

68: 00000001111112222223333444455566678
13579bd3478ac34569b68ac579a789789ba
2468ace569bde78adcee9bdbedccdeacbde

69: 00000001111112222223333444455566679
13579bd3478ac3456a868ac578b789789ab
2468ace569bde79bcede9bdaecddecbadce

70: 0000000111111222222333344445556667a
13579bd3478ac34568968ab5789789789cb
2468ace569bde7dbaece9cdceabadebcdde

71: 0000000111111222222333344445556667a
13579bd3478ac34568968ab5789789789cb
2468ace569bde7cabdee9cddeabbecacdde

72: 0000000111111222222333344445556667a
13579bd3478ac34568968ab5789789789cb
2468ace569bde7dcbaee9cdaecbbedadcde

73: 000000011111122222233334444555666 79
13579bd3478ac34568a689a578b78c789ab
2468ace569bde7c9bdeecdbae9dbeddacce

74: 000000011111122222233334444555667a
13579bd3478ac345698689a578b789789cb
2468ace569bde7abdecedbcce9daedbacde

75: 000000011111122222233334444555667a
13579bd3478ac345689689a578b789789cb
2468ace569bde7cdbaeedbcae9dbecacdde

76: 000000011111122222233334444555667 8
13579bd3478ac34569b68ab578978979aac
2468ace569bde7da8cee9cdcbaedebcdbed

77: 000000011111122222233334444555667 8
13579bd3478ac34569a68ab578979b789ac
2468ace569bde7d8cebe9cdacebdcebaded

78: 000000011111122222233334444555667 8
13579bd3478ac34569b689c578b78a79aa9
2468ace569bde7ac8edeabd9cdedebbdcec

79: 000000011111122222233334444555667 8
13579bd3478ac34568b689c57ab79a789a9
2468ace569bde79ecadaebd8dcecdbbdeec

80: 000000011111122222233334444555667 8
13579bd3469ac34578b678a58ab78979c9a
2468ace578bde96aecdbcded9cebecaeddb

1.29 Table Properties of the 80 STS(15)s ((15,3,1) BIBDs). $|G|$ is the order of the automorphism group. CI is the *chromatic index*, the minimum number of colors with which the blocks can be colored so that no two intersecting blocks receive the same color; when CI = 7, the design is resolvable. PC is the number of parallel classes. Sub is the number of (7,3,1)-subdesigns, and Pa is the number of Pasch configurations (four triples on six points).

#	$\|G\|$	CI	PC	Sub	Pa	#	$\|G\|$	CI	PC	Sub	Pa	#	$\|G\|$	CI	PC	Sub	Pa
1	20160	7	56	15	105	2	192	8	24	7	73	3	96	9	8	3	57
4	8	9	8	3	49	5	32	8	16	3	49	6	24	8	12	3	37
7	288	7	32	3	33	8	4	9	4	1	37	9	2	9	2	1	31
10	2	9	6	1	31	11	2	9	6	1	23	12	3	9	1	1	32
13	8	9	4	1	33	14	12	9	0	1	37	15	4	8	8	1	25
16	168	9	0	1	49	17	24	8	12	1	25	18	4	9	4	1	25
19	12	7	16	1	17	20	3	9	1	1	20	21	3	9	1	1	20
22	3	8	4	1	17	23	1	9	1	0	18	24	1	9	0	0	19
25	1	9	1	0	20	26	1	9	0	0	23	27	1	9	3	0	14
28	1	9	2	0	15	29	3	9	0	0	19	30	2	9	3	0	14
31	4	9	5	0	18	32	1	9	2	0	13	33	1	9	1	0	12
34	1	9	1	0	12	35	3	9	0	0	13	36	4	9	1	0	10
37	12	9	5	0	6	38	1	9	4	0	9	39	1	9	1	0	12
40	1	9	0	0	13	41	1	9	1	0	12	42	2	9	5	0	8
43	6	9	3	0	10	44	2	9	1	0	8	45	1	9	2	0	9
46	1	9	2	0	7	47	1	9	1	0	10	48	1	9	1	0	8
49	1	9	2	0	7	50	1	8	7	0	6	51	1	9	2	0	9
52	1	9	0	0	9	53	1	9	1	0	10	54	1	9	2	0	11
55	1	9	2	0	9	56	1	9	1	0	8	57	1	8	4	0	5
58	1	9	3	0	8	59	3	9	0	0	13	60	1	9	6	0	7
61	21	7	7	1	14	62	3	9	0	0	7	63	3	8	6	0	7
64	3	9	3	0	10	65	1	9	2	0	7	66	1	9	3	0	6
67	1	8	4	0	5	68	1	9	1	0	6	69	1	8	4	0	5
70	1	9	2	0	9	71	1	9	2	0	5	72	1	9	4	0	5
73	4	9	9	0	6	74	4	9	3	0	8	75	3	8	6	0	7
76	5	9	1	0	10	77	3	9	1	0	2	78	4	9	9	0	6
79	36	8	17	0	6	80	60	9	11	0	0						

1.30 **Table** The five nonisomorphic $(15, 7, 3)$ designs.

1:
```
000000011112222
111335533443344
222446655666655
37b797978787878
48c8a8a9a9aa9a9
59dbddbbccbbccb
6aeceecdeededde
```
2:
```
000000011112222
111335533443344
222446655666655
37b797978787878
48c8a8a9a9aa9a9
59dbddbbccbcbbc
6aeceecdeeddeed
```
3:
```
000000011112222
111335533443344
222446655666655
37b797978787878
48c8a8a9aa99aa9
59dbddbbccbcbbc
6aeceecdedeeded
```
4:
```
000000011112222
111335533443344
222446655666655
37b797879787878
48c8a9a8aa99aa9
59dbdbcdbcbcbbc
6aecedeecdeeded
```
5:
```
000000011112222
111335533443344
222446656565656
37b797977888877
48c8a8a9aa99aa9
59dbddbbccbcbbc
6aeceecdedeeded
```

1.31 **Example** The unique $(16, 4, 1)$ design.

```
0000011112222333456
147ad456945684567897
258be7b8cc79a98abbac
369cfadefefbddcfefed
```

1.32 **Table** The three nonisomorphic $(16, 6, 2)$ designs.

1:
```
0000001111222334
1123452345345455
2667896789877666
37aabcdbaa998987
48bddeeccbabccba
59ceffffedfeddef
```
2:
```
0000001111222334
1123452345345455
2667896789877666
37aabcdbaa998987
48bddeeccbacbbca
59ceffffedfdeedf
```
3:
```
0000001111222334
1123452345345455
2667896789877666
37aabcdbaa998987
48bddeeccbcabbac
59ceffffeddfeefd
```

1.33 **Table** The six nonisomorphic $(19, 9, 4)$ designs.

1:
```
0000000001111122223
1111233562334433444
2225544777556666555
3346678888787878786
499acab99a9b9aa9b99
5aebdcdabddcbcbccaa
6bfegefcdefecdfedbd
7cgfhghfehgghfgfege
8dhiiiihgiihighifih
```
2:
```
0000000001111122223
1111233562334433444
2225544777556666555
3346678888787878786
499acab99a9ba99ab99
5aebdcdabcdcbcbdcaa
6bfegefdcffeddeedbc
7cgfhghefhgggehfegf
8dhiiiihgiihhiigfih
```
3:
```
0000000001111122223
1111233562334433444
2225544777565656565
3346678888788787786
499acab99a99abba999
5aebdcdabbcdcccdbaa
6bfegefdcgfeddeedcb
7cgfhghfehhgefffefg
8dhiiiighiiihgghiih
```
4:
```
0000000001111122223
1111233562334433444
2225544777565656565
3346678888788787786
499acab99a9ab99ba99
5aebdcdabdbccccdbaa
6bfegefdcegfddeecbd
7cgfhghfehhgeffffge
8dhiiiighiihgiighih
```

5:
```
0000000001111122223
1111233462334533444
2225545777456666555
3346768888788778687
499aca9a9abb999ab99
5aebdcdbbcdccabdcaa
6bfeegfdcffeddeedbc
7cgfghhefhggeghffge
8dhiiiihgiihihighif
```

6:
```
0000000001111122223
1111233452334533444
2225546677467656565
3346787888578888677
499aaab99bc9a99ab99
5aebcddbcddcbabccaa
6bfegefcdefecdfeddb
7cgfhgghehhgfggfefe
8dhiiihifiiighihgih
```

1.34 **Table** The 18 nonisomorphic $(25, 4, 1)$ designs. Their respective automorphism group orders are: 504,63,9,9,9,150,21,6,3,3,3,3,3,3,3,3,1,1.

1:
```
0000000011111111222222233333444455556667778899aabbil
134567ce34578cd34568de468bh679f78ag79b9aabcddecejm
298dfbhkea6g9kf7c9afkg5cgfihdgifchi8ejjcjdfhgfghkn
iaolgmjnmbohnljonblhmjjdlknmeklnekmkinlimimonooloo
```

2:
```
0000000011111111222222233333444455556667778889abil
13457bce34589cd3456ade489eh6acf7bdg79ab9ab9abdecjm
2689gdfka76fekg798fckh5cfgidghichfi8chjjdfgjehfgkn
iloahnjmbmohlnjobngmljjdknmeklnekmlkinmnilmliooooo
```

3:
```
0000000011111111222222233333444455556667778889abil
13457bde34589ce3456acd489eh6acf7bdg79ab9ab9abcdejm
2689gcfka76fdkg798fehk5cgfidhgicfhi8hcjjfdejgfghkn
iloahmjnbmohnljobngljmjdkmneknleklmkminlniimlooooo
```

4:
```
0000000011111111222222233333444455556667778889abil
13457aef3458bcf34569dg489dh69ef7acg79bc9acabdcdejm
2689bcjha769djg7b8aejh5cbfkdagkebhk8gieihdifefghkn
ilodgknmemohklnocnfkmljgminhnilflimkjnmljnmjlooooo
```

5:
```
0000000011111111222222233333444455556666778899abcfil
134567cd34578de34568ce468ag67bh789f79aab9bacdedgjm
298abhgkba69fhk79bgakf5cdfiedgicehi8djejjcbfghehkn
ieolfmjnmcognjlondlhmjjhlknmfklngkmkinilmiolmnoooo
```

6:
```
0000000011111111222222333333444455556666778899abcde
123468cj23479af3458bg456ah57bi78bd89ce9adabacghiff
5ad97fek6be8gdl7ch9em89fcn6gdkfickgjdlhmeekblhijjg
oignbhmlkjhcinmlfjdonmeikoajlonlgmomhnkoijnfolmnok
```

7:
```
0000000011111111222222333333444445555566666777889al
124789bh2589ace39abde47abcf8bcde79cdf78adg89b9cabm
365egifj46fhjgi5gikhf6ihjegjikfggkjehfhekiadcbdcdn
dcaolmnk7bolmnk8olmnj9nolmknolmhmnolilmnojkjheifgo
```

8:
```
0000000011111111222222333333444455566667777889aacee
12459bdf24569cg3458bh4568bi59bh9ac78ab89cgaddbedfl
3786cihjd78haek96kfgja7fgclgkdiimfi9djebkjcjffhmgn
oanegklmifbmljnecolmnjdkhnmlmeojnhnoglmhloiknokoio
```

9:
```
0000000011111111222222233333444455556677889abcdefgh
13456789345678a34567894679c67ad68be9aab9bdecijkijk
2fbcdgiadg9jcfbaehficb5b8eg89ch7adfchdfgefghmlllmn
onklehjmmlikehnjnmgkdloilhkmjfinkgjolomnokijnnmooo
```

10:
```
0000000011111111222222233333444455566577889abccdfgh
13456789345678a345678b467ad679e69c9b89aabfghdeeijk
2jadebchekbdc9f9ciaedg5f8bg8gbf7afcihjdiemllikjlmn
onmkgfliilnmhgjljmhnfkokmchnidhlegojjkokonnmnmlooo
```

11:
```
00000000111111122222223333344444555566778899acdefgh
1345678b3456789345678a467bc679d68ae9daebcabbkijijk
2iace9fgdjbgcah9cibhdf5a8fg8bfh79gfcfdgehedclmllmn
ojmdhnklekniflmlekmjgnokmhnniglljhmojokoiikjmnnooo
```
12:
```
000000001111111222222233333444455556677889accdfgh
1345678a345678b34567894679e67ac68bd9fagbfabbdeeijk
2j9ebcmickal9dibdielaj5a8df8beg79chcgdhehgfhjiklmn
olhgdfnkhmfnegjgfnhmckomkininjljlkmokoiojnmlnmlooo
```
13:
```
000000001111111222222233333444455556667899accdfgh
134578ae34568bc345679d467ad78be689c7898ababbdeeijk
2f6b9cjg9g7dakh8ahbeif5lbigl9ifamjffhcgdegfhikjlmn
omkdhlnienimfljjclgnmkonckhmdjhenkgjiokoolnmnmlooo
```
14:
```
000000001111111222222233333444455556667899accdfgh
1345789c34568ad34567be467ad78be689c7898ababbdeeijk
2h6beajg9f7bckh8agd9if5lbifl9jgamiffhcgdegfhjiklmn
omidnflkenjglmikclmhnjoncjgmdkhenkhkjoioonmlnmlooo
```
15:
```
000000001111111222222233333444455556667889abcdeil
1345689b345679a34578ab467ad789e689c7bc9daeghffghjm
2cg7afdi8dhfbjcf6eg9kc59ebhacbfdbag8ehcfdgijkijkkn
lnkjohemknigomejinhomdmligoljhoklfonjmkmimnnnllloo
```
16:
```
000000001111111222222233333444455556667889abcdeil
134568ab345679b345789a467ae789c689d7be9cadfghfghjm
2cf7g9dk8dgafich6ebfcj59dbgaebhcbaf8dfegchkijijkkn
lnjihoemjnkohmeiknogdmmlkfoligojlhonimjmkmnnnllloo
```
17:
```
00000000111111122222223333333444455555666677778889a
147adgjm4569chi4569bdf45689ae9bcf9ach89abbcdeabicd
258behkn78ebfkl87caekgdb7cfglgkehefgjfildfighegjdj
369cfiloadgjmnonlohimjimjhoknmojlkinoknmhnkomolmln
```
18:
```
00000000111111122222223333333444455555666677778889a
147adgjm4569cef4569bcd45689ae9bdf9abe89acbcdiabcfd
258behkn78bhkil87jafghhc7jbigcekggfihelhdheglgkfij
369cfiloadgjmnoikoemnlmlfndokolnjmnjomnkinjomlohkm
```

1.3 Parameter Tables

1.35 Table Admissible parameter sets of nontrivial BIBDs with $r \le 41$ and $k \le v/2$. Earlier listings of BIBDs by Hall [1016], Takeuchi [1999], and Kageyama [1241] and papers by Hanani [1042] and Wilson [2144] are frequently referenced. Multiples of known designs are included; although their existence is trivially implied, information concerning their number and resolvability usually is not.

The admissible parameter sets of nontrivial BIBDs satisfying $r \le 41$, $3 \le k \le v/2$ and conditions (1) and (2) of Proposition 1.2 are ordered lexicographically by r, k, and λ (in this order). The column "Nd" contains the number $Nd(v, b, r, k, \lambda)$ of pairwise nonisomorphic BIBD(v, b, r, k, λ) or the best known lower bound for this number. The column "Nr" contains a dash (-) if condition (3) of Proposition 1.10 is not satisfied. Otherwise it contains the number Nr of pairwise nonisomorphic resolutions of BIBD(v, b, r, k, λ)'s or the best known lower bound. The number of nonisomorphic RBIBDs is not necessarily Nr. Indeed, there are seven nonisomorphic resolutions of BIBD(15,35,7,3,1)s but only four nonisomorphic RBIBD(15,35,7,3,1)s (see Example II.2.76). The symbol ? indicates that the existence of the corresponding BIBD (RBIBD, respectively) is in doubt. The meanings of the "Comments" are:

m#x	m-multiple of an existing BIBD #x
m#x*	m-multiple of #x that does not exist or whose existence is undecided
R#x (D#x)	residual (derived) design of #x that exists
R#x* (D#x*)	residual (derived) design of #x that does not exist or whose existence is undecided
#x+#y	union of two designs on the same set of elements
#x↓#y	design #x is a design $(V, \mathcal{B})$ with parameters (v, b, r, k, λ); design #y is a design $(V, \mathcal{D})$ with parameters $(v, b', b-r, k+1, r-\lambda)$; add a new point ∞ to each block of $\mathcal{B}$ to obtain $\widehat{\mathcal{B}}$; then $(V, \widehat{\mathcal{B}} \cup \mathcal{D})$ is a design with parameters $(v+1, b+b', b, k+1, r)$.
PG (AG)	projective (affine) geometry (see §VII.2)
×1	BIBD does not exist by Bruck–Ryser–Chowla (BRC) Theorem (see §II.6.2)
×2	BIBD is a residual of a BIBD that does not exist by the BRC theorem, and $\lambda = 1$ or 2
×3	RBIBD does not exist by Bose's condition (see Theorem II.7.28).
HD	RBIBD$(4t, 8t-2, 4t-1, 2t, 2t-1)$ exists from a symmetric (Hadamard) BIBD$(4t-1, 4t-1, 2t-1, 2t-1, t-1)$; see §V.1.

Typically no references are given under "Ref" for multiple, derived, or residual designs of known BIBDs. A trivial formula giving $Nd(v, mb, mr, k, m\lambda) \geq n+1$ is often used provided $Nd(v, b, r, k, \lambda) \geq n$, $m \geq 2, n \geq 1$ (similarly for Nr). The column "Where?" gives a pointer to an explicit construction.

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
1	7	7	3	3	1	1		- PG(2,2)	II.6.4
2	9	12	4	3	1	1	1	R#3,AG(2,3)	1.22
3	13	13	4	4	1	1		- PG(2,3)	1.26
4	6	10	5	3	2	1	0	R#7,×3	1.18
5	16	20	5	4	1	1	1	R#6,AG(2,4)	1.31
6	21	21	5	5	1	1		- PG(2,4)	VI.18.73
7	11	11	5	5	2	1		-	1.26
8	13	26	6	3	1	2		- [1544]	1.27
9	7	14	6	3	2	4		- 2#1,D#20 [1665]	1.19
10	10	15	6	4	2	3		- R#13 [1665]	1.25
11	25	30	6	5	1	1	1	R#12,AG(2,5)	
12	31	31	6	6	1	1		- PG(2,5)	VI.18.73
13	16	16	6	6	2	3		- [898]	1.32
14	15	35	7	3	1	80	7	PG(3,2) [1241, 1544]	1.28
15	8	14	7	4	3	4	1	R#20,$AG_2(3,2)$ [1241, 898]	1.21
16	15	21	7	5	2	0	0	R#19*,×2	
17	36	42	7	6	1	0	0	R#18*,×2,AG(2,6)	
18	43	43	7	7	1	0		- ×1,PG(2,6)	
19	22	22	7	7	2	0		- ×1	
20	15	15	7	7	3	5		- $PG_2(3,2)$ [898]	1.30
21	9	24	8	3	2	36	9	2#2,D#40 [1547]	1.23
22	25	50	8	4	1	18		- [1339, 1945]	1.34
23	13	26	8	4	2	2461		- 2#3 [1743]	
24	9	18	8	4	3	11		- D#41 [898]	1.24
25	21	28	8	6	2	0		- R#28*,×2	
26	49	56	8	7	1	1	1	R#27,AG(2,7)	
27	57	57	8	8	1	1		- PG(2,7)	VI.18.73
28	29	29	8	8	2	0		- ×1	
29	19	57	9	3	1	11084874829		- [1268]	VI.16.12
30	10	30	9	3	2	960		- D#54 [537, 856, 1174]	VI.16.81

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
31	7	21	9	3	3	10	-	3#1 [696]	1.20
32	28	63	9	4	1	≥ 4747	≥ 7	[1346, 1533, 1548]	III.1.8
33	10	18	9	5	4	21	0	R#41,×3 [898]	VI.16.85
34	46	69	9	6	1	0	-	[1138]	
35	16	24	9	6	3	18920	-	R#40 [1938]	II.6.30
36	28	36	9	7	2	8	0	R#39,×3 [124]	
37	64	72	9	8	1	1	1	R#38,AG(2,8)	
38	73	73	9	9	1	1	-	PG(2,8)	VI.18.73
39	37	37	9	9	2	4	-	[124]	II.6.47
40	25	25	9	9	3	78	-	[694]	II.6.47
41	19	19	9	9	4	6	-	[898]	1.33
42	21	70	10	3	1	≥ 62336617	≥ 63745	[518, 1263]	VI.16.12
43	6	20	10	3	4	4	1	2#4 [1241, 976]	
44	16	40	10	4	2	$\geq 2.2 \cdot 10^6$	339592	2#5 [696, 1267]	
45	41	82	10	5	1	≥ 15	-	[1347]	VI.16.16
46	21	42	10	5	2	≥ 22998	-	2#6 [2064]	
47	11	22	10	5	4	4393	-	2#7,D#63 [323]	
48	51	85	10	6	1	?	-		
49	21	30	10	7	3	3809	0	R#54,×3 [1016, 1241, 1946]	
50	36	45	10	8	2	0	-	R#53*,×2	
51	81	90	10	9	1	7	7	R#52,AG(2,9) [679, 1373]	
52	91	91	10	10	1	4	-	PG(2,9) [679, 1373]	VI.18.73
53	46	46	10	10	2	0	-	×1	
54	31	31	10	10	3	151	-	[1941]	II.6.47
55	12	44	11	3	2	242995846	74700	D#84 [1704]	VI.16.81
56	12	33	11	4	3	≥ 17172470	5	D#85* [1632, 1938]	VI.16.83
57	45	99	11	5	1	≥ 16	?	[1548]	VI.16.31
58	12	22	11	6	5	11603	1	R#63,HD [1016, 1241, 1743]	
59	45	55	11	9	2	≥ 16	0	R#62,×3 [1241, 692]	
60	100	110	11	10	1	0	0	R#61*,AG(2,10) [1378]	
61	111	111	11	11	1	0	-	PG(2,10) [1378]	
62	56	56	11	11	2	≥ 5	-	[1188]	II.6.47
63	23	23	11	11	5	1106	-	[1016, 1172, 1943]	VI.18.73
64	25	100	12	3	1	$\geq 10^{14}$	-	[1544]	VI.16.12
65	13	52	12	3	2	≥ 1897386	-	2#8,D#96 [790]	
66	9	36	12	3	3	22521	426	3#2 [1543, 1707]	
67	7	28	12	3	4	35	-	4#1 [976]	
68	37	111	12	4	1	≥ 51402	-	[587, 1349]	VI.16.14
69	19	57	12	4	2	≥ 423	-	[1533]	VI.16.15
70	13	39	12	4	3	≥ 3702	-	3#3,D#97 [1548, 1940]	
71	10	30	12	4	4	13769944	-	2#10 [696]	
72	25	60	12	5	2	≥ 118884	≥ 748	2#11 [1225, 2062]	
73	61	122	12	6	1	?	-		
74	31	62	12	6	2	≥ 72	-	2#12 [1239]	
75	21	42	12	6	3	≥ 236	-	[1262]	VI.16.18
76	16	32	12	6	4	≥ 111	-	2#13 [1224]	
77	13	26	12	6	5	19072802	-	D#98 [1016, 1267]	
78	22	33	12	8	4	0	-	R#85* [1372]	
79	33	44	12	9	3	≥ 3375	-	R#84 [1551, 1999]	
80	55	66	12	10	2	0	-	R#83*,×2	
81	121	132	12	11	1	≥ 1	≥ 1	R#82,AG(2,11)	
82	133	133	12	12	1	≥ 1	-	PG(2,11)	VI.18.73
83	67	67	12	12	2	0	-	×1	
84	45	45	12	12	3	≥ 3752	-	[1551]	VI.18.73
85	34	34	12	12	4	0	-	×1	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
86	27	117	13	3	1	$\geq 10^{11}$	$\geq 1.4 \cdot 10^{13}$	AG(3,3) [1546, 2148]	VI.16.12
87	40	130	13	4	1	$\geq 10^{6}$	≥ 2	PG(3,3) [1241]	VI.16.14
88	66	143	13	6	1	≥ 1		? [693]	II.3.32
89	14	26	13	7	6	15111019	0	R#98,×3 [1267, 1999]	
90	27	39	13	9	4	$\geq 2.45 \cdot 10^{8}$	68	R#97,$AG_2(3,3)$ [1241, 1380, 1381]	
91	40	52	13	10	3	?	0	R#96*,×3	
92	66	78	13	11	2	≥ 2	0	R#95,×3 [1241, 114]	
93	144	156	13	12	1	?	?	R#94*,AG(2,12)	
94	157	157	13	13	1	?	-	PG(2,12)	
95	79	79	13	13	2	≥ 2	-	[114]	II.6.47
96	53	53	13	13	3	0	-	×1	
97	40	40	13	13	4	≥ 1108800	-	$PG_2(3,3)$ [1374]	VI.18.73
98	27	27	13	13	6	208310	-	[1943]	VI.18.73
99	15	70	14	3	2	≥ 685521	≥ 36	2#14,D#140 [734, 1548]	
100	22	77	14	4	2	≥ 7921	-	[827]	VI.16.15
101	8	28	14	4	6	2310	4	2#15 [1743]	
102	15	42	14	5	4	≥ 896	0	2#16*,D#141* [1265, 2031]	VI.16.85
103	36	84	14	6	2	≥ 5	≥ 2	2#17* [1228, 2130]	VI.16.86
104	15	35	14	6	5	≥ 117	-	D#142 [1016, 1533]	VI.16.86
105	85	170	14	7	1	?	-		
106	43	86	14	7	2	≥ 4	-	2#18* [1]	VI.16.30
107	29	58	14	7	3	≥ 1	-		VI.16.30
108	22	44	14	7	4	≥ 3393	-	2#19* [2031]	VI.16.30
109	15	30	14	7	6	≥ 57810	-	2#20,D#143 [1545]	
110	78	91	14	12	2	0	-	R#113*,×2	
111	169	182	14	13	1	≥ 1	≥ 1	R#112,AG(2,13)	
112	183	183	14	14	1	≥ 1	-	PG(2,13)	VI.18.73
113	92	92	14	14	2	0	-	×1	
114	31	155	15	3	1	$\geq 6 \cdot 10^{16}$	-	[1548]	VI.16.12
115	16	80	15	3	2	$\geq 10^{13}$	-	D#169 [1548]	VI.16.13
116	11	55	15	3	3	≥ 436800	-	[1548]	VI.16.24
117	7	35	15	3	5	109	-	5#1 [1938]	
118	6	30	15	3	6	6	0	3#4 [976, 1548]	
119	16	60	15	4	3	$\geq 6 \cdot 10^{5}$	$\geq 6 \cdot 10^{5}$	3#5,D#170 [1548]	
120	61	183	15	5	1	≥ 10	-	[587]	VI.16.16
121	31	93	15	5	2	≥ 1	-		VI.16.17
122	21	63	15	5	3	$\geq 10^{9}$	-	3#6 [331]	
123	16	48	15	5	4	≥ 294	-	D#171 [352, 734, 1016]	
124	13	39	15	5	5	≥ 76	-	[1016, 2059, 734]	VI.16.17
125	11	33	15	5	6	≥ 127	-	3#7 [324, 1224]	
126	76	190	15	6	1	≥ 1	-	[1612]	II.3.32
127	26	65	15	6	3	≥ 1	-	[1016]	VI.16.89
128	16	40	15	6	5	≥ 25	-	D#172 [1016, 1533, 734]	
129	91	195	15	7	1	≥ 2	?	[246]	VI.16.70
130	16	30	15	8	7	$\geq 9 \cdot 10^{7}$	5	R#143,$AG_3(4,2)$,HD [1271, 1319]	
131	21	35	15	9	6	$\geq 10^{4}$	-	R#142 [1016, 404]	
132	136	204	15	10	1	?	-		
133	46	69	15	10	3	?	-		
134	28	42	15	10	5	≥ 3	-	R#141* [2090]	
135	56	70	15	12	3	≥ 4	-	R#140 [1005]	
136	91	105	15	13	2	0	0	R#139*,×2	
137	196	210	15	14	1	0	0	R#138*,×2,AG(2,14)	
138	211	211	15	15	1	0	-	×1,PG(2,14)	
139	106	106	15	15	2	0	-	×1	
140	71	71	15	15	3	≥ 72	-	[1005, 1832]	II.6.47

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
141	43	43	15	15	5	0		- $\times 1$	
142	36	36	15	15	6	≥ 25634		- [1944]	VI.18.73
143	31	31	15	15	7	≥ 22478260		- $PG_3(4,2)$ [1375]	VI.18.80
144	33	176	16	3	1	$\geq 10^{13}$	≥ 4494390	[1548, 562]	VI.16.12
145	9	48	16	3	4	16585031	149041	4#2 [1707]	
146	49	196	16	4	1	≥ 769		- [396, 978, 587]	VI.16.14
147	25	100	16	4	2	≥ 17		- 2#22	
148	17	68	16	4	3	≥ 542		- D#185 [1999, 734]	
149	13	52	16	4	4	≥ 2462		- 4#3	
150	9	36	16	4	6	270474142		- 2#24 [1705]	
151	65	208	16	5	1	≥ 2	≥ 1	[514, 587]	VI.16.16
152	81	216	16	6	1	?		-	
153	21	56	16	6	4	≥ 1		- 2#25* [1042]	II.3.32
154	49	112	16	7	2	≥ 1	≥ 1	2#26	
155	113	226	16	8	1	?		-	
156	57	114	16	8	2	≥ 1362		- 2#27 [1239]	
157	29	58	16	8	4	≥ 2		- 2#28* [1999]	VI.16.30
158	17	34	16	8	7	≥ 28		- D#186 [734, 1999, 2060]	
159	145	232	16	10	1	?		-	
160	25	40	16	10	6	≥ 43		- R#172 [1236, 1938]	
161	33	48	16	11	5	≥ 19	0	R#171,$\times 3$ [1241, 352]	
162	177	236	16	12	1	?		-	
163	45	60	16	12	4	≥ 1		- R#170 [180]	
164	65	80	16	13	3	?	0	R#169*,$\times 3$	
165	105	120	16	14	2	?		- R#168*	
166	225	240	16	15	1	?	?	R#167*,AG(2,15)	
167	241	241	16	16	1	?		- PG(2,15)	
168	121	121	16	16	2	?		-	
169	81	81	16	16	3	?		-	
170	61	61	16	16	4	≥ 6		- [1398]	II.6.47
171	49	49	16	16	5	≥ 12146		- [1321]	II.6.47
172	41	41	16	16	6	≥ 115307		- [1938]	II.6.47
173	18	102	17	3	2	$\geq 4 \cdot 10^{14}$	≥ 173	D#217* [734, 1040, 1548]	VI.16.81
174	52	221	17	4	1	≥ 206	≥ 30	[392, 587, 1377]	VI.16.14
175	35	119	17	5	2	≥ 1	≥ 1	[1999, 1]	VI.16.17
176	18	51	17	6	5	≥ 582	≥ 2	D#218* [1999, 1243, 734]	VI.16.86
177	35	85	17	7	3	≥ 2	?	[1, 1044, 1548]	
178	120	255	17	8	1	≥ 94	≥ 1	[1729, 1877]	
179	18	34	17	9	8	$\geq 10^3$	0	R#186,$\times 3$ [404, 1241, 1999]	
180	52	68	17	13	4	≥ 6	0	R#185,$\times 3$ [1241, 2065]	
181	120	136	17	15	2	0	0	R#184*,$\times 2$	
182	256	272	17	16	1	≥ 189	≥ 189	R#183,AG(2,16) [1207, 1208]	
183	273	273	17	17	1	≥ 22		- PG(2,16) [660, 1208, 1207]	VI.18.73
184	137	137	17	17	2	0		- $\times 1$	
185	69	69	17	17	4	≥ 4		- [2065]	II.6.47
186	35	35	17	17	8	≥ 108131		- [1944]	VI.18.73
187	37	222	18	3	1	$\geq 10^{10}$		- [1463, 1999]	VI.16.12
188	19	114	18	3	2	$\geq 2 \cdot 10^9$		- 2#29,D#231* [1548]	
189	13	78	18	3	3	$\geq 3 \cdot 10^9$		- 3#8 [1548]	
190	10	60	18	3	4	≥ 961		- 2#30	
191	7	42	18	3	6	418		- 6#1 [1743, 1938]	
192	28	126	18	4	2	≥ 139	≥ 8	2#32	
193	10	45	18	4	6	≥ 14819		- 3#10 [1548]	
194	25	90	18	5	3	$\geq 10^{17}$	$\geq 10^{17}$	3#11 [1548]	
195	10	36	18	5	8	≥ 135922	5	2#33 [1271, 1545]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
196	91	273	18	6	1	≥ 4		- [534, 1607]	VI.16.18
197	46	138	18	6	2	≥ 1		- 2#34*	VI.16.18
198	31	93	18	6	3	$\geq 10^{22}$		- 3#12 [1548]	
199	19	57	18	6	5	≥ 1535		- D#232* [734]	II.7.46
200	16	48	18	6	6	$\geq 10^8$		- 3#13,2#35 [1548]	
201	28	72	18	7	4	≥ 392		? 2#36 [1224]	
202	64	144	18	8	2	≥ 121	≥ 121	2#37 [1225]	
203	145	290	18	9	1	?		-	
204	73	146	18	9	2	≥ 3500		- 2#38 [1239]	
205	49	98	18	9	3	≥ 1		- [1628]	VI.16.30
206	37	74	18	9	4	≥ 852		- 2#39 [1224]	
207	25	50	18	9	6	≥ 79		- 2#40	
208	19	38	18	9	8	≥ 108		- 2#41,D#233 [734]	
209	55	99	18	10	3	?		-	
210	100	150	18	12	2	?		-	
211	34	51	18	12	6	≥ 2		- R#218* [1496]	
212	85	102	18	15	3	?		- R#217*	
213	136	153	18	16	2	?		- R#216*	
214	289	306	18	17	1	≥ 1	≥ 1	R#215,AG(2,17)	
215	307	307	18	18	1	≥ 1		- PG(2,17)	VI.18.73
216	154	154	18	18	2	?		-	
217	103	103	18	18	3	0		- $\times 1$	
218	52	52	18	18	6	0		- $\times 1$	
219	39	247	19	3	1	$\geq 10^{44}$	≥ 1626684	[1463, 562]	VI.16.12
220	20	95	19	4	3	≥ 10040	≥ 204	D#270 [1999, 623, 734]	VI.16.83
221	20	76	19	5	4	≥ 10067	≥ 14	D#271* [734, 1042]	VI.16.85
222	96	304	19	6	1	≥ 1		? [1609]	II.3.32
223	153	323	19	9	1	?		?	
224	20	38	19	10	9	$\geq 10^{16}$		3 R#233,HD [1319]	
225	39	57	19	13	6	?		0 R#232*,$\times 3$	
226	96	114	19	16	3	?		0 R#231*,$\times 3$	
227	153	171	19	17	2	0		0 R#230*,$\times 2$	
228	324	342	19	18	1	?		? R#229*,AG(2,18)	
229	343	343	19	19	1	?		- PG(2,18)	
230	172	172	19	19	2	0		- $\times 1$	
231	115	115	19	19	3	?		-	
232	58	58	19	19	6	0		- $\times 1$	
233	39	39	19	19	9	$\geq 5.87 \cdot 10^{14}$		- [1374]	V.1.28
234	21	140	20	3	2	$\geq 5 \cdot 10^{14}$	≥ 79	2#42,D#307 [1548]	
235	9	60	20	3	5	5862121434	203047732	5#2 [1707]	
236	6	40	20	3	8	13	1	4#4 [1174]	
237	61	305	20	4	1	≥ 18132		- [1999, 587]	VI.16.61
238	31	155	20	4	2	≥ 43		- [1999, 734]	VI.16.15
239	21	105	20	4	3	≥ 26320		- D#308* [1999, 734]	VI.16.15
240	16	80	20	4	4	$\geq 6 \cdot 10^5$	$\geq 6 \cdot 10^5$	4#5 [1548]	
241	13	65	20	4	5	$\geq 10^3$		- 5#3 [1548]	
242	11	55	20	4	6	≥ 348		- [734]	VI.16.15
243	81	324	20	5	1	≥ 1		- [1999]	VI.16.16
244	41	164	20	5	2	≥ 6		- 2#45	
245	21	84	20	5	4	$\geq 10^9$		- 4#6,D#309 [1548]	II.7.46
246	17	68	20	5	5	≥ 7260		- [514, 734]	VI.16.17
247	11	44	20	5	8	≥ 4394		- 4#7	
248	51	170	20	6	2	≥ 446		- 2#48* [2063]	VI.16.91
249	21	70	20	6	5	≥ 1		- D#310 [1042]	VI.16.18
250	21	60	20	7	6	≥ 3810	≥ 1	2#49,D#311* [1]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
251	36	90	20	8	4	≥ 2		- 2#50* [1, 2071]	
252	81	180	20	9	2	≥ 1169	≥ 1169	2#51 [1225]	
253	181	362	20	10	1	?		-	
254	91	182	20	10	2	≥ 46790		- 2#52 [1239]	
255	61	122	20	10	3	≥ 1		- [1628]	VI.16.30
256	46	92	20	10	4	≥ 1		- 2#53* [1628]	VI.16.30
257	37	74	20	10	5	≥ 1		- [1999]	VI.16.30
258	31	62	20	10	6	≥ 152		- 2#54	
259	21	42	20	10	9	≥ 4		- D#312 [1999, 248]	
260	111	185	20	12	2	?		-	
261	45	75	20	12	5	?		-	
262	141	188	20	15	2	?		-	
263	57	76	20	15	5	?		- R#271*	
264	36	48	20	15	8	≥ 1		- [1912]	
265	76	95	20	16	4	≥ 1		- R#270 [1999, 514]	
266	171	190	20	18	2	?		- R#269*	
267	361	380	20	19	1	≥ 1	≥ 1	R#268,AG(2,19)	
268	381	381	20	20	1	≥ 1		- PG(2,19)	VI.18.73
269	191	191	20	20	2	?		-	
270	96	96	20	20	4	≥ 2		- [1839]	VI.18.73
271	77	77	20	20	5	0		- $\times 1$	
272	43	301	21	3	1	$\geq 5 \cdot 10^{64}$		- [1042, 1463]	VI.16.12
273	22	154	21	3	2	$\geq 3 \cdot 10^{9}$		- D#336* [1548]	VI.16.81
274	15	105	21	3	3	$\geq 10^{15}$	$\geq 10^{11}$	3#14 [1548]	
275	8	56	21	3	6	3077244		- [1938]	VI.16.82
276	7	49	21	3	7	1508		- 7#1 [1743, 1938]	
277	64	336	21	4	1	$\geq 1.4 \cdot 10^{31}$	$\geq 2.5 \cdot 10^{37}$	[1546]	VI.16.14
278	8	42	21	4	9	8360901	10	3#15 [696]	
279	85	357	21	5	1	$\geq 3.2 \cdot 10^{38}$	≥ 1	PG(3,4) [1546, 587]	VI.16.70
280	15	63	21	5	6	≥ 2211	≥ 149	3#16* [1549]	VI.16.17
281	106	371	21	6	1	≥ 1		- [1606]	II.3.32
282	36	126	21	6	3	≥ 1	≥ 1	3#17* [1042, 1]	VI.16.86
283	22	77	21	6	5	≥ 3		- D#337,#6↓#153 [1053]	VI.16.18
284	16	56	21	6	7	≥ 1		- #13+#128 [1903]	
285	127	381	21	7	1	?		-	
286	64	192	21	7	2	≥ 1		- [2]	II.3.32
287	43	129	21	7	3	≥ 1		- 3#18* [2144]	VI.16.30
288	22	66	21	7	6	≥ 1		- 3#19*,D#338* [1042]	II.7.47
289	19	57	21	7	7	≥ 1		- [2144]	II.7.46
290	15	45	21	7	9	$\geq 10^{8}$		- 3#20 [1548]	
291	57	133	21	9	3	≥ 1		- [21]	
292	190	399	21	10	1	?		?	
293	22	42	21	11	10	≥ 2	0	R#312,$\times 3$ [1241, 1999, 1013]	
294	232	406	21	12	1	?		-	
295	274	411	21	14	1	?		-	
296	92	138	21	14	3	?		-	
297	40	60	21	14	7	?		- R#311*	
298	295	413	21	15	1	?		-	
299	50	70	21	15	6	≥ 1		- R#310 [1185]	
300	64	84	21	16	5	≥ 10810800	≥ 157	R#309,$AG_2(3,4)$ [1374, 1223]	
301	85	105	21	17	4	?	0	R#308*,$\times 3$	
302	120	140	21	18	3	?		- R#307*	
303	190	210	21	19	2	?	0	R#306*,$\times 3$	
304	400	420	21	20	1	?	?	R#305*,AG(2,20)	
305	421	421	21	21	1	?		- PG(2,20)	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
306	211	211	21	21	2	?		-	
307	141	141	21	21	3	0		- $\times 1$	
308	106	106	21	21	4	0		- $\times 1$	
309	85	85	21	21	5	≥ 213964		- $PG_2(3,4)$ [1223]	VI.18.73
310	71	71	21	21	6	≥ 2		- [1185]	II.6.47
311	61	61	21	21	7	0		- $\times 1$	
312	43	43	21	21	10	≥ 82		- [1013, 2066]	VI.18.73
313	45	330	22	3	1	$\geq 6 \cdot 10^{76}$	≥ 84	[1042, 1463, 1548]	VI.16.12
314	12	88	22	3	4	≥ 20476	≥ 3	2#55	
315	34	187	22	4	2	≥ 1		- [1042]	VI.16.15
316	12	66	22	4	6	$\geq 1.7 \cdot 10^6$	≥ 1	2#56	
317	45	198	22	5	2	≥ 17		? 2#57	
318	111	407	22	6	1	≥ 1		- [1609]	II.3.32
319	12	44	22	6	10	≥ 11604	545	2#58 [324, 1271]	
320	133	418	22	7	1	?		?	
321	45	110	22	9	4	≥ 1353		? 2#59 [1224]	
322	100	220	22	10	2	≥ 1		? 2#60* [528]	IV.2.67
323	221	442	22	11	1	?		-	
324	111	222	22	11	2	?		- 2#61*	
325	56	112	22	11	4	≥ 2696		- 2#62 [1224]	
326	45	90	22	11	5	≥ 1		- [1628]	VI.16.30
327	23	46	22	11	10	≥ 1103		- 2#63,D#351	
328	287	451	22	14	1	?		-	
329	45	66	22	15	7	?		? R#338*	
330	56	77	22	16	6	≥ 3		- R#337 [2045]	
331	133	154	22	19	3	?	0	R#336*,$\times 3$	
332	210	231	22	20	2	0		- R#335*,$\times 2$	
333	441	462	22	21	1	0	0	R#334*,$\times 2$,AG(2,21)	
334	463	463	22	22	1	0		- $\times 1$,PG(2,21)	
335	232	232	22	22	2	0		- $\times 1$	
336	155	155	22	22	3	?		-	
337	78	78	22	22	6	≥ 3		- [2045]	II.6.47
338	67	67	22	22	7	0		- $\times 1$	
339	24	184	23	3	2	$\geq 3 \cdot 10^9$	≥ 1	D#404* [1040, 1548]	VI.16.81
340	24	138	23	4	3	≥ 1	≥ 1	D#405* [144, 1042]	VI.16.83
341	24	92	23	6	5	≥ 1	≥ 1	D#406* [848, 1042]	VI.16.86
342	70	230	23	7	2	≥ 1		? [2]	VI.16.88
343	24	69	23	8	7	≥ 1		? D#407 [1042]	VI.16.88
344	70	161	23	10	3	?		?	
345	231	483	23	11	1	?		?	
346	24	46	23	12	11	$\geq 10^{27}$	130	R#351,HD [1271, 1375, 1999]	
347	231	253	23	21	2	0	0	R#350*,$\times 2$	
348	484	506	23	22	1	0	0	R#349*,$\times 2$,AG(2,22)	
349	507	507	23	23	1	0		- $\times 1$,PG(2,22)	
350	254	254	23	23	2	0		- $\times 1$	
351	47	47	23	23	11	≥ 55		- [620]	VI.18.73
352	49	392	24	3	1	$\geq 6 \cdot 10^{14}$		- [1042, 1463]	VI.16.12
353	25	200	24	3	2	$\geq 10^{14}$		- 2#64,D#438*	
354	17	136	24	3	3	≥ 4968		- [1548]	VI.16.24
355	13	104	24	3	4	$\geq 10^8$		- 4#8 [1548]	
356	9	72	24	3	6	$\geq 10^7$	$\geq 10^5$	6#2 [1548]	
357	7	56	24	3	8	5413		- 8#1 [1743, 1938]	
358	73	438	24	4	1	$\geq 10^7$		- [332]	VI.16.61
359	37	222	24	4	2	≥ 4		- 2#68	
360	25	150	24	4	3	$\geq 10^{22}$		- 3#22,D#439* [1548]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
361	19	114	24	4	4	≥ 424		- 2#69	
362	13	78	24	4	6	$\geq 10^8$		- 6#3 [1548]	
363	10	60	24	4	8	≥ 1759614		- 4#10 [1545]	
364	9	54	24	4	9	$\geq 10^6$		- 3#24 [1548]	
365	25	120	24	5	4	$\geq 10^{17}$	$\geq 10^{17}$	4#11,D#440 [1548]	
366	121	484	24	6	1	≥ 1		- [1042, 1607]	VI.16.31
367	61	244	24	6	2	≥ 1		- 2#73*	VI.16.18
368	41	164	24	6	3	≥ 1		-	VI.16.18
369	31	124	24	6	4	$\geq 10^{22}$		- 4#12 [1548]	
370	25	100	24	6	5	≥ 1		- D#441 [1042]	
371	21	84	24	6	6	≥ 1		- 3#25*,2#75	
372	16	64	24	6	8	$\geq 10^8$		- 4#13 [1548]	
373	13	52	24	6	10	≥ 2572157		- 2#77	
374	49	168	24	7	3	$\geq 10^{52}$	$\geq 10^{52}$	3#26 [1548]	
375	169	507	24	8	1	?		-	
376	85	255	24	8	2	≥ 1		- [1628]	VI.16.30
377	57	171	24	8	3	$\geq 10^{63}$		- 3#27 [1548]	
378	43	129	24	8	4	≥ 1		- [2144]	VI.16.30
379	29	87	24	8	6	≥ 1		- 3#28* [1042]	VI.16.30
380	25	75	24	8	7	≥ 1		- D#442* [2144]	VI.16.31
381	22	66	24	8	8	≥ 1		- 2#78*	VI.16.30
382	33	88	24	9	6	≥ 3376		- 2#79	
383	55	132	24	10	4	?		- 2#80*	
384	25	60	24	10	9	≥ 3		- D#443 [607, 2144]	
385	121	264	24	11	2	≥ 365	≥ 365	2#81 [1225]	
386	265	530	24	12	1	?		-	
387	133	266	24	12	2	≥ 9979200		- 2#82 [1239]	
388	89	178	24	12	3	?		-	
389	67	134	24	12	4	≥ 1		- 2#83* [1]	VI.16.30
390	45	90	24	12	6	≥ 3753		- 2#84	
391	34	68	24	12	8	≥ 1		- 2#85* [1]	VI.16.30
392	25	50	24	12	11	≥ 10		- D#444 [607, 2144]	
393	105	180	24	14	3	?		-	
394	85	136	24	15	4	?		-	
395	46	69	24	16	8	≥ 1		- R#407 [1185]	
396	69	92	24	18	6	?		- R#406*	
397	115	138	24	20	4	?		- R#405*	
398	161	184	24	21	3	?		- R#404*	
399	49	56	24	21	10	≥ 1		- [2144]	VI.16.32
400	253	276	24	22	2	0		- R#403*,$\times 2$	
401	529	552	24	23	1	≥ 1	≥ 1	R#402,AG(2,23)	
402	553	553	24	24	1	≥ 1		- PG(2,23)	VI.18.73
403	277	277	24	24	2	0		- $\times 1$	
404	185	185	24	24	3	0		- $\times 1$	
405	139	139	24	24	4	?		-	
406	93	93	24	24	6	0		- $\times 1$	
407	70	70	24	24	8	≥ 28		- [1185, 620]	II.6.47
408	51	425	25	3	1	$\geq 6 \cdot 10^{53}$	≥ 9419	[1463, 1976]	VI.16.12
409	6	50	25	3	10	19	0	5#4 [1174, 1548]	
410	76	475	25	4	1	≥ 169574	≥ 1	[396, 587, 1047]	VI.16.14
411	16	100	25	4	5	$\geq 10^6$	$\geq 10^6$	5#5 [1548]	
412	101	505	25	5	1	≥ 3		- [393]	VI.16.62
413	51	255	25	5	2	≥ 1		- [1042]	VI.16.17
414	26	130	25	5	4	≥ 1		- D#471* [1042]	II.7.46
415	21	105	25	5	5	$\geq 10^9$		- 5#6 [1548]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
416	11	55	25	5	10	≥ 3337		- 5#7	
417	126	525	25	6	1	≥ 2	≥ 1	[679, 1042, 1578]	VI.16.92
418	176	550	25	8	1	?	?		
419	226	565	25	10	1	?		-	
420	76	190	25	10	3	?		-	
421	46	115	25	10	5	≥ 1		- [2071]	
422	26	65	25	10	9	≥ 19		- D#472 [1042, 1556]	
423	276	575	25	12	1	?		?	
424	26	50	25	13	12	≥ 1		0 R#444,×3 [1241, 1999]	
425	351	585	25	15	1	?		-	
426	51	85	25	15	7	?		-	
427	36	60	25	15	10	≥ 1		- R#443 [1042]	
428	51	75	25	17	8	?		0 R#442*,×3	
429	76	100	25	19	6	≥ 1		0 R#441,×3	
430	476	595	25	20	1	?		-	
431	96	120	25	20	5	≥ 1		- R#440	
432	126	150	25	21	4	?		0 R#439*,×3	
433	176	200	25	22	3	?		0 R#438*,×3	
434	276	300	25	23	2	?		0 R#437*,×3	
435	576	600	25	24	1	?		? R#436*,AG(2,24)	
436	601	601	25	25	1	?		- PG(2,24)	
437	301	301	25	25	2	?		-	
438	201	201	25	25	3	?		-	
439	151	151	25	25	4	0		- ×1	
440	121	121	25	25	5	≥ 1		- [1773]	II.6.47
441	101	101	25	25	6	≥ 1		-	VI.18.73
442	76	76	25	25	8	0		- ×1	
443	61	61	25	25	10	≥ 24		- [1720]	II.6.47
444	51	51	25	25	12	≥ 1		- [1999]	V.1.39
445	27	234	26	3	2	$\geq 10^{11}$	≥ 910	2#86,D#511*	
446	40	260	26	4	2	$\geq 10^{6}$	≥ 1	2#87	
447	14	91	26	4	6	≥ 4		- [1042, 1588]	II.5.29
448	105	546	26	5	1	≥ 1	≥ 1	[41]	IV.2.2
449	66	286	26	6	2	≥ 1	≥ 1	2#88 [958]	
450	27	117	26	6	5	≥ 1		- D#512* [1042]	VI.16.86
451	14	52	26	7	12	≥ 1363846	1363486	2#89 [1264]	
452	92	299	26	8	2	≥ 1		- [19]	
453	27	78	26	9	8	≥ 8072	≥ 13	2#90,D#513	
454	235	611	26	10	1	?		-	
455	40	104	26	10	6	≥ 1		? 2#91* [1]	
456	66	156	26	11	4	≥ 494		? 2#92 [1224]	
457	144	312	26	12	2	≥ 1		? 2#93* [528]	IV.2.67
458	313	626	26	13	1	?		-	
459	157	314	26	13	2	?		- 2#94*	
460	105	210	26	13	3	?		-	
461	79	158	26	13	4	≥ 940		- 2#95 [1224]	
462	53	106	26	13	6	≥ 1		- 2#96* [2144]	VI.16.30
463	40	80	26	13	8	≥ 390		- 2#97	
464	27	54	26	13	12	≥ 208311		- 2#98,D#514	
465	40	65	26	16	10	≥ 1		- R#472 [2067]	
466	105	130	26	21	5	?		0 R#471*,×3	
467	300	325	26	24	2	0		- R#470*,×2	
468	625	650	26	25	1	≥ 33	≥ 33	R#469,AG(2,25) [1251]	
469	651	651	26	26	1	≥ 17		- PG(2,25) [1251]	VI.18.73
470	326	326	26	26	2	0		- ×1	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
471	131	131	26	26	5	?		-	
472	66	66	26	26	10	≥ 588		- [2067, 1720]	II.6.47
473	55	495	27	3	1	$\geq 6 \cdot 10^{76}$		- [1463]	VI.16.12
474	28	252	27	3	2	$\geq 10^{55}$		- D#564* [1548]	VI.16.13
475	19	171	27	3	3	$\geq 10^{17}$		- 3#29 [1548]	
476	10	90	27	3	6	$\geq 10^{12}$		- 3#30 [1548]	
477	7	63	27	3	9	17785		- 9#1 [1743, 1938]	
478	28	189	27	4	3	$\geq 10^{32}$	$\geq 10^{26}$	3#32,D#565* [1548]	
479	55	297	27	5	2	≥ 1	≥ 1	[1042, 848]	IV.2.67
480	10	54	27	5	12	$\geq 10^{8}$	0	3#33 [1548]	
481	136	612	27	6	1	≥ 1		- [1610]	II.3.32
482	46	207	27	6	3	$\geq 10^{28}$		- 3#34* [1042, 416]	VI.16.90
483	28	126	27	6	5	≥ 2		- D#566* [2130]	VI.16.18
484	16	72	27	6	9	≥ 18921		- 3#35	
485	28	108	27	7	6	≥ 5047	≥ 1	3#36,D#567 [848, 1224]	VI.16.87
486	64	216	27	8	3	$\geq 10^{77}$	$\geq 10^{77}$	3#37 [1548]	
487	217	651	27	9	1	?		-	
488	109	327	27	9	2	≥ 1		- [1548]	VI.16.57
489	73	219	27	9	3	$\geq 10^{90}$		- 3#38 [1548]	
490	55	165	27	9	4	≥ 1		- [1]	VI.16.30
491	37	111	27	9	6	$\geq 10^{37}$		- 3#39 [1548]	
492	28	84	27	9	8	≥ 3		- D#568* [1548, 2130]	II.7.48
493	25	75	27	9	9	$\geq 10^{28}$		- 3#40 [1548]	
494	19	57	27	9	12	$\geq 10^{16}$		- 3#41 [1548]	
495	55	135	27	11	5	?		?	
496	100	225	27	12	3	?		-	
497	28	63	27	12	11	≥ 246		- D#569 [1236, 1379, 710]	
498	325	675	27	13	1	?		?	
499	28	54	27	14	13	$\geq 9 \cdot 10^{21}$	7570	R#514,HD [1271, 1319, 2039]	
500	190	342	27	15	2	?		-	
501	55	99	27	15	7	?		-	
502	460	690	27	18	1	?		-	
503	154	231	27	18	3	?		-	
504	52	78	27	18	9	≥ 2		- R#513 [957]	
505	91	117	27	21	6	?		- R#512*	
506	208	234	27	24	3	?		- R#511*	
507	325	351	27	25	2	?	0	R#510*,×3	
508	676	702	27	26	1	?	?	R#509*,AG(2,26)	
509	703	703	27	27	1	?		- PG(2,26)	
510	352	352	27	27	2	?		-	
511	235	235	27	27	3	0		- ×1	
512	118	118	27	27	6	0		- ×1	
513	79	79	27	27	9	≥ 1463		- [1087]	II.6.47
514	55	55	27	27	13	≥ 1		- [1999, 514]	V.1.28
515	57	532	28	3	1	$\geq 10^{90}$	≥ 1	[1042]	VI.16.12
516	15	140	28	3	4	$\geq 10^{15}$	$\geq 10^{11}$	4#14 [1548]	
517	9	84	28	3	7	≥ 330	≥ 9	7#2	
518	85	595	28	4	1	$\geq 10^{15}$		- [1042, 332]	VI.16.14
519	43	301	28	4	2	≥ 1		-	VI.16.15
520	29	203	28	4	3	≥ 1		- D#586*	II.7.46
521	22	154	28	4	4	≥ 7922		- 2#100	
522	15	105	28	4	6	≥ 31300		- [127]	VI.16.15
523	13	91	28	4	7	$\geq 10^{8}$		- 7#3 [1548]	
524	8	56	28	4	12	≥ 2310	31	4#15 [1174, 1548]	
525	15	84	28	5	8	≥ 104	≥ 1	4#16*,2#102 [1]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
526	141	658	28	6	1	≥ 1		- [1605]	
527	36	168	28	6	4	≥ 5	≥ 3	4#17*,2#103	
528	21	98	28	6	7	≥ 1		- #75+#153	
529	15	70	28	6	10	≥ 118		- 2#104	
530	169	676	28	7	1	≥ 1		- [1044, 1548]	VI.16.65
531	85	340	28	7	2	≥ 2		- 2#105* [1, 959]	VI.16.30
532	57	228	28	7	3	≥ 1		- [1042]	VI.16.30
533	43	172	28	7	4	≥ 4		- 4#18*,2#106	
534	29	116	28	7	6	≥ 1		- 2#107,D#587*	
535	25	100	28	7	7	≥ 1		- [2144]	VI.16.31
536	22	88	28	7	8	≥ 35		- 4#19*,2#108	
537	15	60	28	7	12	$\geq 10^8$		- 4#20 [1548]	
538	50	175	28	8	4	≥ 1		- [1]	VI.16.89
539	225	700	28	9	1	?		?	
540	85	238	28	10	3	?		-	
541	309	721	28	12	1	?		-	
542	78	182	28	12	4	?		- 2#110*	
543	45	105	28	12	7	≥ 1		- #84+#163	
544	169	364	28	13	2	≥ 765	≥ 765	2#111 [1225]	
545	365	730	28	14	1	?		-	
546	183	366	28	14	2	$\geq 10^9$		- 2#112 [1239]	
547	92	184	28	14	4	?		- 2#113*	
548	53	106	28	14	7	≥ 1		- [2144]	VI.16.30
549	29	58	28	14	13	≥ 1		- D#588 [2144]	
550	36	63	28	16	12	≥ 8784		- R#569 [1236, 710]	
551	477	742	28	18	1	?		-	
552	57	84	28	19	9	?	0	R#568*,×3	
553	561	748	28	21	1	?		-	
554	141	188	28	21	4	?		-	
555	81	108	28	21	7	≥ 1		- R#567	
556	57	76	28	21	10	?		-	
557	99	126	28	22	6	?		- R#566*	
558	162	189	28	24	4	?		- R#565*	
559	225	252	28	25	3	?	0	R#564*,×3	
560	351	378	28	26	2	0		- R#563*,×2	
561	729	756	28	27	1	≥ 7	≥ 7	R#562,AG(2,27) [1251]	
562	757	757	28	28	1	≥ 3		- PG(2,27) [679]	VI.18.73
563	379	379	28	28	2	0		- ×1	
564	253	253	28	28	3	?		-	
565	190	190	28	28	4	0		- ×1	
566	127	127	28	28	6	?		-	
567	109	109	28	28	7	≥ 1		-	VI.18.73
568	85	85	28	28	9	?		-	
569	64	64	28	28	12	≥ 8784		- [710]	VI.18.73
570	30	290	29	3	2	$\geq 2 \cdot 10^{51}$	≥ 1	D#655* [1040, 1548]	VI.16.81
571	88	638	29	4	1	≥ 2	≥ 1	[1042, 332, 1047]	IV.2.2
572	30	174	29	5	4	≥ 1	≥ 4	D#656 [1042, 623]	VI.16.85
573	30	145	29	6	5	≥ 1	≥ 1	D#657* [1042, 33]	VI.16.86
574	175	725	29	7	1	≥ 1		? [1184]	VI.16.31
575	117	377	29	9	2	≥ 1		? [1034]	VI.16.70
576	30	87	29	10	9	≥ 1		? D#658* [1]	VI.16.88
577	117	261	29	13	3	?		?	
578	378	783	29	14	1	?		?	
579	30	58	29	15	14	≥ 1	0	R#588,×3 [1241, 2144]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
580	88	116	29	22	7	?	0	R#587*,×3	
581	175	203	29	25	4	?	0	R#586*,×3	
582	378	406	29	27	2	?	0	R#585*,×3	
583	784	812	29	28	1	?	?	R#584*,AG(2,28)	
584	813	813	29	29	1	?	-	PG(2,28)	
585	407	407	29	29	2	?	-		
586	204	204	29	29	4	?	-		
587	117	117	29	29	7	0	-	×1	
588	59	59	29	29	14	≥ 1	-		VI.18.73
589	61	610	30	3	1	$\geq 2 \cdot 10^{24}$	-	[1042, 1463]	VI.16.12
590	31	310	30	3	2	$\geq 6 \cdot 10^{16}$	-	2#114,D#677*	
591	21	210	30	3	3	$\geq 10^{24}$	$\geq 10^{21}$	3#42 [1548]	
592	16	160	30	3	4	$\geq 10^{13}$	-	2#115	
593	13	130	30	3	5	$\geq 10^{8}$	-	5#8 [1548]	
594	11	110	30	3	6	≥ 436801	-	2#116	
595	7	70	30	3	10	54613	-	10#1 [1545]	
596	6	60	30	3	12	34	1	6#4,3#43 [1174, 1548]	
597	46	345	30	4	2	≥ 1	-	[1042]	VI.16.15
598	16	120	30	4	6	$\geq 10^{15}$	$\geq 10^{15}$	6#5 [1548]	
599	10	75	30	4	10	≥ 29638	-	5#10 [1548]	
600	121	726	30	5	1	≥ 1	-	[1042]	VI.16.62
601	61	366	30	5	2	≥ 11	-	2#120	
602	41	246	30	5	3	$\geq 10^{46}$	-	3#45	
603	31	186	30	5	4	≥ 1	-	2#121,D#678*	
604	25	150	30	5	5	$\geq 10^{17}$	$\geq 10^{17}$	5#11 [1548]	
605	21	126	30	5	6	$\geq 10^{24}$	-	6#6 [1548]	
606	16	96	30	5	8	≥ 12	-	2#123	
607	13	78	30	5	10	≥ 31	-	2#124	
608	11	66	30	5	12	$\geq 10^{6}$	-	6#7 [1548]	
609	151	755	30	6	1	≥ 1	-	[1042, 2144]	VI.16.54
610	76	380	30	6	2	≥ 1	-	2#126	
611	51	255	30	6	3	≥ 1	-	3#48* [1042]	VI.16.18
612	31	155	30	6	5	$\geq 10^{23}$	-	5#12,D#679 [1548]	
613	26	130	30	6	6	≥ 1	-	2#127	
614	16	80	30	6	10	$\geq 10^{8}$	-	5#13 [1548]	
615	91	390	30	7	2	≥ 3	?	2#129	
616	21	90	30	7	9	$\geq 10^{18}$	≥ 1	3#49 [1]	
617	36	135	30	8	6	≥ 3	-	3#50* [1, 1497, 2130]	
618	16	60	30	8	14	$\geq 9 \cdot 10^{7}$	≥ 6	2#130	
619	81	270	30	9	3	$\geq 10^{108}$	$\geq 10^{108}$	3#51 [1548]	
620	21	70	30	9	12	$\geq 10^{4}$	-	2#131	
621	271	813	30	10	1	?	-		
622	136	408	30	10	2	?	-	2#132*	
623	91	273	30	10	3	$\geq 10^{125}$	-	3#52 [1548]	
624	55	165	30	10	5	≥ 2	-	[1034]	VI.16.30
625	46	138	30	10	6	≥ 1	-	2#133*,3#53* [1]	
626	31	93	30	10	9	≥ 152	-	3#54,D#680*	
627	28	84	30	10	10	≥ 5	-	2#134* [1548, 2130]	II.7.48
628	166	415	30	12	2	?	-		
629	56	140	30	12	6	≥ 5	-	2#135	
630	34	85	30	12	10	≥ 1	-	[1628]	VI.16.30
631	91	210	30	13	4	?	?	2#136*	
632	196	420	30	14	2	?	?	2#137*	
633	421	842	30	15	1	?	-		
634	211	422	30	15	2	?	-	2#138*	
635	141	282	30	15	3	?	-		

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
636	106	212	30	15	4	?		- 2#139*	
637	85	170	30	15	5	?		-	
638	71	142	30	15	6	≥ 9		- 2#140	
639	61	122	30	15	7	≥ 1		- [2144]	VI.16.30
640	43	86	30	15	10	≥ 1		- 2#141* [1042]	VI.16.30
641	36	72	30	15	12	≥ 25635		- 2#142	
642	31	62	30	15	14	$\geq 10^6$		- 2#143,D#681	
643	171	285	30	18	3	?		-	
644	286	429	30	20	2	?		-	
645	96	144	30	20	6	?		-	
646	58	87	30	20	10	?		- R#658*	
647	301	430	30	21	2	?		-	
648	116	145	30	24	6	?		- R#657*	
649	145	174	30	25	5	≥ 1		- R#656 [1839]	
650	261	290	30	27	3	?		- R#655*	
651	406	435	30	28	2	0		- R#654*,×2	
652	841	870	30	29	1	≥ 1	≥ 1	R#653,AG(2,29)	
653	871	871	30	30	1	≥ 1		- PG(2,29)	VI.18.73
654	436	436	30	30	2	0		- ×1	
655	291	291	30	30	3	?		-	
656	175	175	30	30	5	≥ 2		- [331, 1839]	VI.18.73
657	146	146	30	30	6	0		- ×1	
658	88	88	30	30	10	0		- ×1	
659	63	651	31	3	1	$\geq 10^{42}$	≥ 82160	PG(5,2) [1463, 1548]	VI.16.12
660	32	248	31	4	3	≥ 1	≥ 1	D#729* [1042, 144]	VI.16.83
661	125	775	31	5	1	$\geq 1.9 \cdot 10^{97}$	$\geq 5.2 \cdot 10^{109}$	AG(3,5) [1546]	IV.2.2
662	156	806	31	6	1	$\geq 1.6 \cdot 10^{116}$	≥ 1	PG(3,5) [1546]	IV.2.2
663	63	279	31	7	3	≥ 1	≥ 1	[1042, 1]	VI.16.87
664	32	124	31	8	7	≥ 1	≥ 1	D#730* [1042, 1714]	VI.16.87
665	63	217	31	9	4	≥ 1	≥ 1	[1]	VI.16.87
666	280	868	31	10	1	?	?		
667	435	899	31	15	1	?	?		
668	32	62	31	16	15	$\geq 10^{28}$	≥ 1	R#681,$AG_4(5,2)$,HD [1319]	
669	63	93	31	21	10	$\geq 10^{17}$	0	R#680* [1900, 2058]	
670	125	155	31	25	6	$\geq 10^{12}$	$\geq 10^{12}$	R#679,$AG_2(3,5)$ [1223]	
671	156	186	31	26	5	?	0	R#678*,×3	
672	280	310	31	28	3	?	0	R#677*,×3	
673	435	465	31	29	2	0	0	R#676*,×2	
674	900	930	31	30	1	0	0	R#675*,×2,AG(2,30)	
675	931	931	31	31	1	0		- ×1,PG(2,30)	
676	466	466	31	31	2	0		- ×1	
677	311	311	31	31	3	?		-	
678	187	187	31	31	5	0		- ×1	
679	156	156	31	31	6	$\geq 10^{17}$		- $PG_2(3,5)$ [1223]	VI.18.73
680	94	94	31	31	10	0		- ×1	
681	63	63	31	31	15	$\geq 10^{17}$		- $PG_4(5,2)$ [1223]	VI.18.73
682	33	352	32	3	2	$\geq 10^{13}$	$\geq 4.4 \cdot 10^6$	2#144,D#775* [562]	
683	9	96	32	3	8	$\geq 10^7$	$\geq 10^5$	8#2 [1548]	
684	97	776	32	4	1	≥ 5985		- [332, 396]	VI.16.61
685	49	392	32	4	2	≥ 770		- 2#146 [396]	
686	33	264	32	4	3	≥ 1		- D#776* [1042]	II.7.46
687	25	200	32	4	4	$\geq 10^{22}$		- 4#22 [1548]	
688	17	136	32	4	6	≥ 1		- 2#148	
689	13	104	32	4	8	$\geq 10^8$		- 8#3 [1548]	
690	9	72	32	4	12	$\geq 10^8$		- 4#24 [1548]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
691	65	416	32	5	2	≥ 3	≥ 1	2#151	
692	81	432	32	6	2	≥ 1		- 2#152* [1042]	IV.2.7
693	33	176	32	6	5	≥ 1		- D#777* [1042]	VI.16.18
694	21	112	32	6	8	≥ 1		- 4#25*,2#153	
695	49	224	32	7	4	$\geq 10^{52}$	$\geq 10^{52}$	4#26 [1548]	
696	225	900	32	8	1	?		-	
697	113	452	32	8	2	≥ 1		- 2#155* [957]	VI.16.64
698	57	228	32	8	4	$\geq 10^{63}$		- 4#27 [1548]	
699	33	132	32	8	7	≥ 1		- D#778 [1042]	II.7.46
700	29	116	32	8	8	≥ 3		- 4#28*,2#157	
701	17	68	32	8	14	≥ 12		- 2#158	
702	145	464	32	10	2	?		- 2#159*	
703	25	80	32	10	12	≥ 44		- 2#160	
704	33	96	32	11	10	≥ 20		? 2#161,D#779*	
705	177	472	32	12	2	?		- 2#162*	
706	45	120	32	12	8	≥ 1		- 2#163	
707	33	88	32	12	11	≥ 1		- D#780* [1042]	
708	65	160	32	13	6	?		? 2#164*	
709	105	240	32	14	4	?		- 2#165*	
710	225	480	32	15	2	?		? 2#166*	
711	481	962	32	16	1	?		-	
712	241	482	32	16	2	?		- 2#167*	
713	161	322	32	16	3	?		-	
714	121	242	32	16	4	≥ 1		- 2#168* [1]	VI.16.31
715	97	194	32	16	5	?		-	
716	81	162	32	16	6	?		- 2#169*	
717	61	122	32	16	8	≥ 1		- 2#170	
718	49	98	32	16	10	≥ 45		- 2#171	
719	41	82	32	16	12	≥ 115308		- 2#172	
720	33	66	32	16	15	≥ 1		- D#781 [2110]	
721	305	488	32	20	2	?		-	
722	369	492	32	24	2	?		-	
723	93	124	32	24	8	?		- R#730*	
724	217	248	32	28	4	?		- R#729*	
725	465	496	32	30	2	0		- R#728*,×2	
726	961	992	32	31	1	≥ 1	≥ 1	R#727,AG(2,31)	
727	993	993	32	32	1	≥ 1		- PG(2,31)	VI.18.82
728	497	497	32	32	2	0		- ×1	
729	249	249	32	32	4	?		-	
730	125	125	32	32	8	0		- ×1	
731	67	737	33	3	1	$\geq 10^{35}$		- [1042, 1463]	VI.16.12
732	34	374	33	3	2	$\geq 10^{41}$		- D#811* [1548]	VI.16.81
733	23	253	33	3	3	$\geq 2 \cdot 10^{14}$		- [1548]	VI.16.24
734	12	132	33	3	6	$\geq 10^{8}$	≥ 1	3#55 [1548]	
735	7	77	33	3	11	155118		- 11#1 [1545]	
736	100	825	33	4	1	≥ 5985	≥ 1	[332, 396, 1047]	IV.2.2
737	12	99	33	4	9	$\geq 10^{10}$	≥ 1	3#56	
738	45	297	33	5	3	$\geq 10^{54}$	≥ 1	3#57 [2, 1548]	
739	166	913	33	6	1	?		-	
740	56	308	33	6	3	≥ 1		- [1042]	IV.2.7
741	34	187	33	6	5	≥ 1		- D#812* [1042]	VI.16.86
742	16	88	33	6	11	≥ 1		- #13+#484	
743	12	66	33	6	15	≥ 11604	≥ 12	3#58	
744	232	957	33	8	1	≥ 1	≥ 1	[688]	
745	45	165	33	9	6	≥ 35805		? 3#59 [1224]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
746	100	330	33	10	3	≥ 1	?	3#60* [528]	IV.2.67
747	331	993	33	11	1	?		-	
748	166	498	33	11	2	?		-	
749	111	333	33	11	3	≥ 1		- 3#61* [528]	IV.2.67
750	67	201	33	11	5	≥ 1		- [2144]	VI.16.30
751	56	168	33	11	6	$\geq 10^{71}$		- 3#62 [1548]	
752	34	102	33	11	10	≥ 1		- D#813* [1042]	VI.16.88
753	31	93	33	11	11	≥ 1		- [1042]	II.7.46
754	23	69	33	11	15	≥ 1103		- 3#63	
755	364	1001	33	12	1	?		-	
756	155	341	33	15	3	?		-	
757	496	1023	33	16	1	≥ 1	≥ 1	[1877]	
758	34	66	33	17	16	≥ 1	0	R#781,×3 [1241, 2110]	
759	133	209	33	21	5	?		-	
760	56	88	33	21	12	?		- R#780*	
761	694	1041	33	22	1	?		-	
762	232	348	33	22	3	?		-	
763	100	150	33	22	7	?		-	
764	78	117	33	22	9	?		-	
765	64	96	33	22	11	?		- R#779*	
766	760	1045	33	24	1	?		-	
767	100	132	33	25	8	≥ 1	0	R#778,×3 [1241, 1013]	
768	144	176	33	27	6	?		- R#777*	
769	232	264	33	29	4	?	0	R#776*,×3	
770	320	352	33	30	3	?		- R#775*	
771	496	528	33	31	2	?	0	R#774*,×3	
772	1024	1056	33	32	1	≥ 11	≥ 11	R#773,AG(2,32) [679]	
773	1057	1057	33	33	1	≥ 6		- PG(2,32) [679]	VI.18.28
774	529	529	33	33	2	?		-	
775	353	353	33	33	3	0		- ×1	
776	265	265	33	33	4	?		-	
777	177	177	33	33	6	?		-	
778	133	133	33	33	8	≥ 1		- [1013]	VI.18.73
779	97	97	33	33	11	?		-	
780	89	89	33	33	12	0		- ×1	
781	67	67	33	33	16	≥ 1		- [2110]	VI.18.73
782	69	782	34	3	1	$\geq 4 \cdot 10^{41}$	≥ 1	[1042, 1047, 1463]	VI.16.12
783	18	204	34	3	4	$\geq 4 \cdot 10^{14}$	≥ 1	2#173	
784	52	442	34	4	2	≥ 207	≥ 1	2#174	
785	18	153	34	4	6	≥ 1		- [1042]	VI.16.84
786	35	238	34	5	4	≥ 2	≥ 2	2#175,D#869*	
787	171	969	34	6	1	≥ 1		- [46]	II.3.32
788	18	102	34	6	10	≥ 4	≥ 3	2#176	
789	35	170	34	7	6	≥ 3	≥ 1	2#177,D#870* [43]	VI.16.87
790	120	510	34	8	2	≥ 1	≥ 1	2#178	
791	18	68	34	9	16	$\geq 10^3$	≥ 1	2#179	
792	35	119	34	10	9	≥ 1		- D#871* [1042]	
793	341	1054	34	11	1	?	?		
794	52	136	34	13	8	≥ 1	?	2#180	
795	35	85	34	14	13	≥ 1		- D#872* [1]	
796	120	272	34	15	4	?	?	2#181*	
797	256	544	34	16	2	$\geq_{477603}$	$\geq_{477603}$	2#182 [1225]	
798	545	1090	34	17	1	?		-	
799	273	546	34	17	2	$\geq 10^{12}$		- 2#183 [1239]	
800	137	274	34	17	4	≥ 1		- 2#184* [382]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
801	69	138	34	17	8	≥ 1		- 2#185	
802	35	70	34	17	16	≥ 1854		- 2#186,D#873	
803	715	1105	34	22	1	?		-	
804	69	102	34	23	11	?	0	R#813*,×3	
805	154	187	34	28	6	?		- R#812*	
806	341	374	34	31	3	?	0	R#811*,×3	
807	528	561	34	32	2	0		- R#810*,×2	
808	1089	1122	34	33	1	0	0	R#809*,×2,AG(2,33)	
809	1123	1123	34	34	1	0		- ×1	
810	562	562	34	34	2	0		- ×1	
811	375	375	34	34	3	?		-	
812	188	188	34	34	6	0		- ×1	
813	103	103	34	34	11	?		-	
814	36	420	35	3	2	$\geq 2 \cdot 10^{50}$	≥ 1	D#961* [1040, 1548]	VI.16.81
815	15	175	35	3	5	$\geq 10^{15}$	$\geq 10^{11}$	5#14 [1548]	
816	6	70	35	3	14	48	0	7#4 [1174, 1548]	
817	36	315	35	4	3	≥ 1	≥ 1	D#962* [1042, 144]	VI.16.83
818	16	140	35	4	7	$\geq 10^{15}$	$\geq 10^{15}$	7#5 [1548]	
819	8	70	35	4	15	≥ 2224	82	5#15 [697, 1271]	
820	141	987	35	5	1	≥ 1		- [1042]	VI.16.16
821	71	497	35	5	2	≥ 1		- [1042]	VI.16.17
822	36	252	35	5	4	≥ 2		- D#963* [1042, 2130]	VI.16.85
823	29	203	35	5	5	≥ 2		- [1042, 380]	II.7.46
824	21	147	35	5	7	$\geq 10^{24}$		- 7#6 [1548]	
825	15	105	35	5	10	≥ 1	≥ 1	5#16*,#102+#280 [1]	
826	11	77	35	5	14	$\geq 10^{6}$		- 7#7 [1548]	
827	36	210	35	6	5	≥ 1	≥ 1	#103+#282,D#964* [1042, 144]	
828	211	1055	35	7	1	?		-	
829	106	530	35	7	2	≥ 1		- [4]	
830	71	355	35	7	3	≥ 1		- [2144]	VI.16.30
831	43	215	35	7	5	≥ 1		- 5#18*,#106+#287	
832	36	180	35	7	6	≥ 1		- D#965* [1042]	II.7.46
833	31	155	35	7	7	≥ 5		- $PG_2(4,2)$ [2043]	II.7.46
834	22	110	35	7	10	≥ 1		- 5#19*,#108+#288	
835	16	80	35	7	14	≥ 1		- #131↓#259	
836	15	75	35	7	15	$\geq 10^{9}$		- 5#20 [1548]	
837	36	140	35	9	8	≥ 4	≥ 6	D#966* [1042, 1629]	VI.16.87
838	316	1106	35	10	1	?		-	
839	106	371	35	10	3	?		-	
840	64	224	35	10	5	≥ 1		- [22]	II.3.32
841	46	161	35	10	7	?		-	
842	36	126	35	10	9	≥ 2		- D#967* [1042, 2130]	
843	22	77	35	10	15	≥ 1		- #104↓#290	
844	176	560	35	11	2	?		?	
845	36	105	35	12	11	≥ 1	≥ 1	D#968* [1042, 1566]	VI.16.88
846	456	1140	35	14	1	?		-	
847	92	230	35	14	5	?		-	
848	66	165	35	14	7	?		-	
849	36	90	35	14	13	≥ 1		- D#969* [1042]	
850	246	574	35	15	2	?		-	
851	99	231	35	15	5	?		-	
852	36	84	35	15	14	≥ 1		- D#970*, #142+#264	
853	176	385	35	16	3	?		?	
854	561	1155	35	17	1	?		?	
855	36	70	35	18	17	≥ 91	≥ 91	R#873,HD [404, 2110]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
856	96	168	35	20	7	?		-	
857	351	585	35	21	2	?		-	
858	141	235	35	21	5	?		-	
859	51	85	35	21	14	?		- R#872*	
860	85	119	35	25	10	?		- R#871*	
861	316	395	35	28	3	?		-	
862	136	170	35	28	7	?		- R#870*	
863	64	80	35	28	15	?		-	
864	204	238	35	30	5	?		- R#869*	
865	561	595	35	33	2	0		0 R#868*,×2	
866	1156	1190	35	34	1	?		? R#867*,AG(2,34)	
867	1191	1191	35	35	1	?		- PG(2,34)	
868	596	596	35	35	2	0		- ×1	
869	239	239	35	35	5	?		-	
870	171	171	35	35	7	?		-	
871	120	120	35	35	10	?		-	
872	86	86	35	35	14	0		- ×1	
873	71	71	35	35	17	≥ 9		- [2110, 619]	VI.18.73
874	73	876	36	3	1	$\geq 10^{34}$		- [1042, 1463]	VI.16.12
875	37	444	36	3	2	$\geq 10^{10}$		- 2#187,D#991*	
876	25	300	36	3	3	$\geq 10^{25}$		- 3#64 [1548]	
877	19	228	36	3	4	$\geq 10^{17}$		- 4#29 [1548]	
878	13	156	36	3	6	$\geq 10^{17}$		- 6#8 [1548]	
879	10	120	36	3	8	$\geq 10^{12}$		- 4#30 [1548]	
880	9	108	36	3	9	$\geq 10^{14}$	$\geq 10^{5}$	9#2 [1707]	
881	7	84	36	3	12	412991		- 12#1 [1545]	
882	109	981	36	4	1	$\geq 1.6 \cdot 10^{13}$		- [396]	VI.16.61
883	55	495	36	4	2	≥ 1		- [1042]	IV.2.7
884	37	333	36	4	3	$\geq 10^{40}$		- 3#68,D#992* [1548]	
885	28	252	36	4	4	$\geq 10^{32}$	$\geq 10^{26}$	4#32 [1548]	
886	19	171	36	4	6	$\geq 10^{20}$		- 3#69	
887	13	117	36	4	9	$\geq 10^{8}$		- 9#3 [1548]	
888	10	90	36	4	12	$\geq 10^{9}$		- 6#10 [1548]	
889	145	1044	36	5	1	≥ 1	≥ 1	[1042, 41]	VI.16.70
890	25	180	36	5	6	$\geq 10^{38}$	$\geq 10^{38}$	6#11 [1548]	
891	10	72	36	5	16	$\geq 10^{8}$	27121734	4#33,2#195 [1548, 1633]	
892	181	1086	36	6	1	≥ 1		- [1042, 2144]	VI.16.54
893	91	546	36	6	2	≥ 5		- 2#196	
894	61	366	36	6	3	≥ 1		- 3#73* [1042]	VI.16.18
895	46	276	36	6	4	≥ 1		- 4#34*,2#197	
896	37	222	36	6	5	≥ 2		- D#993 [1042]	
897	31	186	36	6	6	$\geq 10^{51}$		- 6#12 [1548]	
898	21	126	36	6	9	≥ 1		- 3#75	
899	19	114	36	6	10	≥ 1		- 2#199	
900	16	96	36	6	12	$\geq 10^{19}$		- 6#13 [1548]	
901	13	78	36	6	15	$\geq 10^{11}$		- 3#77 [1548]	
902	217	1116	36	7	1	≥ 1		? [1537]	VI.16.30
903	28	144	36	7	8	≥ 5432	≥ 1	4#36 [1, 1224]	
904	64	288	36	8	4	$\geq 10^{77}$	$\geq 10^{77}$	4#37 [1548]	
905	22	99	36	8	12	≥ 1		- 3#78* [1042]	VI.16.30
906	289	1156	36	9	1	?		-	
907	145	580	36	9	2	≥ 1		- 2#203* [959]	
908	97	388	36	9	3	≥ 1		- [1]	VI.16.30
909	73	292	36	9	4	$\geq 10^{90}$		- 4#38 [1548]	
910	49	196	36	9	6	≥ 5		- 2#205* [1151]	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
911	37	148	36	9	8	$\geq 10^{37}$		- 4#39,D#994* [1548]	
912	33	132	36	9	9	$\geq 10^{39}$		- 3#79	II.7.46
913	25	100	36	9	12	$\geq 10^{28}$		- 4#40 [1548]	
914	19	76	36	9	16	$\geq 10^{16}$		- 4#41 [1548]	
915	325	1170	36	10	1	?		-	
916	55	198	36	10	6	?		- 3#80*,2#209*	
917	121	396	36	11	3	$\geq 10^{188}$	$\geq 10^{188}$	3#81 [1548]	
918	397	1191	36	12	1	?		-	
919	199	597	36	12	2	?		-	
920	133	399	36	12	3	$\geq 10^{208}$		- 3#82 [1548]	
921	100	300	36	12	4	?		- 2#210*	
922	67	201	36	12	6	≥ 1		- 3#83* [2144]	VI.16.30
923	45	135	36	12	9	$\geq 10^{57}$		- 3#84	
924	37	111	36	12	11	≥ 1		- D#995* [1042]	II.7.46
925	34	102	36	12	12	≥ 2		- 3#85*,2#211	VI.16.88
926	469	1206	36	14	1	?		-	
927	505	1212	36	15	1	?		-	
928	85	204	36	15	6	?		- 2#212*	
929	136	306	36	16	4	?		- 2#213*	
930	289	612	36	17	2	≥ 3481	≥ 3481	2#214 [1225]	
931	613	1226	36	18	1	?		-	
932	307	614	36	18	2	$\geq 8 \cdot 10^{13}$		- 2#215 [1239]	
933	205	410	36	18	3	?		-	
934	154	308	36	18	4	?		- 2#216*	
935	103	206	36	18	6	?		- 2#217*	
936	69	138	36	18	9	?		-	
937	52	104	36	18	12	?		- 2#218*	
938	37	74	36	18	17	≥ 1		- D#996 [1042]	
939	685	1233	36	20	1	?		-	
940	115	207	36	20	6	?		-	
941	721	1236	36	21	1	?		-	
942	91	156	36	21	8	?		-	
943	49	84	36	21	15	?		- R#970*	
944	253	414	36	22	3	?		-	
945	55	90	36	22	14	?		- R#969*	
946	208	312	36	24	4	?		-	
947	70	105	36	24	12	?		- R#968*	
948	91	126	36	26	10	?		- R#967*	
949	105	140	36	27	9	?		- R#966*	
950	973	1251	36	28	1	?		-	
951	145	180	36	29	7	?	0	R#965*,×3	
952	1045	1254	36	30	1	?		-	
953	175	210	36	30	6	?		- R#964*	
954	217	252	36	31	5	?	0	R#963*,×3	
955	280	315	36	32	4	?		- R#962*	
956	385	420	36	33	3	?		- R#961*	
957	595	630	36	34	2	?		- R#960*	
958	1225	1260	36	35	1	?	?	R#959*,AG(2,35)	
959	1261	1261	36	36	1	?		- PG(2,35)	
960	631	631	36	36	2	?		-	
961	421	421	36	36	3	?		-	
962	316	316	36	36	4	0		- ×1	
963	253	253	36	36	5	?		-	
964	211	211	36	36	6	0		- ×1	
965	181	181	36	36	7	?		-	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
966	141	141	36	36	9	?	-		
967	127	127	36	36	10	?	-		
968	106	106	36	36	12	0	-	$\times 1$	
969	91	91	36	36	14	0	-	$\times 1$	
970	85	85	36	36	15	?	-		
971	75	925	37	3	1	$\geq 10^{196}$	≥ 1	[1013, 1042, 1174]	VI.16.12
972	112	1036	37	4	1	$\geq 1.69 \cdot 10^{13}$	≥ 210	[1042, 396]	IV.2.2
973	75	555	37	5	2	≥ 1	≥ 1	[1042, 41]	VI.16.31
974	186	1147	37	6	1	≥ 1	≥ 1	[1042, 958]	IV.2.2
975	112	592	37	7	2	≥ 1	?	[1042]	
976	297	1221	37	9	1	?	?		
977	408	1258	37	12	1	?	?		
978	75	185	37	15	7	≥ 1	≥ 1	[1714]	
979	112	259	37	16	5	?	?		
980	630	1295	37	18	1	?	?		
981	38	74	37	19	18	≥ 1	0	R#996,$\times 3$ [1241, 2110]	
982	75	111	37	25	12	?	0	R#995*,$\times 3$	
983	112	148	37	28	9	?	?	R#994*	
984	186	222	37	31	6	≥ 1	0	R#993,$\times 3$ [1241, 1773]	
985	297	333	37	33	4	?	0	R#992*,$\times 3$	
986	408	444	37	34	3	?	0	R#991*,$\times 3$	
987	630	666	37	35	2	0	0	R#990*,$\times 2$	
988	1296	1332	37	36	1	?	?	R#989*,AG(2,36)	
989	1333	1333	37	37	1	?	-	PG(2,36)	
990	667	667	37	37	2	0	-	$\times 1$	
991	445	445	37	37	3	0	-	$\times 1$	
992	334	334	37	37	4	0	-	$\times 1$	
993	223	223	37	37	6	≥ 1	-	[1773]	
994	149	149	37	37	9	?	-		
995	112	112	37	37	12	?	-		
996	75	75	37	37	18	≥ 1	-	[1839]	V.1.39
997	39	494	38	3	2	$\geq 10^{44}$	≥ 89	2#219,D#1071*	
998	58	551	38	4	2	≥ 1	-	[1042]	IV.2.7
999	20	190	38	4	6	≥ 1	≥ 4	2#220	
1000	20	152	38	5	8	≥ 1	≥ 3	2#221	
1001	96	608	38	6	2	≥ 1	≥ 1	2#222 [958]	
1002	39	247	38	6	5	≥ 1	-	D#1072* [1042]	VI.16.18
1003	77	418	38	7	3	≥ 2	?	[1042, 1]	VI.16.70
1004	20	95	38	8	14	≥ 1	-	[1042]	VI.16.88
1005	153	646	38	9	2	≥ 1	?	2#223* [958, 1548]	VI.16.31
1006	115	437	38	10	3	?	-		
1007	20	76	38	10	18	$\geq 10^{16}$	≥ 4	2#224	
1008	77	266	38	11	5	?	?		
1009	210	665	38	12	2	?	-		
1010	39	114	38	13	12	≥ 1	?	2#225*,D#1073* [1042]	VI.16.88
1011	96	228	38	16	6	?	?	2#226*	
1012	153	342	38	17	4	?	?	2#227*	
1013	324	684	38	18	2	≥ 1	?	2#228* [528]	IV.2.67
1014	685	1370	38	19	1	?	-		
1015	343	686	38	19	2	?	-	2#229*	
1016	229	458	38	19	3	?	-		
1017	172	344	38	19	4	?	-	2#230*	
1018	115	230	38	19	6	?	-	2#231*	
1019	77	154	38	19	9	?	-		
1020	58	116	38	19	12	?	-	2#232*	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
1021	39	78	38	19	18	$\geq 5.87 \cdot 10^{14}$	-	2#233,D#1074 [1374]	
1022	666	703	38	36	2	?	-	R#1025*	
1023	1369	1406	38	37	1	≥ 1	≥ 1	R#1024,AG(2,37)	
1024	1407	1407	38	38	1	≥ 1	-	PG(2,37)	VI.18.82
1025	704	704	38	38	2	?	-		
1026	79	1027	39	3	1	$\geq 10^{56}$	-	[1463]	VI.16.12
1027	40	520	39	3	2	$\geq 6 \cdot 10^{24}$	-	D#1163* [1548]	VI.16.13
1028	27	351	39	3	3	$\geq 10^{28}$	$\geq 10^{30}$	3#86 [1548]	
1029	14	182	39	3	6	$\geq 2 \cdot 10^{34}$	-	[1548]	VI.16.82
1030	7	91	39	3	13	1033129	-	13#1 [696]	
1031	40	390	39	4	3	$\geq 10^{33}$	$\geq 10^{33}$	3#87,D#1164* [1548]	
1032	40	312	39	5	4	≥ 1	≥ 1	D#1165* [1, 1042]	VI.16.85
1033	196	1274	39	6	1	≥ 1	-	[18]	II.3.32
1034	66	429	39	6	3	≥ 1	≥ 1	3#88 [1833]	
1035	40	260	39	6	5	≥ 1	-	D#1166* [1042]	VI.16.86
1036	16	104	39	6	13	≥ 1	-	#13+#742	
1037	14	91	39	6	15	≥ 1	-	[1042]	VI.16.86
1038	14	78	39	7	18	$\geq 10^{11}$	0	3#89 [1548]	
1039	40	195	39	8	7	≥ 1	≥ 1	D#1167* [1, 1042]	VI.16.87
1040	105	455	39	9	3	≥ 1	-	[21]	II.3.32
1041	27	117	39	9	12	$\geq 10^{17}$	$\geq 10^{17}$	3#90 [1548]	
1042	40	156	39	10	9	≥ 1	≥ 3	3#91*,D#1168* [1042, 1629]	VI.16.87
1043	66	234	39	11	6	≥ 21584	?	3#92 [1224]	
1044	144	468	39	12	3	≥ 1	?	3#93* [528]	IV.2.67
1045	40	130	39	12	11	≥ 1	-	D#1169* [1042]	VI.16.88
1046	469	1407	39	13	1	?	-		
1047	235	705	39	13	2	?	-		
1048	157	471	39	13	3	≥ 1	-	3#94* [528]	IV.2.67
1049	118	354	39	13	4	?	-		
1050	79	237	39	13	6	$\geq 10^{125}$	-	3#95 [1548]	
1051	53	159	39	13	9	≥ 1	-	3#96* [1]	
1052	40	120	39	13	12	$\geq 10^{33}$	-	3#97,D#1170 [1548]	
1053	37	111	39	13	13	≥ 1	-	[1042]	II.7.46
1054	27	81	39	13	18	≥ 208311	-	3#98	
1055	40	104	39	15	14	≥ 1	-	D#1171* [1042]	
1056	222	481	39	18	3	?	-		
1057	703	1443	39	19	1	?	?		
1058	40	78	39	20	19	≥ 1	≥ 1	R#1074,HD [2110]	
1059	196	364	39	21	4	?	-		
1060	976	1464	39	26	1	?	-		
1061	326	489	39	26	3	?	-		
1062	196	294	39	26	5	?	-		
1063	76	114	39	26	13	?	-	R#1073*	
1064	66	99	39	26	15	?	-		
1065	209	247	39	33	6	?	-	R#1072*	
1066	456	494	39	36	3	?	-	R#1071*	
1067	703	741	39	37	2	0	0	R#1070*,×2	
1068	1444	1482	39	38	1	0	0	R#1069*,×2,AG(2,38)	
1069	1483	1483	39	39	1	0	-	×1,PG(2,38)	
1070	742	742	39	39	2	0	-	×1	
1071	495	495	39	39	3	?	-		
1072	248	248	39	39	6	0	-	×1	
1073	115	115	39	39	13	0	-	×1	
1074	79	79	39	39	19	≥ 2091	-	[1087]	VI.18.73
1075	81	1080	40	3	1	$\geq 10^{48}$	$\geq 10^{7}$	AG(4,3) [1463, 1548]	VI.16.12

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
1076	21	280	40	3	4	$\geq 10^{24}$	$\geq 10^{21}$	4#42 [1548]	
1077	9	120	40	3	10	$\geq 10^{8}$	$\geq 10^{5}$	10#2 [1548]	
1078	6	80	40	3	16	76	1	8#4,4#43 [1548]	
1079	121	1210	40	4	1	$\geq 10^{13}$		- [332, 375]	VI.16.61
1080	61	610	40	4	2	$\geq 10^{4}$		- 2#237	
1081	41	410	40	4	3	≥ 1		- D#1192*	II.7.46
1082	31	310	40	4	4	≥ 1		- 2#238	
1083	25	250	40	4	5	$\geq 10^{23}$		- 5#22 [1548]	
1084	21	210	40	4	6	≥ 1		- 2#239	
1085	16	160	40	4	8	$\geq 10^{15}$	$\geq 10^{15}$	8#5 [1548]	
1086	13	130	40	4	10	$\geq 10^{14}$		- 10#3 [1548]	
1087	11	110	40	4	12	≥ 1		- 2#242	
1088	9	90	40	4	15	$\geq 10^{6}$		- 5#24 [1548]	
1089	161	1288	40	5	1	≥ 1		- [1042]	VI.16.16
1090	81	648	40	5	2	≥ 1		- 2#243	
1091	41	328	40	5	4	$\geq 10^{46}$		- 4#45,D#1193*	
1092	33	264	40	5	5	≥ 1		- [1042]	VI.16.17
1093	21	168	40	5	8	$\geq 10^{24}$		- 8#6 [1548]	
1094	17	136	40	5	10	≥ 1		- 2#246	
1095	11	88	40	5	16	$\geq 10^{7}$		- 8#7 [1548]	
1096	201	1340	40	6	1	≥ 1		- [18]	II.3.32
1097	51	340	40	6	4	≥ 1		- 4#48*,2#248	
1098	21	140	40	6	10	≥ 1		- 5#25*,2#249	
1099	49	280	40	7	5	$\geq 10^{53}$	$\geq 10^{53}$	5#26 [1548]	
1100	21	120	40	7	12	$\geq 10^{18}$	≥ 1	4#49,2#250	
1101	281	1405	40	8	1	?		-	
1102	141	705	40	8	2	≥ 1		- [19]	
1103	71	355	40	8	4	≥ 1		- [2144]	VI.16.30
1104	57	285	40	8	5	$\geq 10^{63}$		- 5#27 [1548]	
1105	41	205	40	8	7	≥ 1		- D#1194* [1042]	II.7.46
1106	36	180	40	8	8	≥ 3		- 4#50*,2#251	
1107	29	145	40	8	10	≥ 1		- 5#28*,#157+#379	
1108	21	105	40	8	14	≥ 1		- [1042]	VI.16.30
1109	81	360	40	9	4	$\geq 10^{108}$	$\geq 10^{108}$	4#51 [1548]	
1110	361	1444	40	10	1	?		-	
1111	181	724	40	10	2	≥ 2		- 2#253* [1, 959]	VI.16.30
1112	121	484	40	10	3	≥ 1		- [1]	VI.16.31
1113	91	364	40	10	4	$\geq 10^{125}$		- 4#52 [1548]	
1114	73	292	40	10	5	≥ 1		- [2144]	VI.16.30
1115	61	244	40	10	6	≥ 10		- 2#255* [272]	
1116	46	184	40	10	8	≥ 1		- 4#53*,2#256* [1]	
1117	41	164	40	10	9	≥ 1		- D#1195* [1042]	II.7.46
1118	37	148	40	10	10	≥ 1		- 2#257	
1119	31	124	40	10	12	≥ 152		- 4#54	
1120	25	100	40	10	15	≥ 1		- #160+#384	
1121	21	84	40	10	18	≥ 5		- 2#259	
1122	441	1470	40	12	1	?		-	
1123	111	370	40	12	4	?		- 2#260*	
1124	45	150	40	12	10	≥ 1		- 2#261*,#84+#543	
1125	481	1480	40	13	1	?		?	
1126	105	300	40	14	5	?		-	
1127	561	1496	40	15	1	?		-	
1128	141	376	40	15	4	?		- 2#262*	
1129	81	216	40	15	7	≥ 1		- [2144]	
1130	57	152	40	15	10	?		- 2#263*	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
1131	36	96	40	15	16	≥ 1		- 2#264	
1132	76	190	40	16	8	≥ 1		- 2#265	
1133	171	380	40	18	4	?		- 2#266*	
1134	361	760	40	19	2	≥ 7417	≥ 7417	2#267 [1225]	
1135	761	1522	40	20	1	?		-	
1136	381	762	40	20	2	$\geq 3 \cdot 10^{16}$		- 2#268 [1239]	
1137	191	382	40	20	4	?		- 2#269*	
1138	153	306	40	20	5	?		-	
1139	96	192	40	20	8	≥ 3		- 2#270	
1140	77	154	40	20	10	?		- 2#271*	
1141	41	82	40	20	19	≥ 1		- D#1196 [2110]	
1142	121	220	40	22	7	?		-	
1143	921	1535	40	24	1	?		-	
1144	231	385	40	24	4	?		-	
1145	93	155	40	24	10	?		-	
1146	65	104	40	25	15	?		- R#1171*	
1147	1001	1540	40	26	1	?		-	
1148	81	120	40	27	13	$\geq 10^{13}$	$\geq 10^{13}$	R#1170,$AG_3(4,3)$ [1223]	
1149	217	310	40	28	5	?		-	
1150	91	130	40	28	12	?		- R#1169*	
1151	1161	1548	40	30	1	?		-	
1152	291	388	40	30	4	?		-	
1153	117	156	40	30	10	?		- R#1168*	
1154	156	195	40	32	8	?		- R#1167*	
1155	221	260	40	34	6	?		- R#1166*	
1156	273	312	40	35	5	?		- R#1165*	
1157	351	390	40	36	4	?		- R#1164*	
1158	481	520	40	37	3	?	0	R#1163*,×3	
1159	741	780	40	38	2	0		- R#1162*,×2	
1160	1521	1560	40	39	1	?	?	R#1161*,AG(2,39)	
1161	1561	1561	40	40	1	?		- PG(2,39)	
1162	781	781	40	40	2	0		- ×1	
1163	521	521	40	40	3	?		-	
1164	391	391	40	40	4	?		-	
1165	313	313	40	40	5	0		- ×1	
1166	261	261	40	40	6	0		- ×1	
1167	196	196	40	40	8	0		- ×1	
1168	157	157	40	40	10	0		- ×1	
1169	131	131	40	40	12	?		-	
1170	121	121	40	40	13	$\geq 10^{29}$		- $PG_3(4,3)$ [1223]	VI.18.73
1171	105	105	40	40	15	≥ 4		- [1183]	
1172	42	574	41	3	2	$\geq 6 \cdot 10^{24}$	≥ 1	D [1040, 1548]	VI.16.81
1173	124	1271	41	4	1	≥ 2	≥ 1	[332, 1042, 1047]	III.2.9
1174	165	1353	41	5	1	≥ 15	≥ 1	[396, 1042]	III.2.9
1175	42	287	41	6	5	≥ 2	≥ 2	D [1, 2, 1042]	VI.16.86
1176	42	246	41	7	6	≥ 1	≥ 1	D [1, 1042]	VI.16.87
1177	288	1476	41	8	1	≥ 1	≥ 1	[958]	II.7.50
1178	370	1517	41	10	1	?	?		
1179	247	779	41	13	2	?	?		
1180	42	123	41	14	13	≥ 1	?	D [1]	
1181	247	533	41	19	3	?	?		
1182	780	1599	41	20	1	?	?		
1183	42	82	41	21	20	≥ 1	0	R#1196,×3 [2110]	
1184	124	164	41	31	10	?	0	R#1195*,×3	
1185	165	205	41	33	8	?	0	R#1194*,×3	

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
1186	288	328	41	36	5	?	0	R#1193*,×3	
1187	370	410	41	37	4	?	0	R#1192*,×3	
1188	780	820	41	39	2	?	0	R#1191*,×3	
1189	1600	1640	41	40	1	?	?	R#1190*,AG(2,40)	
1190	1641	1641	41	41	1	?	-	PG(2,40)	
1191	821	821	41	41	2	?	-		
1192	411	411	41	41	4	?	-		
1193	329	329	41	41	5	?	-		
1194	206	206	41	41	8	0	-	×1	
1195	165	165	41	41	10	?	-		
1196	83	83	41	41	20	≥ 1	-	[2110]	VI.18.73

See Also

§II.2	BIBDs with block size 3.
§II.3	Existence results on designs with "small" block size.
§II.7	Resolvable designs.
§II.6	Symmetric designs.
§II.5	Steiner systems.
§IV.2	PBD constructions make BIBDs.
[1016]	A general introduction to combinatorics and in particular to design theory.
[1271]	Contains exhaustive catalogues of BIBDs and their resolutions in electronic form.

References Cited: [1, 2, 4, 18, 19, 21, 22, 33, 41, 43, 46, 114, 124, 127, 144, 180, 246, 248, 272, 323, 324, 331, 332, 352, 375, 380, 382, 392, 393, 396, 404, 416, 514, 518, 528, 534, 537, 562, 587, 607, 619, 620, 623, 660, 679, 688, 692, 693, 694, 696, 697, 710, 734, 790, 827, 848, 856, 898, 957, 958, 959, 976, 978, 1005, 1013, 1016, 1034, 1040, 1042, 1044, 1047, 1053, 1087, 1138, 1151, 1172, 1174, 1183, 1184, 1185, 1188, 1207, 1208, 1223, 1224, 1225, 1228, 1236, 1239, 1241, 1243, 1251, 1262, 1263, 1264, 1265, 1267, 1268, 1271, 1319, 1321, 1339, 1346, 1347, 1349, 1372, 1373, 1374, 1375, 1377, 1378, 1379, 1380, 1381, 1398, 1463, 1496, 1497, 1533, 1537, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1551, 1556, 1566, 1578, 1588, 1605, 1606, 1607, 1609, 1610, 1612, 1628, 1629, 1632, 1633, 1665, 1704, 1705, 1707, 1714, 1720, 1729, 1743, 1773, 1832, 1833, 1839, 1877, 1900, 1903, 1912, 1938, 1940, 1941, 1943, 1944, 1945, 1946, 1976, 1999, 2031, 2039, 2043, 2045, 2058, 2059, 2060, 2062, 2063, 2064, 2065, 2066, 2067, 2071, 2090, 2110, 2130, 2144, 2148]

2 Triple Systems

Charles J. Colbourn

2.1 Definitions and Examples

2.1 A *triple system (TS(v, λ))* $(V, \mathcal{B})$ is a set V of v elements together with a collection $\mathcal{B}$ of 3-subsets (*blocks* or *triples*) of V with the property that every 2-subset of V occurs in exactly λ blocks $B \in \mathcal{B}$. The size of V is the *order* of the TS. It is a *Steiner triple system*, or STS(v), when $\lambda = 1$.

2.2 **Examples** A TS(6, 2) is given in Example 1.18. A Steiner triple system of order 7 is given in Example I.1.3.

2.3 **Remark** A Steiner triple system of order v can exist only when $v-1$ is even because every element occurs with $v-1$ others, and in each block in which it occurs it appears with two other elements. Moreover, every block contains three pairs and hence $\binom{v}{2}$ must be a multiple of 3. Thus, it is necessary that $v \equiv 1, 3 \pmod 6$. This condition was shown to be sufficient in 1847.

2.4 **Theorem** [1300] A Steiner triple system of order v exists if and only if $v \equiv 1, 3 \pmod 6$.

2.5 **Theorem** A $\mathrm{TS}(v, \lambda)$ exists if and only if $v \neq 2$ and $\lambda \equiv 0 \pmod{\gcd(v-2, 6)}$.

2.2 Direct Constructions

2.6 Let W_n be an $(n+1)$-dimensional vector space over $\mathbb{F}_2$. A *punctured* subspace of W_n is obtained from a subspace by removing the zero vector. The *n-dimensional projective space* $\mathrm{PG}(n, 2)$ is the set of all punctured subspaces of W_n, ordered by inclusion. Punctured subspaces of dimension one are *points*, and those of dimension two are *lines*.

2.7 **Theorem** (Projective triple system) The points and lines of $\mathrm{PG}(n, 2)$ form the elements and triples of an $\mathrm{STS}(2^{n+1}-1)$.

2.8 **Construction** A projective triple system of order 2^k-1. Let the points be the nonzero vectors of length k over $\mathbb{F}_2$ and $\{a, b, c\}$ be a block if $a+b+c=0$.

2.9 For V_n an n-dimensional vector space over $\mathbb{F}_3$, the *n-dimensional affine space* $\mathrm{AG}(n, 3)$ is the set of all subspaces of V_n *and their cosets*, ordered by set inclusion. Points are vectors, and lines are translates of 1-dimensional subspaces.

2.10 **Theorem** (Affine triple system) The points and lines of $\mathrm{AG}(n, 3)$ form the elements and triples of an $\mathrm{STS}(3^n)$.

2.11 **Theorem** [1670] Let p be a prime, $n \geq 1$, and $p^n \equiv 1 \pmod 6$. Let $\mathbb{F}_{p^n}$ be a finite field on a set X of size $p^n = 6t+1$ with 0 as its zero element, and ω a primitive root of unity. Then $\{\{\omega^i + j, \omega^{2t+i} + j, \omega^{4t+i} + j\} : 0 \leq i < t, j \in X\}$ (with computations in $\mathbb{F}_{p^n}$) is the set of blocks of an $\mathrm{STS}(p^n)$ on X.

2.12 **Theorem** (Netto triple system) Let p be a prime, $n \geq 1$, and $p^n \equiv 7 \pmod{12}$. Let $\mathbb{F}_{p^n}$ be a finite field on a set X of size $p^n = 6t+1 = 12s+7$ with 0 as its zero element and ω a primitive root of unity. Then $\{\{\omega^{2i} + j, \omega^{2t+2i} + j, \omega^{4t+2i} + j\} : 0 \leq i < t, j \in X\}$ forms the blocks of an $\mathrm{STS}(p^n)$ on X.

2.13 **Remark** Constructions VI.53.17 and VI.53.19 give a direct method for producing STSs using Skolem sequences. Algorithm VII.6.71 gives a fast computational method for constructing STSs.

2.3 Recursive Constructions

2.14 **Construction** (Moore) If there exist an $\mathrm{STS}(u)$ and an $\mathrm{STS}(v)$ that contains an $\mathrm{STS}(w)$ subsystem (see §2.5), then there exists an $\mathrm{STS}(u(v-w)+w)$. Because every $\mathrm{STS}(v)$ contains a subsystem of orders 0 and 1, if there exist an $\mathrm{STS}(u)$ and an $\mathrm{STS}(v)$, then there exist an $\mathrm{STS}(uv)$ and an $\mathrm{STS}(u(v-1)+1)$.

2.15 **Construction** An $\mathrm{STS}(2v+1)$ from an $\mathrm{STS}(v)$. Let $(V, \mathcal{B})$ be an $\mathrm{STS}(v)$ on element set V. Let $X = (V \times \{0, 1\}) \cup \{\infty\}$. For every block $\{x, y, z\} \in \mathcal{B}$, form blocks $\{(x, \alpha), (y, \beta), (z, \gamma)\}$ for $\alpha, \beta, \gamma \in \{0, 1\}$ with $\alpha + \beta + \gamma \equiv 0 \pmod 2$. Adjoin the blocks $\{\infty, (x, 0), (x, 1)\}$ for $x \in V$.

2.16 **Remark** Construction 2.15 applied to Example I.1.40 produces an STS(15). This STS(15) contains within it an STS(7) on the elements $\{0,\dots,6\}\times\{0\}$, a *subdesign* of the STS.

2.17 **Construction** An STS($3v$) from an STS(v) (Bose Construction). Let $(V,\oplus)$ be an idempotent, commutative quasigroup. On $V\times\mathbb{Z}_3$, let

$$\mathcal{D}=\{(x,i),(y,i),(x\oplus y,(i+1) \bmod 3)\} : x,y\in V,\ x\neq y,\ i\in\mathbb{Z}_3\},\text{ and}$$
$$\mathcal{C}=\{\{(x,0),(x,1),(x,2)\} : x\in V\}.$$

Then $(V\times\mathbb{Z}_3,\mathcal{C}\cup\mathcal{D})$ is an STS($3v$).

2.4 Isomorphism and Automorphism

2.18 Two set systems $(V,\mathcal{B})$ and $(W,\mathcal{D})$ are *isomorphic* if there is a bijection (*isomorphism*) ϕ from V to W so that the number of times B appears as a block in $\mathcal{B}$ is the same as the number of times $\phi(B)=\{\phi(x) : x\in B\}$ appears as a block in $\mathcal{D}$. An isomorphism from a set system to itself is an *automorphism.*

2.19 **Remark** Up to isomorphism, there are a unique STS(7); a unique STS(9) (Example 1.22); two STS(13)s (Table 1.26); 80 STS(15)s (Table 1.28); and 11,084,874,829 STS(19)s ([1268], also §VII.6). There are a unique TS$(6,2)$, 4 TS$(7,2)$s (Table 1.19), 10 TS$(7,3)$s (Table 1.20), and 36 TS$(9,2)$s (Table 1.23). See §II.1 for further enumeration results.

2.20 **Theorem** (see [578]) The number of STS(v)s is $v^{v^2\left(\frac{1}{6}+o(1)\right)}$ as $v\to\infty$.

2.21 **Theorem** [589] Determining isomorphism of triple systems (of arbitrary index) is polynomial time equivalent to determining isomorphism of graphs.

2.22 **Theorem** [1603] Isomorphism of STS(v)s can be determined in $v^{\log v+O(1)}$ time.

2.23 **Remark** The $v^{\log v+O(1)}$ method can be parallelized: Isomorphism of STS(v)s can be determined in $O((\log v)^2)$ time with $O(v^{\log v+2})$ processors [581].

2.24 A TS(v,λ) is *cyclic* if it admits an automorphism of order v, and *k-rotational* if it admits an automorphism containing one fixed point and k cycles each of length $\frac{v-1}{k}$.

2.25 **Theorem** (see [578]) There is a cyclic triple system of order v and index λ if and only if:

1. $\lambda\equiv 1,5 \pmod 6$ and $v\equiv 1,3 \pmod 6$, $(v,\lambda)\neq(9,1)$;
2. $\lambda\equiv 2,10 \pmod{12}$ and $v\equiv 0,1,3,4,7,9 \pmod{12}$, $(v,\lambda)\neq(9,2)$;
3. $\lambda\equiv 3 \pmod 6$ and $v\equiv 1 \pmod 2$;
4. $\lambda\equiv 4,8 \pmod{12}$ and $v\equiv 0,1 \pmod 3$;
5. $\lambda\equiv 6 \pmod{12}$ and $v\equiv 0,1,3 \pmod 4$; or
6. $\lambda\equiv 0 \pmod{12}$ and $v\geq 3$.

2.26 Two cyclic TS(v,λ)s are (*multiplier*) *equivalent* if, when they share the cyclic automorphism $i\mapsto(i+1) \bmod v$, there is an isomorphism from one to the other of the form $i\mapsto\mu\cdot i \bmod v$.

2.27 **Theorem** (Bays–Lambossy, see [578]) If $\mathcal{B}_1$ and $\mathcal{B}_2$ are cyclic collections of subsets of the same set V for $|V|$ a prime, then the two collections are isomorphic if and only if they are multiplier equivalent.

2.28 Remark Theorem 2.27 holds more generally than for prime orders, but does not extend to all orders. Here are three difference families generating three isomorphic but inequivalent cyclic TS(16, 2)s:

1. $\{\{0,1,2\},\ \{0,2,9\},\ \{0,3,6\},\ \{0,4,8\},\ \{0,5,10\}\}$;
2. $\{\{0,1,3\},\ \{0,1,6\},\ \{0,2,7\},\ \{0,3,10\},\ \{0,4,8\}\}$;
3. $\{\{0,1,7\},\ \{0,1,10\},\ \{0,2,5\},\ \{0,2,13\},\ \{0,4,8\}\}$.

This design has a full automorphism group of order 128. Indeed there are isomorphic but inequivalent STS(v)s as well; the smallest example has order $v = 49 = 7^2$ [1737].

2.29 Table [578] The number of (multiplier) inequivalent cyclic TS(v, λ)s for small v and λ. When x/y is given, the first number is the count for simple systems, the second number for all.

$v\backslash\lambda$	1	2	3	4	5	6	7
5			1/1			0/1	
6		0		1/2		0	
7	1/1	1/2	1/3	1/4	1/5	0/7	0/8
8						1/12	
9	0	0	1/4	1/3	0/4	0/24	1/27
10		0		9/21		0	
11			6/8			6/209	
12		0/4		62/180		62/3561	
13	1/1	7/9	23/47	71/253	117/1224	117/5285	71/20347
14						0	
15	2/2	0/9	237/421	902/2981	0/15686	6577/375372	?/?
16		67/71		6916/21742		66418/2460490	

2.30 Table [578] The number of (multiplier) inequivalent cyclic STS(v)s for $19 \le v \le 57$.

Order	#	Order	#	Order	#	Order	#
19	4	21	7	25	12	27	8
31	80	33	84	37	820	39	798
43	9508	45	11616	49	157340	51	139828
55	3027456	57	2353310				

2.31 Theorem [1741] A cyclic STS($n \cdot u$) containing a cyclic sub-STS(u) exists if and only if $n \cdot u \equiv 1, 3 \pmod 6$, $n \cdot u \neq 9$, $u \equiv 1, 3 \pmod 6$, $u \neq 9$, and if $u \equiv 3 \pmod 6$, then $n \neq 3$.

2.32 Theorem (see [578]) A 1-rotational TS(v, λ) exists if and only if

$\lambda = 1$	and	$v \equiv 3, 9 \pmod{24}$
$\lambda \equiv 1, 5 \pmod 6$, $\lambda > 1$	and	$v \equiv 1, 3 \pmod 6$
$\lambda \equiv 2, 4 \pmod 6$	and	$v \equiv 0, 1 \pmod 3$
$\lambda \equiv 3 \pmod 6$	and	$v \equiv 1 \pmod 2$
$\lambda \equiv 0 \pmod 6$	and	$v \neq 2$

2.33 Theorem [556] Let v, k be positive integers such that $1 \le k \le (v-1)/2$. Then a k-rotational STS(v) exists if and only if all of $v \equiv 1, 3 \pmod 6$; $v \equiv 3 \pmod 6$ if $k = 1$; $v \equiv 1 \pmod k$; and $v \not\equiv 7, 13, 15, 21 \pmod{24}$ if $(v-1)/k$ is even.

2.34 Theorem [130] Almost all Steiner triple systems have no automorphism other than the trivial one.

2.35 Table ([1268] with corrections) The *type* of an automorphism is the lengths of the cycles of points induced by its action (written in exponential notation omitting the fixed points). In the table on the left, the numbers of STS(19)s that admit one or more *basic automorphisms*, those of type a^m for $a \geq 2$ prime, are given. The systems are partitioned by the order of the automorphism group (Ord) and the subset of basic automorphisms represented; to distinguish subsets arising for the same group order, a letter indicates the class (Cl) of the partition. In the table on the right, classes are refined to further indicate the remaining automorphisms. Systems whose group is generated by a single basic automorphism are omitted in the second table. Any type of automorphism not explicitly mentioned does not arise as the type of an automorphism of an STS(19).

Basic Automorphisms								
Ord	Cl	19^1	2^9	3^6	2^8	2^6	3^4	#STSs
432				⋆	⋆	⋆	⋆	1
171		⋆		⋆				1
144				⋆	⋆	⋆		1
108				⋆	⋆	⋆	⋆	1
96				⋆	⋆	⋆		1
57		⋆		⋆				2
54				⋆		⋆	⋆	2
32					⋆	⋆		3
24				⋆	⋆	⋆		11
19		⋆						1
18	a		⋆	⋆				1
	b			⋆	⋆		⋆	2
	c			⋆		⋆	⋆	6
	d			⋆		⋆		2
16					⋆	⋆		13
12	a			⋆	⋆	⋆		8
	b			⋆	⋆			7
	c			⋆		⋆		12
	d				⋆	⋆	⋆	10
9				⋆				19
8	a				⋆	⋆		84
	b				⋆			17
6	a		⋆	⋆				14
	b			⋆	⋆			14
	c			⋆		⋆		116
	d				⋆		⋆	10
	e					⋆	⋆	28
4	a				⋆	⋆		839
	b				⋆			662
	c					⋆		620
3	a			⋆				12664
	b						⋆	64
2	a		⋆					169
	b				⋆			78961
	c					⋆		70392
totals		4	184	12885	80645	72150	124	164758

Nonbasic Automorphisms											
Cl	9^2	6^3	$3^2 6^2$	$2^1 4^4$	$2^1 8^2$	8^2	4^4	$2^2 6^2$	$2^2 4^3$	#
432			⋆			⋆	⋆	⋆		1
171	⋆									1
144			⋆	⋆	⋆		⋆			1
108			⋆					⋆		1
96			⋆				⋆			1
57										2
54			⋆							2
32				⋆			⋆			3
24			⋆							11
18a		⋆								1
18b								⋆		2
18c			⋆							6
18d			⋆							2
16						⋆	⋆			1
							⋆			1
				⋆	⋆		⋆			5
				⋆						6
12a			⋆							8
12b										7
12c										12
12d								⋆		10
9	⋆									9
										10
8a							⋆			2
										82
8b				⋆			⋆			5
					⋆		⋆			10
						⋆	⋆			2
6a		⋆								14
6b										14
6c			⋆							104
										12
6d								⋆		10
6e										28
4a										839
4b				⋆						498
							⋆			153
										11
4c									⋆	48
										572
totals	10	15	137	518	16	4	185	24	48	

2.5 Subsystems, Holes, and Embedding

2.36 A *partial triple system* $\mathrm{PTS}(v,\lambda)$ is a set V of v elements and a collection $\mathcal{B}$ of triples, so that each unordered pair of elements occurs in at most λ triples of $\mathcal{B}$. Its *leave* is the multigraph on vertex set V in which the edge $\{x,y\}$ appears $\lambda - s$ times when there are precisely s triples of $\mathcal{B}$ containing $\{x,y\}$. An *incomplete triple system* of order v and index λ, and with a *hole* of size w, is a $\mathrm{PTS}(v,\lambda)$ $(V,\mathcal{B})$ with the property that for some $W \subseteq V$, $|W| = w$,

1. if $x,y \in W$, no triple of $\mathcal{B}$ contains $\{x,y\}$; and
2. if $x \in V \setminus W$ and $y \in V$, then exactly λ triples of $\mathcal{B}$ contain $\{x,y\}$.

Such a partial system is denoted $\mathrm{ITS}(v,w;\lambda)$. When an $\mathrm{ITS}(v,w;\lambda)$ $(V,\mathcal{B})$ exists having a hole on $W \subseteq V$, if there is a $\mathrm{TS}(w,\lambda)$ $(W,\mathcal{D})$, the system $(V,\mathcal{B}\cup\mathcal{D})$ is a $\mathrm{TS}(v,\lambda)$. In this system, the $\mathrm{TS}(w,\lambda)$ is a *subsystem*.

2.37 **Theorem** [747] (Doyen–Wilson Theorem) Let $v,w \equiv 1,3 \pmod 6$ and $v \geq 2w+1$. Then there exists an $\mathrm{STS}(v)$ containing an $\mathrm{STS}(w)$ as a subdesign.

2.38 **Theorem** [1957] An $\mathrm{ITS}(v,w;\lambda)$ exists if and only if

1. $w = 0$ and $\lambda \equiv 0 \pmod{\gcd(v-2,6)}$,
2. $v = w$, or
3. $0 < w < v$ and
   (a) $v \geq 2w+1$,
   (b) $\lambda\left(\binom{v}{2} - \binom{w}{2}\right) \equiv 0 \pmod 3$, and
   (c) $\lambda(v-1) \equiv \lambda(v-w) \equiv 0 \pmod 2$.

2.39 **Theorem** [745] A subsystem-free $\mathrm{STS}(v)$ exists for all $v \equiv 1,3 \pmod 6$.

2.40 Let $(V,\mathcal{B})$ be a $\mathrm{PTS}(v,\lambda)$ and $(W,\mathcal{D})$ a $\mathrm{TS}(w,\mu)$ for which $V \subseteq W$ and $\mathcal{B}$ is a submultiset of $\mathcal{D}$. Then $(W,\mathcal{D})$ is an *enclosing* of $(V,\mathcal{B})$. When $\lambda = \mu$, the enclosing is an *embedding*. When $v = w$, the enclosing is an *immersion*. When both equalities hold, the enclosing is a *completion*. An enclosing is *faithful* if the only triples of $\mathcal{D}$ wholly contained in V are those in $\mathcal{B}$.

2.41 **Theorem** [361] Any partial Steiner triple system of order v can be embedded in a Steiner triple system of order w if $w \equiv 1,3 \pmod 6$ and $w \geq 2v+1$.

2.42 **Conjecture** [551] Every $\mathrm{PTS}(v,1)$ has an enclosing in a $\mathrm{TS}(w,\mu)$ in which

$$(w-v)+(\mu-1) \leq \begin{cases} 3 & \text{if } v \equiv 4 \pmod 6,\ v \geq 16, \\ 2 & \text{otherwise.} \end{cases}$$

2.43 **Remark** Even the determination of when a $\mathrm{TS}(v,\lambda)$ can be enclosed in a $\mathrm{TS}(w,\mu)$ faithfully is not solved. Two partial results are in Theorems 2.44 and 2.45.

2.44 **Theorem** [268] A $\mathrm{TS}(v,\lambda)$ has a faithful enclosing in a $\mathrm{TS}(w,\mu)$ whenever $\mu \geq \lambda$, $\mu \equiv 0 \pmod{\gcd(w-2,6)}$, and $w \geq 2v+1$.

2.45 **Theorem** [267] A $\mathrm{TS}(v,\lambda)$ has a faithful enclosing in a $\mathrm{TS}(w,2\lambda)$ if and only if $w \geq (3v-1)/2$.

2.6 Leaves, Excesses, and Neighborhoods

2.46 **Theorem** [785] The maximum number of triples in a PTS(v, λ) is

$$\begin{cases} \lfloor \frac{v}{3} \lfloor \frac{\lambda(v-1)}{2} \rfloor \rfloor - 1 & \text{if} \quad v \equiv 2(6) \text{ and } \lambda \equiv 4(6) \\ & \text{or} \quad v \equiv 5(6) \text{ and } \lambda \equiv 1(3) \\ \lfloor \frac{v}{3} \lfloor \frac{\lambda(v-1)}{2} \rfloor \rfloor & \text{otherwise} \end{cases}$$

2.47 **Theorem** [573] Let G be a graph on $v \equiv 1 \pmod 2$ vertices with every vertex of degree 0 or 2, having $0 \pmod 3$ edges if $v \equiv 1, 3 \pmod 6$ or $1 \pmod 3$ edges if $v \equiv 5 \pmod 6$. Then G is the leave of a PTS$(v, 1)$ unless $v = 7$ and $G = 2\{C_3\} \cup K_1$, or $v = 9$ and $G = C_4 \cup C_5$.

2.48 **Conjecture** [1668] Let G be a graph with maximum degree k on $v \geq 4k + 2$ vertices and m edges in which the degree of every vertex is congruent to $v - 1$ modulo 2, and for which $\binom{v}{2} - m \equiv 0 \pmod 3$. Then G is the leave of a PTS$(v, 1)$.

2.49 Let $\mathcal{B}$ be a collection of 3-subsets on element set V of cardinality v. For every 2-subset $\{x, y\}$ of V, let λ_{xy} be the number of triples in $\mathcal{B}$ in which $\{x, y\}$ occurs. If $\lambda_{xy} \geq \lambda$ for all $\{x, y\} \subset V$, $(V, \mathcal{B})$ is a *covering* $CT(v, \lambda)$ whose *excess* is the multigraph (V, E) in which for every 2-subset $\{x, y\}$ the edge $\{x, y\}$ appears $\lambda_{xy} - \lambda$ times in E. The covering is *minimal* if every triple in $\mathcal{B}$ contains a pair $\{w, z\}$ for which $\lambda_{wz} = \lambda$, and *minimum* if $\mathcal{B}$ is the smallest among all CT(v, λ)s.

2.50 **Theorem** [785] The number of triples in a minimum $CT(v, \lambda)$ is

$$\mu(v, \lambda) = \begin{cases} \lceil \frac{v}{3} \lceil \frac{\lambda(v-1)}{2} \rceil \rceil + 1 & \text{if} \quad v \equiv 2(6) \text{ and } \lambda \equiv 2(6) \\ & \text{or} \quad v \equiv 5(6) \text{ and } \lambda \equiv 2(3) \\ \lceil \frac{v}{3} \lceil \frac{\lambda(v-1)}{2} \rceil \rceil & \text{otherwise} \end{cases}$$

2.51 **Theorem** [574] Every multigraph with vertex degrees from $\{0, 2\}$ on $v \equiv 1 \pmod 2$ vertices, having e edges with $e \equiv 0 \pmod 3$ when $v \equiv 1, 3 \pmod 6$ or $e \equiv 2 \pmod 3$ when $v \equiv 5 \pmod 6$, is an excess of a CT$(v, 1)$.

2.52 The *neighborhood* of an element x in a TS(v, λ) is the λ-regular multigraph on $v - 1$ vertices whose edges are the pairs occurring in triples with x.

2.53 **Theorem** [571, 524] Let G be an n-vertex λ-regular simple graph, other than two disjoint triangles. Then if $\lambda \equiv 0 \pmod{\gcd(n - 1, 6)}$, G is a λ-neighborhood. Indeed for $n \geq 8$, $n \equiv 0, 2 \pmod 3$, every λ-regular n-vertex *multigraph* with $\lambda \equiv 0 \pmod{\gcd(n - 1, 6)}$ is a λ-neighborhood.

2.54 A *double star* of triples based on a pair $\{x, y\}$ of a v-set V is a partial triple system on V so that every triple contains at least one of $\{x, y\}$, and every element $z \in V \setminus \{x, y\}$ appears in exactly one triple with x and exactly one triple with y. Equivalently, a double star is a simultaneous specification of the neighborhoods of x and y, a *double neighborhood*.

2.55 **Theorem** [541] Every double star on $n \equiv 1, 3 \pmod 6$ elements can be completed to a Steiner triple system of order n.

2.7 Intersection, Support, and Large Sets

2.56 Let $(V, \mathcal{B})$ and $(V, \mathcal{D})$ be two STS(v)s. Their *intersection size* is $|\mathcal{B} \cap \mathcal{D}|$. They are *disjoint* when their intersection size is zero. A set of $v - 2$ STS(v)s $\{(V, \mathcal{B}_i) : i = 1, \ldots, v - 2\}$ is a *large set* if every two systems in the set are disjoint.

2.57 Theorem [2009] Let $(V, \mathcal{B})$ and $(V, \mathcal{D})$ be two STS(v)s. Then there exists a permutation π on V such that $(V, \mathcal{B})$ and $(\pi(V), \pi(\mathcal{D}))$ are disjoint.

2.58 Theorem [1464] Let $v \equiv 1, 3 \pmod 6$, $v \geq 15$, and $0 \leq d \leq \binom{v}{2}$ with $d \notin \{\binom{v}{2} - 5, \binom{v}{2} - 3, \binom{v}{2} - 2, \binom{v}{2} - 1\}$. Then there exist two STS(v)s whose intersection size is d.

2.59 Let $(V, \mathcal{B})$ be a TS(v, λ). The *support size* is the number of distinct triples in $\mathcal{B}$.

2.60 Theorem [561, 565, 578] Let $m_v = \lceil \frac{v(v-1)}{6} \rceil$, $s_v = \lceil \frac{v(v+2)}{6} \rceil$, and

$$M_{v,\lambda} = \max\left(\tfrac{\lambda v(v-1)}{6}, \tbinom{v}{3}\right).$$

Define PS(v, λ) $= \varnothing$ if $\lambda \not\equiv 0 \pmod{\gcd(v-2, 6)}$. Otherwise when $v - 2 \neq \lambda$, PS(v, λ) is:

$v \pmod{12}$	PS(v, λ)
0, 4	$s_v, s_v + 2, s_v + 3, \ldots, M_{v,\lambda}$
1, 3, 7, 9	$m_v, m_v + 4, m_v + 6, m_v + 7, \ldots, M_{v,\lambda}$
2	$s_v + 7, \ldots, M_{v,\lambda}$
5, 11	$m_v + 6, m_v + 9, m_v + 10, \ldots, M_{v,\lambda}$
6, 10	$s_v + 1, s_v + 2, \ldots, M_{v,\lambda}$
8	$s_v + 6, s_v + 8, s_v + 9, \ldots, M_{v,\lambda}$

When $\lambda = v - 2$, PS(v, λ) is defined similarly, but with the omission of $\{M_{v,\lambda} - 5, M_{v,\lambda} - 3, M_{v,\lambda} - 2, M_{v,\lambda} - 1\}$. Then for $v \notin \{6, 7, 8, 9, 10, 12, 14\}$, and $\lambda \geq 1$, there is a TS(v, λ) with support size s if and only if $s \in$ PS(v, λ) except possibly when $v \equiv 8 \pmod{12}$ and $s = s_v + 7$.

2.61 For a TS(v, λ), let c_i be the number of distinct blocks that are each i-times repeated in the system. The *fine structure* of the TS is $(c_1, c_2, \ldots, c_\lambda)$.

2.62 Theorem [569, 570] Let $v \geq 17$. Then $(3s - 2t + \delta, t, \lfloor v(v-1)/6 \rfloor - s)$ is the fine structure of a TS($v, 3$) if and only if

- $v \equiv 1, 3 \pmod 6$; $\delta = 0$; $0 \leq t \leq s \leq v(v-1)/6$; $s \notin \{1, 2, 3, 5\}$; and $(t, s) \notin \{(1,4), (2,4), (3,4), (1,6), (2,6), (3,6), (5,6), (2,7), (5,7), (1,8), (3,8), (5,8)\}$ or
- $v \equiv 5 \pmod 6$; $\delta = 1$; $0 \leq t < s \leq \lfloor v(v-1)/6 \rfloor$; $s \notin \{1, 2, 4, 5\}$; and $(t, s) \notin \{(1,3), (2,3), (0,6), (1,6), (2,6), (3,6), (0,7), (1,7), (2,7), (3,7), (5,7), (0,8), (1,8), (2,8), (6,8), (7,8), (1,9)\}$.

2.63 Theorem [1482, 1483, 2015] There exists a large set of STS(v)s if and only if $v \equiv 1, 3 \pmod 6$ and $v \neq 7$.

2.64 Theorem When $v \equiv 0, 4 \pmod 6$, there are $\frac{v-2}{2}$ disjoint TS($v, 2$)s and when $v \equiv 2 \pmod 6$ there are $\frac{v-2}{6}$ disjoint TS($v, 2$)s [2008]. When $v \equiv 5 \pmod 6$, there are $\frac{v-2}{3}$ disjoint TS($v, 3$)s [2011]. From these large sets and Theorem 2.63, it follows that a *simple* TS(v, λ) exists if and only if $\lambda \leq v - 2$ and $\lambda \equiv 0 \pmod{\gcd(v-2, 6)}$.

2.65 An *overlarge set* of STS(v)s is a partition of all triples on $v + 1$ points into $v + 1$ disjoint STS(v)s.

2.66 Theorem The $v + 1$ derived designs of a Steiner quadruple system of order $v + 1$ form an overlarge set of STS(v)s; hence, these exist for all $v \equiv 1, 3 \pmod 6$.

2.67 Two STS(v)s are *almost disjoint* if they share exactly one triple. A *large set of mutually almost disjoint (MAD)* STS(v)s is a set of k STS(v)s that are pairwise almost disjoint, and for which every triple on v points appears in at least one of the STSs.

2.68 **Theorem** (see [1462]) There exists a large set of k MAD STS(v)s only if $k \in \{v, v+1\}$ when $v > 7$. A large set of v MAD STS(v)s exists if and only if $v \equiv 1, 3 \pmod 6$.

2.69 **Conjecture** [970] A large set of $v+1$ MAD STS(v)s exists if and only if $v \equiv 1, 3 \pmod 6$ and $v \geq 13$. (Solutions are known for $v = 13$ and $v = 15$.)

2.70 **Remark** The existence of large sets of *Kirkman* triple systems of order v when $v \equiv 3 \pmod 6$, known as *Sylvester's Problem*, remains open. See [1423] for a survey. Sylvester posed the problem when $v = 15$ [442] and settled existence when v is a power of three.

2.71 **Example** [690] A large set of KTS(15)s. Consider the KTS(15) in which the rows form the parallel classes:

0,1,9	2,4,12	5,10,11	7,8,α	3,6,β
0,2,7	3,4,8	5,6,12	9,11,α	1,10,β
0,3,11	1,7,12	6,8,10	2,5,α	4,9,β
0,4,6	1,8,11	2,9,10	3,12,α	5,7,β
0,5,8	1,2,3	6,7,9	4,10,α	11,12,β
0,10,12	3,5,9	4,7,11	1,6,α	2,8,β
1,4,5	2,6,11	3,7,10	8,9,12	0,α,β

Under the automorphism fixing α and β and mapping $i \mapsto (i+1) \bmod 13$, thirteen disjoint KTS(15)s are produced; this is a large set.

2.72 Two STS(v)s $(V, \mathcal{A})$ and $(V, \mathcal{B})$ are *orthogonal* if $\mathcal{A} \cap \mathcal{B} = \varnothing$, and whenever $\{\{a,b,w\},\{x,y,w\}\} \subset \mathcal{A}$ and $\{\{a,b,s\},\{x,y,t\}\} \subset \mathcal{B}$, one has $s \neq t$.

2.73 **Theorem** [549] If $v \equiv 1, 3 \pmod 6$, $v \geq 7$, and $v \neq 9$, then there exist two orthogonal STS(v)s.

2.74 **Theorem** [712] There exist three mutually orthogonal STS(v)s whenever $v \equiv 1, 3 \pmod 6$, $v \geq 19$, except possibly when $v = 6n+3$ for $n \in \{3,\ 17,\ 27,\ 29,\ 31,\ 34,\ 35,\ 37,\ 38,\ 40,\ \ldots,\ 51,\ 57,\ 58,\ 59\}$.

2.8 Resolvability

2.75 A set of blocks is a *partial parallel class (PPC)* if no two blocks in the set share an element. A PPC is an *almost parallel class* if it contains $\frac{v-1}{3}$ blocks; when it contains $\frac{v}{3}$ blocks, it is a *parallel class* or *resolution class*. A partition of all blocks of a TS(v, λ) into parallel classes is a *resolution* and the STS is *resolvable*. An STS(v) together with a resolution of its blocks is a *Kirkman triple system*, KTS(v).

2.76 **Example** In 1850, the Reverend Thomas P. Kirkman posed the question:

Kirkman's schoolgirl problem:
Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily, so that no two walk twice abreast.

This is equivalent to finding a KTS(15), a resolution of some Steiner triple system of order 15. Of the eighty nonisomorphic STS(15)s (Table II.1.28), exactly four are resolvable.

However, there are *seven* nonisomorphic *resolved* systems, seven KTS(15)s. These are given here, using the numbering of the underlying STSs and displaying blocks as columns.

The Seven Solutions of the Kirkman Schoolgirl Problem							
#	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1a	adefg	abcdf	abcdg	abcfg	abcde	abcef	abceg
	bjhik	hemkj	jmehi	dlikh	fhlik	lidjh	ndhij
	cnmol	ignol	kofln	enjmo	gjomn	mkgon	ofklm
1b	adefg	abcdf	abcdg	abcfg	abcde	abceg	abcef
	bjhik	hemkj	jmehi	dilhj	flhij	ldikh	nhdik
	cnmol	ignol	kofln	ekonm	gnkmo	mfjno	ojglm
7a	adefg	abceg	abcdf	abcfg	abcde	abcef	abcdg
	bjikh	hdlkj	jemhi	dlihk	fmhij	lidhj	nheki
	comln	ifonm	kgnlo	enjmo	goknl	mkgon	ojfml
7b	adefg	abceg	abcdf	abcfg	abcde	abcdg	abcef
	bjikh	hdlkj	jemhi	dmhji	flikh	lheik	nidjh
	comln	ifonm	kgnlo	eoknl	gnjmo	mjfno	okglm
15a	abcfg	abcde	abceg	abcdf	adefg	abcdg	abcef
	dihmj	fhikl	ldkih	nejih	bhkji	hmejk	jldhi
	eklno	gjnmo	mfojn	ogmlk	conlm	iofnl	kngmo
15b	abcfg	abcde	abceg	abcdf	adefg	abcef	abcdg
	dihmj	fhikl	ldkih	nejih	bjhik	hmdkj	jlehi
	eklno	gjnmo	mfojn	ogmlk	cnmol	iognl	knfom
61	adefg	abcfg	abcde	abcdf	abcdg	abcef	abceg
	bijlh	dijhk	fhimk	heljk	jmehi	lkdhi	ndhij
	cknom	elmno	gjonl	ignom	kofln	mngoj	ofkml

2.77 **Theorem** [1484, 1781] There exists a KTS(v) if and only if $v \equiv 3 \pmod 6$.

2.78 **Theorem** [1792] Let $v, w \equiv 3 \pmod 6$ and $v \geq 3w$. Then there exists a KTS(v) containing a sub-KTS(w) (the resolution of the KTS(v) extends that of the KTS(w)).

2.79 A *Hanani triple system* is an STS(v) with a partition of its blocks into $(v-1)/2$ maximum parallel classes, and a single partial parallel class with $(v-1)/6$ blocks.

2.80 **Theorem** [2095] A Hanani triple system of order v exists if and only if $v \equiv 1 \pmod 6$ and $v \notin \{7, 13\}$.

2.81 A *block-coloring* of a TS(v, λ) is an assignment of colors to the blocks so that no two blocks of the same color intersect (equivalently, a partition of the blocks into partial parallel classes).

2.82 **Conjecture** [787] (Special case of the Erdős–Faber–Lovász Conjecture) Every STS(v) admits a block-coloring with at most v colors.

2.83 **Theorem** (see [578]) There is a triple system TS(v, λ) that admits a block-coloring in $\left\lceil \frac{\lambda v(v-1)/6}{\lfloor v/3 \rfloor} \right\rceil$ colors, in which at most one color class is not a partial parallel class with $\lfloor \frac{v}{3} \rfloor$ blocks, whenever $\lambda \equiv 0 \pmod{\gcd(v-2, 6)}$ and $v \geq 3$, except when $v = 6$ and $\lambda \equiv 2 \pmod 4$, $(v, \lambda) = (13, 1)$, or $v = 7$ and $\lambda \in \{1, 3, 5\}$.

2.84 **Remark** Not every Steiner triple system has even a single parallel class. The minimum size of a maximum cardinality partial parallel class in an STS(v) remains open.

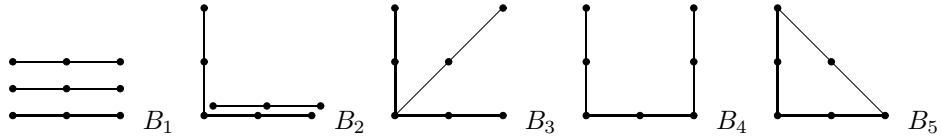
2.85 **Theorem** [78] Every STS(v) contains a partial parallel class containing at least $(v/3) - cv^{1/2}(\ln v)^{3/2}$ blocks, for c an absolute constant.

2.86 **Conjecture** (see [578]) For all $v \equiv 1, 3 \pmod 6$, $v \geq 15$, there exists an STS(v) whose largest partial parallel class has fewer than $\lfloor v/3 \rfloor$ blocks.

2.9 Configurations in Steiner Triple Systems

2.87 A (k,ℓ)-*configuration* in an STS(v) is simply a set of ℓ lines whose union contains precisely k points. It is *constant* if every STS(v) contains the same number of copies of the configuration, *variable* otherwise.

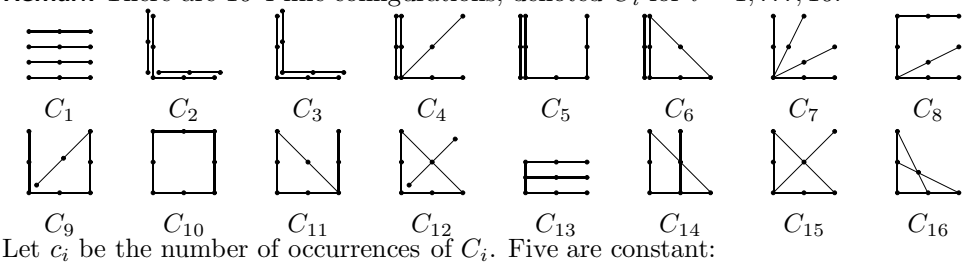
2.88 **Remark** Each configuration with at most three lines is constant. The number of 1-line configurations is just the number of triples, $v(v-1)/6$. There are two 2-line configurations. A pair of disjoint triples occurs $v(v-1)(v-3)/72$ times, while a pair of intersecting triples appears $v(v-1)(v-3)/8$ times. The five 3-line configurations B_i, $i=1,\ldots,5$ are



Set $n_v = v(v-1)(v-3)$. The number b_i of times that B_i occurs satisfies

$$b_1 = n_v(v-7)(v^2-19v+96)/1296;\ \ b_2 = n_v(v-7)(v-9)/48;$$
$$b_3 = n_v(v-4)/48;\ \ b_4 = n_v(v-7)/8;\ \ b_5 = n_v/6 = 4a_2/3.$$

2.89 **Remark** There are 16 4-line configurations, denoted C_i for $i=1,\ldots,16$:



Let c_i be the number of occurrences of C_i. Five are constant:

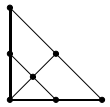
$$c_4 = n_v(v-7)(v-9)(v-11)/288;\quad c_7 = n_v(v-5)(v-7)/384;$$
$$c_8 = n_v(v-7)(v-9)/16;\quad c_{11} = n_v(v-7)/4;\quad \text{and}\quad c_{15} = n_v/6.$$

2.90 **Theorem** [945] The number of occurrences of each variable 4-line configuration is determined by the number of occurrences of any single one of them. Indeed,

$$\begin{aligned}
c_1 &= n_v(v-9)(v-10)(v-13)(v^2-22v+141)/31104 + c_{16}\\
c_2 &= n_v(v-9)(v-10)(v^2-22v+129)/576 - 6c_{16}\\
c_3 &= n_v(v-9)^2(v-11)/128 + 3c_{16}\\
c_5 &= n_v(v-9)(v^2-20v+103)/48 + 12c_{16}\\
c_6 &= n_v(v-9)(v-10)/36 - 4c_{16}\\
c_9 &= n_v(v-9)^2/8 - 12c_{16}\\
c_{10} &= n_v(v-8)/8 + 3c_{16}\\
c_{12} &= n_v(v-9)/4 + 12c_{16}\\
c_{13} &= n_v(v^2-18v+85)/48 - 4c_{16}\\
c_{14} &= n_v/4 - 6c_{16}
\end{aligned}$$

2.91 **Theorem** [949, 1472] For every $v \equiv 1,3 \pmod 6$, $v \notin \{7,13\}$, there is an *anti-Pasch* Steiner triple system, an STS(v) in which no four triples are isomorphic to the *Pasch configuration* C_{16}.

2.92 **Theorem** [2164] A *mitre configuration* with 7 points and 5 lines is pictured on the right. There is an *anti-mitre* STS(v) (one that contains no configuration isomorphic to the mitre configuration) if and only if $v \equiv 1,3 \pmod 6$ and $v \neq 9$.



2.93 Theorem [955] Let $P(v)$ be the maximum number of Pasch configurations in a Steiner triple system on v points, and let $M(v) = v(v-1)(v-3)/24$. Then $P(v) \le M(v)$, with equality if and only if $v = 2^{d+1} - 1$ (the STS is projective). Moreover, for $v \neq 2^{d+1} - 1$, $\limsup_{v\to\infty} P(v)/M(v) = 1$.

2.94 Theorem [578] The number of mitres in an STS(v) is at most $v(v-1)(v-3)(v-7)/24$, and equality is attained if and only if v is a power of 3 and the STS(v) is a Hall triple system (see §VI.28).

2.95 For $\ell \ge 2$, an STS(v) is *ℓ-sparse* if there is no set of $\sigma + 2$ points that underlie σ triples for $1 < \sigma \le \ell$.

2.96 Remarks In 1976, Erdős [786] conjectured that an ℓ-sparse STS(v) exists for every integer $\ell \ge 2$. Every STS(v) is 3-sparse. An STS is 4-sparse exactly when it is anti-Pasch; see Theorem 2.91. It is 5-sparse when it is both anti-Pasch and anti-mitre. A 5-sparse STS(v) is known to exist when $v \equiv 3 \pmod 6$ and $v \ge 21$, and for many other orders [2163]. However a complete characterization is not known. Only finitely many 6-sparse STSs are known; see [826]. No ℓ-sparse STS(v) is known for any $\ell \ge 7$.

2.97 An STS(v) $(V, \mathcal{B})$ is *G-uniform* if for every triple $\{x, y, z\}$, the graph on vertex set $V \setminus \{x, y, z\}$ with edges $\{\{a, b\} : \{a, b, w\} \in \mathcal{B}, a, b \in V \setminus \{x, y, z\}, w \in \{x, y\}\}$ is isomorphic to G. When G consists of a single $(v-3)$-cycle, the STS is *perfect*.

2.98 Remark The projective, affine, Hall, and Netto triple systems are all uniform. However perfect systems are known for only 14 orders: 7, 9, 25, 33, 79, 139, 367, 811, 1531, 25771, 50923, 61339, 69991, and 135859 [826].

2.10 Coloring and Independent Sets

2.99 In a set system $(V, \mathcal{B})$, a set $W \subseteq V$ is *independent* if there is no $B \in \mathcal{B}$ with $B \subseteq W$.

2.100 Theorem [268] The size of a largest independent set in a TS(v, λ) is

$$\begin{cases} (v+1)/2 & \text{if} \quad v \equiv 3 \pmod 4 \\ & \text{or} \quad v \equiv 1 \pmod 4 \text{ and } \lambda \equiv 0 \pmod 2, \\ \frac{v}{2} & \text{if} \quad v \equiv 0 \pmod 2, \\ (v-1)/2 & \text{if} \quad v \equiv 1 \pmod 4 \text{ and } \lambda \equiv 1 \pmod 2 \end{cases}$$

2.101 Theorem [1739] The size of the smallest maximum independent set in an STS(v) is bounded below by $c_1\sqrt{v \ln v}$ and above by $c_2\sqrt{v \ln v}$, for absolute constants c_1 and c_2.

2.102 A set system $S = (V, \mathcal{B})$ is *(weakly) m-colorable* if V can be partitioned into m sets, each of which is independent. It is *(weakly) m-chromatic* if it is weakly m-colorable but not weakly $(m-1)$-colorable.

2.103 Theorem [638] For all $m \ge 3$, there exists v_m so that for every $v > v_m$ with $v \equiv 1, 3 \pmod 6$, there exists a weakly m-chromatic STS(v).

2.104 Theorem (see [578]) There is a 3-chromatic STS(v) whenever $v \equiv 1, 3 \pmod 6$.

2.105 Theorem [1004] There is a 4-chromatic STS(v) whenever $v \equiv 1, 3 \pmod 6$ and $v \ge 21$. There is no 4-chromatic STS(v) for $v \le 15$, and the case $v = 19$ is in doubt.

2.11 Decomposability

2.106 Remark Theorem 2.64 constructs triple systems that are *decomposable* into Steiner triple systems. More generally, a $\mathrm{TS}(v,\lambda)$ is decomposable if its block set is the (multiset) union of the block sets of a $\mathrm{TS}(v,\lambda_1)$ and a $\mathrm{TS}(v,\lambda_2)$ with $1 \le \lambda_1 \le \lambda_2 < \lambda$. It is *indecomposable* otherwise. For fixed v, there exist only finitely many indecomposable $\mathrm{TS}(v,\lambda)$s [784].

2.107 Theorem [2204] Whenever $\lambda \equiv 0 \pmod{\gcd(v-2,6)}$ and $v \ge 24\lambda - 5$, an indecomposable, simple $\mathrm{TS}(v,\lambda)$ exists.

2.12 Nested and Derived Triple Systems

2.108 A $\mathrm{TS}(v,\lambda)$ $(V,\mathcal{B})$ is *nested* in (a 2-$(v,4,\lambda)$ design) $(V,\mathcal{D})$ when there is a mapping $\psi : \mathcal{B} \mapsto V$ for which the collection $\{B \cup \{\psi(B)\} : B \in \mathcal{B}\}$ is equal to $\mathcal{D}$.

2.109 Theorem [535, 1965] Whenever there exists a $\mathrm{TS}(v,\lambda)$, there exists a nested $\mathrm{TS}(v,\lambda)$.

2.110 Remarks It is not known whether there is any $\mathrm{TS}(v,\lambda)$ that cannot be nested. Indeed, for $v \equiv 1 \pmod 6$ and $v \le 61$, every $\mathrm{STS}(v)$ admitting a cyclic automorphism can be nested so that the resulting 2-$(v,4,2)$ design shares the same cyclic automorphism.

2.111 Conjecture (Novák [1687]) For $v \equiv 1 \pmod 6$, every $\mathrm{STS}(v)$ admitting a cyclic automorphism can be nested so that the resulting 2-$(v,4,2)$ design shares the same cyclic automorphism.

2.112 Remark (see [578]) Triple systems can also be extended to designs of higher strength t, and can be produced as derived designs of 3-$(v,4,\lambda)$ designs. Every $\mathrm{STS}(v)$ is the derived design of some 3-$(v,4,1)$ design when $v \le 15$. However, it is open whether every $\mathrm{STS}(v)$ is derived for larger values of v.

2.13 Directed and Mendelsohn Triple Systems

2.113 The transitive tuple (x,y,z) *contains* the three ordered pairs (x,y), (x,z), and (y,z). A *directed triple system* $\mathrm{DTS}(v,\lambda)$ is a v-set V and a collection of transitive tuples (*blocks*) each having distinct elements of V for which every ordered pair is contained in exactly λ blocks. The *underlying* $\mathrm{TS}(v,2\lambda)$ is obtained by omitting the ordering.

2.114 Theorem [552] Every $\mathrm{TS}(v,2\lambda)$ underlies a $\mathrm{DTS}(v,\lambda)$.

2.115 The cyclic tuple $\langle x,y,z\rangle$ *contains* the three ordered pairs (x,y), (y,z), and (z,x). A *Mendelsohn triple system* $\mathrm{MTS}(v,\lambda)$ is a v-set V and a collection of cyclic tuples (*blocks*) each having distinct elements of V for which every ordered pair is contained in exactly λ blocks.

2.116 Theorem

1. [1586] An $\mathrm{MTS}(v,\lambda)$ exists if and only if $\lambda v(v-1) \equiv 0 \pmod 3$ and $(v,\lambda) \ne (6,1)$.
2. [523] Not every $\mathrm{TS}(v,2\lambda)$ underlies an $\mathrm{MTS}(v,\lambda)$; indeed, it is NP-complete to decide.

See Also

§I.1	Connections of STS(v)s to other designs.
§I.2	Triple systems are often the first class of designs studied in the history of designs.
§II.1	Existence and enumeration results.
§II.4	Triple systems are obtained by derivation on designs of higher strength t.
§II.5	Steiner quadruple systems are extensions of STSs.
§II.7	Kirkman triple systems are special types of resolvable designs.
§III.2	Steiner triple systems are equivalent to Steiner quasigroups.
§IV.3	Generalizations to pairwise balanced designs.
§IV.4	Existence results for GDDs with block size three.
§VI.2	Balanced ternary designs with block size three.
§VI.3	Triple systems arise in balanced tournament scheduling.
§VI.5	"Large" automorphism groups of triple systems.
§VI.7	More on configurations.
§VI.11	CTs are coverings with block size three.
§VI.12	Triple systems are cycle decompositions with cycle length three.
§VI.13	Defining sets of triple systems.
§VI.16	Cyclic triple systems are difference families with block size three.
§VI.20	Directed triple systems.
§VI.24	Triple systems are graph decompositions into triangles.
§VI.25	Embeddings of triple systems on surfaces.
§VI.28	Hall triple systems are STSs in which every three points not on a triple generate an sub-STS(9).
§VI.30	Triple systems on an infinite number of points.
§VI.33.1	KTSs are used to produce low density parity check codes.
§VI.35	Mendelsohn triple systems.
§VI.36	Nested triple systems are a class of nested designs.
§VI.40	PTSs are packings with block size three.
§VI.53	Skolem sequences are used to construct triple systems.
§VI.56	STSs are used to produce cover-free families.
§VI.51	Triple systems arise in tournament scheduling.
§VI.60	Trades are used extensively to prove theorems on support and intersection.
§VII.1	Point codes and block codes of STSs.
§VII.5	STSs are equivalent to Steiner 1-factorizations of graphs.
§VII.6	Many algorithmic techniques and complexity results have been established for triple systems.
§VII.7	Connections with linear algebra.
[578]	A comprehensive introduction to triple systems.

References Cited: [78, 130, 267, 268, 361, 442, 523, 524, 535, 541, 549, 551, 552, 556, 561, 565, 569, 570, 571, 573, 574, 578, 581, 589, 638, 690, 712, 745, 747, 784, 785, 786, 787, 826, 945, 949, 955, 970, 1004, 1268, 1300, 1423, 1462, 1464, 1472, 1482, 1483, 1484, 1586, 1603, 1668, 1670, 1687, 1737, 1739, 1741, 1781, 1792, 1957, 1965, 2008, 2009, 2011, 2015, 2095, 2163, 2164, 2204]

3 BIBDs with Small Block Size

R. Julian R. Abel
Malcolm Greig

3.1 Existence Results for BIBDs for Specific k and λ

3.1 Remarks The existence question for BIBDs with small k is: Given k and λ, for what values of v are Proposition II.1.2 (integrality conditions) and Theorem II.1.9 (Fisher's inequality) sufficient? This problem has been addressed for all λ when $k \leq 9$. For $k \geq 10$, much less is known, although for some such k, there are known bounds on v for existence of near-resolvable BIBD$(v, k, k-1)$s (and hence also BIBD$(v, k, k+1)$s with $v \equiv 1 \pmod{k}$; see §II.7.5).

The notation B(k, λ) is used for the set of v values for which a BIBD(v, k, λ) is known. Theorem IV.3.7 establishes that, for every fixed k and λ, there is a constant $C(k, \lambda)$, so that if $v > C(k, \lambda)$ and v satisfies $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$, then there exists a BIBD(v, k, λ). Table 3.3 summarizes the known results for $k \leq 9$.

3.2 Proposition For any v, k, if $\lambda_{\min}$ is the minimum λ for which the integrality conditions are satisfied, then $\lambda_{\min}$ divides $k(k-1)$ (if k is odd) or $k(k-1)/2$ (if k is even).

3.3 Table A summary of known results.

k, λ	Reference	Possible Values of v	Exceptions	Possible Exceptions	Largest Possible Exception
3,1	[1042]	1,3 mod 6	none	none	
3,2	[1042]	0,1 mod 3	none	none	
3,3	[1042]	1 mod 2	none	none	
3,6	[1042]	all	none	none	
4,1	[1042]	1,4 mod 12	none	none	
4,2	[1042]	1 mod 3	none	none	
4,3	[1042]	0,1 mod 4	none	none	
4,6	[1042]	all	none	none	
5,1	[1042]	1,5 mod 20	none	none	
5,2	[1042]	1,5 mod 10	15	none	
5,4	[1042]	0,1 mod 5	none	none	
5,5	[1042]	1 mod 4	none	none	
5,10	[1042]	1 mod 2	none	none	
5,20	[1042]	all	none	none	
6,1	[41, 46, 1138]	1,6 mod 15	16,21,36,46	Table 3.4	801
6,2	[1042]	1,6 mod 15	21	none	
6,3	[1042]	1 mod 5	none	none	
6,5	[1042]	0,1 mod 3	none	none	
6,15	[1042]	all	none	none	

k, λ	Reference	Possible Values of v	Exceptions	Possible Exceptions	Largest Possible Exception
7,1	[3, 4, 961, 1184]	1,7 mod 42	43	Tables 3.5, 3.6	2605
7,2	[4, 42]	1,7 mod 21	22	Table 3.7	994
7,3	[42, 1044, 2194, 2214]	1,7 mod 14	none	none	
7,6	[1042]	0,1 mod 7	none	none	
7,7	[1042]	1 mod 6	none	none	
7,14	[42]	1 mod 3	none	none	
7,21	[42, 1044]	1 mod 2	none	none	
7,42	[1042]	all	none	none	
8,1	[3, 961]	1,8 mod 56	none	Tables 3.8, 3.9	3753
8,2	[19]	1,8 mod 28	29,36	Table 3.10	589
8,4	[19, 1372]	1 mod 7	22	none	
8,7	[19, 2182]	0,1 mod 8	none	none	
8,14	[19]	0,1 mod 4	none	none	
8,28	[19]	0,1 mod 2	none	none	
8,56	[19]	all	none	none	
9,1	[3, 961]	1,9 mod 72	none	Tables 3.11, 3.12	16497
9,2	[20]	1,9 mod 36	none	Table 3.13	1845
9,3	[21]	1,9 mod 24	none	Table 3.13	385
9,4	[20]	1,9 mod 18	none	Table 3.13	783
9,6	[21]	1,9 mod 12	none	Table 3.13	213
9,8	[20]	0,1 mod 9	none	none	
9,9	[34]	1 mod 8	none	none	
9,12	[21]	1,3 mod 6	none	none	
9,18	[22]	1 mod 4	none	none	
9,24	[22]	0,1 mod 3	none	none	
9,36	[22]	1 mod 2	none	none	
9,72	[22]	all	none	none	

3.4 Table Values of v for which existence of a BIBD$(v, 6, 1)$ remains undecided.

51 61 81 166 226 231 256 261 286 316 321
346 351 376 406 411 436 441 471 501 561 591
616 646 651 676 771 796 801

3.5 Table Values of t for which existence of a BIBD$(42t + 1, 7, 1)$ remains undecided.

2 3 5 6 12 14 17 19 22 27 33 37 39 42 47 59 62

3.6 Table Values of t for which existence of a BIBD$(42t + 7, 7, 1)$ remains undecided.

3 19 34 39

3.7 Table Values of v for which existence of a BIBD$(v, 7, 2)$ remains undecided.

274 358 574 694 988 994

3.8 Table Values of t for which existence of a BIBD$(56t + 1, 8, 1)$ remains undecided.

2 3 4 5 6 7 14 19 20 21 22 24 25 26
27 28 31 32 34 35 39 40 46 52 59 61 62 67

3.9 Table Values of t for which existence of a BIBD$(56t + 8, 8, 1)$ remains undecided.

3 11 13 20 22 23 25 26 27 28

3.10 **Table** Values of v, λ with $\lambda > 1$ for which existence of a BIBD$(v, 8, \lambda)$ remains undecided. There is no BIBD for $(v, k, \lambda) = (22, 8, 4)$, $(29, 8, 2)$, or $(36, 8, 2)$.

v	λ	v	λ	v	λ	v	λ	v	λ	v	λ
365	2	393	2,5	477	2	484	2	533	2	540	2
589	2	785	3,5	1121	3,5	1128	3,5	1177	3,5		

3.11 **Table** Values of t for which existence of a BIBD$(72t + 1, 9, 1)$ remains undecided.

2	3	4	5	7	11	12	15	20	21	22	24	27	31
32	34	37	38	40	42	43	45	47	50	52	53	56	60
61	62	67	68	75	76	84	92	94	96	102	132	174	191
194	196	201	204	209									

3.12 **Table** Values of t for which existence of a BIBD$(72t + 9, 9, 1)$ remains undecided.

2	3	4	5	12	13	14	18	22	23	25	26	27	28	31
33	34	38	40	41	43	46	47	52	59	61	62	67	68	76
85	93	94	102	103	139	148	174	183	192	202	203	209	229	

3.13 **Table** Values (v, k, λ) with $\lambda > 1$ for which existence of a BIBD$(v, 9, \lambda)$ remains undecided.

(177,9,3)	(189,9,2)	(213,9,6)	(253,9,2)	(315,9,4)
(345,9,3)	(385,9,3)	(459,9,4)	(505,9,2)	(765,9,2)
(783,9,4)	(837,9,2)	(1197,9,2)	(1837,9,2)	(1845,9,2)

3.14 **Table** Parameter sets (v, k, λ) with $\lambda(v - 1) \equiv 0 \pmod{(k - 1)}$, $\lambda v(v - 1) \equiv 0 \pmod{k(k - 1)}$, $v \leq 43$ and $k \leq v/2$ for which no BIBD exists. These nonexistence results are generally due to Fisher's inequality or to the known necessary conditions for symmetric and quasi-residual designs. The nonexistence of a $(22, 8, 4)$ design was shown by computer search [1372].

Fisher:	(16,6,1)	(21,6,1)	(25,10,3)	(34,12,2)	(36,15,2)	(36,15,4)
Symmetric:	(22,7,2)	(29,8,2)	(34,12,4)	(43,7,1)	(43,15,5)	
Quasi residual:	(15,5,2)	(21,6,2)	(36,6,1)	(22,8,4)	(36,8,2)	

3.15 **Remark** The only BIBD(v, k, λ)s with $v \leq 43$ and $k \leq v/2$ whose existence remains unsolved have the parameters: (39,13,6), (40,14,7), and (42,10,3).

3.16 **Remark** There exists a k-GDD of type $k^{t(k-1)+1}$ (or equivalently, a BIBD$(k(k-1)t + k, k, 1)$ containing a parallel class) if any one of the following conditions is satisfied:

1. $k \leq 5$.
2. $k = 6$ and $t \neq 1$, 2, 7, 9, 11, 39, 50, or 51.
3. $k = 7$, t is not in Table 3.6, and $t \neq 24$.
4. $k = 8$ and t is not in Table 3.9.
5. $k = 9$, t is not in Table 3.12, and $t \neq 16$, 20, 48, 60, 92, 104, 147, 166, 187, 191, or 205.

3.17 **Remark** k-GDDs of type $(k(k-1))^t$ can sometimes be useful for BIBD constructions. For $k = 3, 4$, and 5, k-GDDs of type $(k(k-1))^t$ exist for all $t \geq k$. For $k = 6$, not much is known, as most recursive constructions require the existence of k-GDDs of types $(k(k-1))^x$ and $(k(k-1))^{x+1}$ for some small value of x; at present, none is known for $k = 6$. Tables 3.18 through 3.21 summarize known results for $k \in \{6, 7, 8, 9\}$ and $t < 100$.

3.18 **Table** Values of $t < 100$ for which existence of a 6-GDD of type 30^t is known.

6	16	21	26	31	36	41	51	61	66	71	76	78	81	86	90	91	96

3.19 Table Values of $t < 100$ for which existence of a 7-GDD of type 42^t is known.

7	8	9	15	17	28	33	36	41	49	50	56	57	63	64	65	70	71
72	73	77	78	80	81	85	88	91	92	96	97	99					

3.20 Table Values of $t < 100$ for which existence of a 8-GDD of type 56^t is known.

8	9	10	15	16	17	29	30	33	36	37	41	43	44	49	50	51	53
54	55	57	58	63	64	65	71	72	73	74	79	80	81	82	83	84	85
86	87	88	89	90	91	92	93	94	95	96	97	98	99				

3.21 Table Values of $t < 100$ for which existence of a 9-GDD of type 72^t is known.

9	10	17	19	49	54	55	57	58	64	65	66	73	74	80	81	89	90	91

3.2 Recursive Constructions

3.22 Theorem A BIBD(v, k, λ) exists if any one of the following conditions holds:

1. $v = w + r/\lambda$, where there exist a BIBD$(r/\lambda, k, \lambda)$ and an RBIBD$(w, k-1, \lambda)$ whose blocks form r parallel classes.
2. $v = (w-1)m + 1$, $\lambda = \lambda_1\lambda_2$, where a (k, λ_1)-GDD of type $(k-1)^{(w-1)/(k-1)}$, a BIBD$((k-1)m+1, k, \lambda_1\lambda_2)$, and TD$_{\lambda_2}(k, m)$ exist.
3. $v = v_1(v_2 - \alpha) + \alpha$, $\lambda = \lambda_1\lambda_2$ where α is 0 or 1, a TD$_{\lambda_2}(k, v_2 - \alpha)$ exists, and BIBD(v_1, k, λ_1) and BIBD(v_2, k, λ) both exist.

3.23 Remark Most recursive BIBD constructions start with a GDD (usually a truncated transversal design), use Wilson's Fundamental GDD construction (Theorem IV.2.5, using Remark IV.2.6) to obtain a larger GDD, and finally fill in the groups of the larger GDD. Some examples follow.

3.24 Example Suppose TD$(10, t)$ exists and $0 \le u \le t$. Then a $\{9, 10\}$-GDD of type t^9u^1 exists, and because 9-GDD of type 8^x exists for $x \in \{9, 10\}$, a 9-GDD of type $(8t)^9(8u)^1$ also exists. Therefore, if $\alpha = 1$ or 9 and $\{8t + \alpha, 8u + \alpha\} \subset$ B$(9, 1)$, then $8(9t + u) + \alpha \in$ B$(9, 1)$.

3.25 Example Suppose TD$(9, t)$ exists and $0 \le u \le t$. Then a $\{8, 9\}$-GDD of type t^8u^1 exists, and because a 7-GDD of type 42^x exists for $x \in \{8, 9\}$, a 7-GDD of type $(42t)^8(42u)^1$ also exists. Therefore, if $\alpha = 1$ or 7 and $\{42t + \alpha, 42u + \alpha\} \subset$ B$(7, 1)$, then $42(8t + u) + \alpha \in$ B$(7, 1)$.

3.26 Example Suppose TD$(8, t)$ exists and $0 \le u \le t$. Then a $\{7, 8\}$-GDD of type t^7u^1 exists, and because a $(7, 3)$-GDD of type 2^x exists for $x \in \{7, 8\}$, a $(7, 3)$-GDD of type $(2t)^7(2u)^1$ also exists. Therefore, if $\{2t + 1, 2u + 1\} \subset$ B$(7, 3)$, then $2(7t + u) + 1 \in$ B$(7, 3)$.

3.27 Example Suppose TD$(9, t)$ exists and $0 \le u, w \le t$. Then a $\{7, 8, 9\}$-GDD of type $t^7u^1w^1$ exists, and because $(7, 21)$-GDDs of type 2^x exist for $x \in \{7, 8, 9\}$, a $(7, 21)$-GDD of type $(2t)^7(2u)^1(2w)^1$ also exists. Therefore, if $\{2t + 1, 2u + 1, 2w + 1\} \subset$ B$(7, 21)$, then $2(7t + u + w) + 1 \in$ B$(7, 21)$.

3.28 Example Suppose there exists an RBIBD$(w, k, 1)$ whose blocks form r parallel classes. Then if $x \le r$, adding each of x infinite points to a different parallel class gives a $\{k, k+1\}$-GDD of type 1^wx^1. If $k, k-1$ are prime powers, then k-GDDs of type $(k-1)^t$ exist for $t = k, k+1$; hence, a k-GDD of type $(k-1)^w((k-1)x)^1$ exists. Therefore, if $(k-1)x + 1 \in$ B$(k, 1)$, then $(k-1)(w + x) + 1 \in$ B$(k, 1)$.

3.29 **Remark** Theorem 3.30, the singular indirect product or incomplete TD construction, has been useful for BIBDs with $k \geq 6$ and $\lambda = 1$.

3.30 **Theorem** Suppose $v = k(w-f)+(f+(k-1)\cdot a)$ where a TD$(k, w-f+a)$−TD(k,a), a PBD$(w, \{k\} \cup f^*, 1)$ and a BIBD$(f+(k-1)a, k, 1)$ all exist. Then $v \in$ B$(k,1)$. If, in addition, a k-GDD of type $k^{(f+(k-1)a)/k}$ and TD$(k, w-f+a)$−TD$(k,a) - (w-f)\cdot$TD$(k,1)$ exist, then so does a k-GDD of type $k^{v/k}$.

3.31 **Examples**

1. Because an RBIBD(65,5,1) exists, there is a PBD$(81, \{6\}\cup 16^*)$. A BIBD$(76,6,1)$ and a TD$(6,77)$−TD$(6,12)$ also exist; hence there exists a BIBD$(v,6,1)$ for $v = 466 = 6(81-16) + (76 = 16 + 5\cdot 12)$.
2. Because an RBIBD$(28,4,1)$ exists, a PBD$(37, \{5\}\cup 9^*)$ also exists. A 5-GDD of type 5^5 and a TD$(5,32)$−TD(5,4)−28·TD$(5,1)$ also exist; this gives a 5-GDD of type $5^{v/5}$ for $v = 165 = 5(37-9) + (25 = 9 + 4\cdot 4)$.

3.3 Miscellaneous Constructions

3.32 **Table** Most of these constructions have nonabelian automorphism groups. In each case, the table includes the parameters (v,k,λ), the point set X, the order of the automorphism group G, suitable generators of this group, and a set of base blocks to be developed using G. If s is the order of the largest subgroup of G that leaves a base block invariant, then that base block generates a total of $|G|/s$ blocks in the BIBD.

(v,k,λ)	Solution
$(21,6,4)$	$X = \mathbb{Z}_7 \times \mathbb{Z}_3$, $\lvert G\rvert = 21$. Generating automorphisms (for $x \in \mathbb{Z}_7$, $s = 0,1,2$): $\alpha = (x_s, 2x_s, 4x_s)$, $\beta = (0_s, 1_s, 2_s, \ldots, 6_s)$. Base blocks: $(0_0, 5_0, 3_1, 3_2, 5_2, 6_2)$, $(0_0, 1_0, 2_0, 4_0, 3_1, 6_2)$, $(0_0, 1_0, 0_1, 2_1, 0_2, 4_2)$, $(0_0, 3_0, 0_1, 6_1, 0_2, 5_2)$.
$(66,6,1)$	$X = \mathbb{Z}_{13} \times (\mathbb{Z}_3 \cup \{a,b\}) \cup \{\infty\}$, $\lvert G\rvert = 39$. Generating automorphisms (for $x \in \mathbb{Z}_{13}$, $t = a,b$, $s \in \mathbb{Z}_3 \cup \{a,b\}$): $\alpha = (\infty), (x_0, 3x_1, 9x_2), (x_t, 3x_t, 9x_t)$, $\beta = (\infty), (0_s, 1_s, 2_s, \ldots, 12_s)$. Base blocks: $(2_0, 5_0, 4_1, 9_1, 0_a, 6_a)$, $(1_0, 2_0, 6_0, 12_2, 5_b, 8_b)$, $(7_0, 9_0, 10_1, 1_2, 3_a, 4_b)$, $(2_a, 6_a, 5_a, 4_b, 12_b, 10_b)$, $(\infty, 0_0, 0_1, 0_2, 0_a, 0_b)$.
$(76,6,1)$	$X = \mathbb{Z}_{19} \times (\mathbb{Z}_3 \cup \{a\})$, $\lvert G\rvert = 57$. Generating automorphisms (for $x,y \in \mathbb{Z}_{19}$, $s \in \mathbb{Z}_3 \cup \{a\}$): $\alpha = (x_0, 7x_1, 11x_2)$, $(y_a, 7y_a, 11y_a)$, $\beta = (0_s, 1_s, 2_s, \ldots, 18_s)$. Base blocks: $(0_0, 1_0, 3_0, 14_0, 10_2, 0_a)$, $(0_0, 7_0, 0_1, 2_2, 1_a, 3_a)$, $(3_0, 2_1, 14_2, 1_a, 7_a, 11_a)$, $(12_0, 8_1, 18_2, 3_a, 2_a, 14_a)$, $(7_0, 16_0, 11_1, 17_1, 1_2, 5_2)$, $(13_0, 17_0, 15_1, 5_1, 10_2, 16_2)$.
$(96,6,1)$	$X = \mathbb{Z}_{48} \times \{0,1\}$, $\lvert G\rvert = 48$. Generating automorphisms (for $s = 0,1$): $\alpha = (0_s, 1_s, 2_s, \ldots, 47_s)$. Base blocks: $(0_0, 8_0, 16_0, 24_0, 32_0, 40_0)$, $(0_1, 8_1, 16_1, 24_1, 32_1, 40_1)$, $(0_0, 1_0, 3_0, 13_0, 28_0, 0_1)$, $(0_0, 4_0, 11_0, 17_1, 36_1, 38_1)$, $(0_0, 5_0, 19_0, 1_1, 24_1, 42_1)$, $(0_0, 9_0, 26_0, 4_1, 7_1, 40_1)$, $(0_0, 6_0, 8_1, 9_1, 18_1, 22_1)$, $(0_0, 18_0, 11_1, 28_1, 33_1, 39_1)$.

(v,k,λ)	Solution
$(106,6,1)$	$X=\mathbb{Z}_{53}\times\{0,1\}$, $\lvert G\rvert=53$. Generating automorphisms (for $s=0,1$): $\alpha=(0_s,1_s,2_s,\ldots,52_s)$. Base blocks: $(0_0,1_0,3_0,11_0,38_0,0_1)$, $(0_0,13_0,30_0,23_1,35_1,51_1)$, $(0_0,5_0,19_0,25_0,36_1,39_1)$, $(0_0,4_0,28_1,30_1,37_1,47_1)$, $(0_0,7_0,29_0,8_1,16_1,48_1)$, $(0_0,2_1,7_1,25_1,29_1,49_1)$, $(0_0,9_0,21_0,12_1,13_1,27_1)$.
$(111,6,1)$	$X=\mathbb{Z}_{37}\times\mathbb{Z}_3$, $\lvert G\rvert=111$. Generating automorphisms (for $x\in\mathbb{Z}_{37}$, $s=0,1,2$): $\alpha=(x_0,10x_1,26x_2)$, $\beta=(0_s,1_s,2_s,\ldots,36_s)$. Base blocks: $(0_0,1_0,3_0,7_0,17_0,0_1)$, $(0_0,5_0,19_1,28_1,10_2,30_2)$, $(5_0,33_0,13_1,34_1,19_2,7_2)$, $(9_0,27_0,16_1,11_1,12_2,36_2)$, $(10_0,23_0,26_1,8_1,1_2,6_2)$, $(13_0,24_0,19_1,18_1,5_2,32_2)$, $(26_0,34_0,1_1,7_1,10_2,33_2)$.
$(136,6,1)$	$X=(\mathbb{Z}_{45}\times\mathbb{Z}_3)\cup\{\infty\}$, $\lvert G\rvert=135$. Generating automorphisms (for $x\in\mathbb{Z}_{45}$, $s=0,1,2$): $\alpha=(\infty),(x_0,16x_1,31x_2)$, $\beta=(\infty),(0_s,1_s,2_s,\ldots,44_s)$. Base blocks: $(0_0,3_0,15_0,35_0,6_2,10_2)$, $(0_0,22_0,11_1,30_1,1_2,18_2)$, $(0_0,5_0,18_1,41_1,13_2,42_2)$, $(0_0,11_0,17_0,4_2,5_2,28_2)$, $(0_0,1_0,0_1,16_1,0_2,31_2)$, $(\infty,0_0,9_0,18_0,27_0,36_0)$.
$(141,6,1)$	$X=(\mathbb{Z}_{35}\times(\mathbb{Z}_3\cup\{a\}))\cup\{\infty\}$, $\lvert G\rvert=105$. Generating automorphisms (for $x,y\in\mathbb{Z}_{35}$, $s\in\mathbb{Z}_3\cup\{a\}$): $\alpha=(\infty),(x_0,16x_1,11x_2),(y_a,16y_a,11y_a)$, $\beta=(\infty),(0_s,1_s,2_s,\ldots,34_s)$. Base blocks: $(0_0,16_0,24_0,24_1,15_2,25_2)$, $(0_0,3_0,26_0,13_1,33_1,34_a)$, $(0_0,13_0,18_0,15_1,7_2,0_a)$, $(0_0,2_0,14_1,23_1,26_a,32_a)$, $(0_0,4_0,29_1,6_2,9_a,20_a)$, $(0_0,1_0,12_2,2_a,4_a,19_a)$, $(\infty,0_0,7_0,14_0,21_0,28_0)$, $(\infty,0_a,7_a,14_a,21_a,28_a)$.
$(171,6,1)$	$X=\mathbb{Z}_{57}\times\mathbb{Z}_3$, $\lvert G\rvert=171$. Generating automorphisms (for $x\in\mathbb{Z}_{57}$, $s=0,1,2$): $\alpha=(x_0,7x_1,49x_2)$, $\beta=(0_s,1_s,2_s,\ldots,56_s)$. Base blocks: $(0_0,19_0,39_0,41_0,14_1,38_2)$, $(0_0,21_0,44_0,48_0,26_1,11_2)$, $(0_0,1_0,43_0,8_2,15_2,44_2)$, $(0_0,3_0,31_0,23_1,43_1,36_2)$, $(0_0,40_0,50_0,11_1,25_2,34_2)$, $(0_0,12_0,0_1,27_1,0_2,18_2)$, $(37_0,42_0,31_1,9_1,46_2,6_2)$.
$(196,6,1)$	$X=\mathbb{Z}_{49}\times(\mathbb{Z}_3\cup\{a\})$, $\lvert G\rvert=147$. Generating automorphisms (for $x,y\in\mathbb{Z}_{49}$, $s\in\mathbb{Z}_3\cup\{a\}$): $\alpha=(x_0,30x_1,18x_2),(y_a,30y_a,18y_a)$, $\beta=(0_s,1_s,2_s,\ldots,48_s)$. Base blocks: $(0_0,2_0,12_0,45_0,3_1,11_a)$, $(0_0,3_0,8_0,5_1,17_1,39_a)$ $(0_0,9_0,36_0,24_1,44_1,37_a)$, $(0_0,15_0,34_1,41_1,47_2,18_a)$ $(0_0,7_0,31_0,13_1,35_2,41_a)$, $(0_0,14_0,32_1,10_2,22_a,44_a)$ $(0_0,23_0,21_1,39_1,19_a,25_a)$, $(0_0,33_1,0_a,5_a,29_a,47_a)$, $(0_0,1_0,0_1,30_1,0_2,18_2)$, $(8_0,19_0,44_1,31_1,46_2,48_2)$.
$(201,6,1)$	$X=\mathbb{Z}_{67}\times\mathbb{Z}_3$, $\lvert G\rvert=201$. Generating automorphisms (for $x\in\mathbb{Z}_{67}$, $s=0,1,2$): $\alpha=(x_s,29x_s,37x_s)$, $\beta=(0_s,1_s,2_s,\ldots,66_s)$. Base blocks: $(0_0,1_0,4_2,9_2,34_2,62_2)$, $(0_1,2_1,15_1,8_2,27_2,49_2)$, $(0_0,3_0,22_0,54_1,13_2,40_2)$, $(0_0,36_0,40_0,31_1,34_1,5_2)$, $(0_0,50_0,55_0,6_1,24_1,26_2)$, $(0_0,2_0,3_1,14_1,35_1,25_2)$, $(3_1,20_1,44_1,36_2,39_2,59_2)$, $(0_0,0_1,30_1,38_1,66_1,0_2)$.

(v,k,λ)	Solution
$(35,7,3)$	$X=\mathbb{Z}_7\times(\mathbb{Z}_3\cup\{a,b\})$, $\lvert G\rvert=21$. Generating automorphisms (for $x\in\mathbb{Z}_7,\ t=a,b,\ s\in\mathbb{Z}_3\cup\{a,b\}$): $\alpha=((x_0,2x_1,4x_2),(x_t,2x_t,4x_t)$, $\beta=(0_s,1_s,2_s,\ldots,6_s)$. Base blocks: $(5_1,0_0,1_0,4_a,5_a,3_b,5_b)$, $(3_1,5_1,6_1,6_2,2_a,3_a,5_b)$, $(1_1,2_1,4_1,6_2,1_0,6_a,3_b)$, $(2_1,6_1,4_2,5_2,1_0,3_0,0_b)$, $(5_1,6_1,3_2,5_2,6_0,3_0,0_a)$, $(4_1,1_2,2_0,0_b,1_b,2_b,4_b)$, $(0_a,1_a,2_a,3_a,4_a,5_a,6_a)$.
$(64,7,2)$	$X=(\mathbb{Z}_{19}\times\mathbb{Z}_3)\cup\{\infty_1,\infty_2,\ldots,\infty_7\}$, $\lvert G\rvert=57$. Generating automorphisms (for $x\in\mathbb{Z}_{19},\ i=1,2,\ldots,7,\ s=0,1,2$): $\alpha=(\infty_i),(x_0,7x_1,11x_2)$, $\beta=(\infty_i),(0_s,1_s,2_s,\ldots,18_s)$. Base blocks: $(0_0,10_0,12_0,14_0,18_0,0_1,2_1)$, $(\infty_1,1_0,7_0,7_1,11_1,11_2,1_2)$, $(\infty_2,1_0,8_0,7_1,18_1,11_2,12_2)$, $(\infty_3,9_0,10_0,6_1,13_1,4_2,15_2)$, $(\infty_4,9_0,14_0,6_1,3_1,4_2,2_2)$, $(\infty_5,12_0,15_0,8_1,10_1,18_2,13_2)$, $(\infty_6,2_0,13_0,14_1,15_1,3_2,10_2)$, $(\infty_7,4_0,14_0,9_1,3_1,6_2,2_2)$, $(\infty_1,\infty_2,\infty_3,\infty_4,\infty_5,\infty_6,\infty_7)$ (twice).
$(36,8,4)$	$X=\mathbb{Z}_7\times(\mathbb{Z}_3\cup\{a,b\})$, $\lvert G\rvert=21$. Generating automorphisms (for $x\in\mathbb{Z}_7,\ t=a,b,\ s\in\mathbb{Z}_3\cup\{a,b\}$): $\alpha=(\infty),(x_0,2x_1,4x_2),(x_t,2x_t,4x_t)$, $\beta=(\infty),(0_s,1_s,2_s,\ldots,6_s)$. Base blocks: $(0_1,1_1,6_2,1_0,6_0,5_a,0_b,5_b)$, $(4_1,5_1,4_0,6_0,0_a,1_a,4_b,6_b)$, $(3_1,5_1,6_1,4_2,5_0,4_a,5_a,1_b)$, $(1_1,6_1,2_2,5_2,4_0,3_0,0_a,0_b)$, $(\infty,4_1,6_1,1_2,5_2,2_0,3_0,0_b)$, $(\infty,3_1,6_2,5_0,3_a,5_a,6_a,0_b)$, $(\infty,0_t,1_t,2_t,3_t,4_t,5_t,6_t)$, $(t=1,a)$ $(\infty,0_b,1_b,2_b,3_b,4_b,5_b,6_b)$ (twice).
$(57,9,3)$	$X=\mathbb{Z}_{19}\times\mathbb{Z}_3$, $\lvert G\rvert=57$. Generating automorphisms (for $x\in\mathbb{Z}_{19},\ s=0,1,2$): $\alpha=(x_0,7x_1,11x_2)$, $\beta=(0_s,1_s,2_s,\ldots,18_s)$. Base blocks: $(0_0,1_0,3_0,5_0,13_0,3_1,11_1,2_2,14_2)$, $(0_0,2_0,5_0,6_0,9_0,0_1,13_1,10_2,17_2)$, $(4_0,9_0,10_0,9_1,6_1,13_1,6_2,4_2,15_2)$.
$(105,9,3)$	$X=\mathbb{Z}_{35}\times\mathbb{Z}_3$, $\lvert G\rvert=105$. Generating automorphisms (for $x\in\mathbb{Z}_{35},\ s=0,1,2$): $\alpha=(x_s,11x_s,16x_s)$, $\beta=(0_s,1_s,2_s,\ldots,34_s)$. Base blocks: $(0_0,5_0,13_0,8_1,14_1,29_1,12_2,19_2,21_2)$, $(0_0,9_0,13_0,1_1,5_1,8_1,9_1,28_1,22_2)$, $(0_0,1_0,8_0,20_0,34_0,6_1,0_2,5_2,16_2)$, $(0_0,2_1,3_1,5_1,2_2,4_2,20_2,25_2,33_2)$, $(1_0,11_0,16_0,3_1,33_1,13_1,4_2,9_2,29_2)$.
$(64,10,5)$	$X=(\mathbb{Z}_{21}\times\mathbb{Z}_3)\cup\{\infty\}$, $\lvert G\rvert=63$. Generating automorphisms (for $x\in\mathbb{Z}_{21},\ s=0,1,2$): $\alpha=(x_0,4x_1,16x_2)$, $\beta=(0_s,1_s,2_s,\ldots,20_s)$. Base blocks: $(0_0,1_0,3_0,6_0,14_0,3_1,4_1,13_1,19_1,19_2)$, $(0_0,2_0,6_0,19_0,14_1,19_1,1_2,2_2,11_2,16_2)$, $(0_0,9_0,12_0,19_0,20_0,2_1,5_1,6_1,8_1,5_2)$, $(\infty,5_0,10_0,15_0,20_1,19_1,18_1,17_2,13_2,9_2)$, $(\infty,1_0,8_0,15_0,4_1,11_0,18_1,16_2,2_2,9_2)$, $(\infty,3_0,10_0,17_0,12_1,19_1,5_1,6_2,13_2,20_2)$.
$(35,14,13)$	$X=\mathbb{Z}_7\times(\mathbb{Z}_3\cup\{a,b\})$, $\lvert G\rvert=21$. Generating automorphisms (for $x\in\mathbb{Z}_7,\ t=a,b,\ s\in\mathbb{Z}_3\cup\{a,b\}$): $\alpha=(x_0,2x_1,4x_2),(x_t,2x_t,4x_t)$, $\beta=(0_s,1_s,2_s,\ldots,6_s)$. Base blocks: $(1_1,2_1,4_1,1_2,2_2,6_2,1_0,0_a,1_a,4_a,5_a,2_b,4_b,5_b)$, $(1_1,2_1,4_1,6_2,1_0,4_0,5_0,6_0,2_a,3_a,6_a,1_b,4_b,6_b)$, $(0_1,3_1,5_1,6_1,0_2,1_2,2_2,5_2,1_0,3_a,2_b,3_b,4_b,6_b)$, $(0_1,1_1,2_1,4_1,3_2,5_2,6_2,3_0,5_0,6_0,0_a,3_a,6_a,2_b)$, $(0_a,1_a,2_a,3_a,4_a,5_a,6_a,0_b,1_b,2_b,3_b,4_b,5_b,6_b)$.

See Also

§II.6	Nonexistence results for symmetric and quasi-residual BIBDs.
§II.7	Resolvable designs are used in some recursive constructions for nonresolvable designs.
§VI.16	Difference family constructions provide most of the small ingredients needed for recursive constructions.
§VII.2	Several BIBDs come from special structures in affine and projective geometries.
[225]	An extensive textbook presentation of direct and recursive construction for BIBDs.
[1042]	A major paper, proving existence results for $k \leq 5$, for $k = 6$ with $\lambda \neq 1$, and for $k = 7$ with $\lambda \in \{6, 7, 42\}$.

References Cited: [3, 4, 19, 20, 21, 22, 34, 41, 42, 46, 225, 961, 1042, 1044, 1138, 1184, 1372, 2182, 2194, 2214]

4 t-Designs with $t \geq 3$

Gholamreza B. Khosrovshahi
Reinhard Laue

4.1 Definitions

4.1 A t-(v, k, λ) *design*, a t-design in short, is a pair $(X, \mathcal{B})$ where X is a v-set of *points* and $\mathcal{B}$ is a collection of k-subsets of X (*blocks*) with the property that every t-subset of X is contained in exactly λ blocks. The parameter λ is the *index* of the design.

4.2 A t-(v, k, λ) design is also denoted by $S_\lambda(t, k, v)$. If $\lambda = 1$, then λ is usually omitted.

4.3 **Remark** A 2-(v, k, λ) design is a *balanced incomplete block design*. See §II.1. A design is *simple* if no two blocks are identical.

4.4 **Example** Let $X = \{1, \ldots, 6\}$. Let $\mathcal{B} = \{124, 126, 134, 135, 156, 235, 236, 245, 346, 456\}$. Then $(X, \mathcal{B})$ is a 2-$(6, 3, 2)$ design.

4.5 **Example** Let X be the set of corner points of a cube. Consider two kinds of blocks: The first kind consists of any corner point and its three neighbors; The second kind consists of any two neighbors and their antipodes. Hence, there are altogether $8+6 = 14$ blocks. Any choice of three corner points can be completed in a unique way to exactly one block. These blocks $\mathcal{B}$, together with X form a 3-$(8, 4, 1)$ design.

4.6 **Example** Let $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b\}$ and choose the 30 base blocks, shown with braces and commas omitted:

045678 023456 012346 023567 014567 014568 012568 023578 024569 014569
024579 02346a 01245a 02347a 02457a 03468b 02345b 01245b 01246b 02356b
01458b 01248b 04567b 02348b 02458b 04569b 02459b 03469b 0456ab 0235ab

Applying the automorphism $(0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ a)(b)$ yields 330 blocks that form a 4-$(12, 6, 10)$ design.

4.7 **Remark** The 4-$(12, 6, 10)$ design from Example 4.6 is the basis of *Block Design for Piano* [1211]. The composer explains: "There are 12 notes, distributed into 6-note

arpeggios, in such a way that every combination of four particular notes comes together exactly 10 times in 10 different arpeggios."

4.2 Properties and Theorems

4.8 **Theorem** If $(X, \mathcal{B})$ is a t-(v, k, λ) design and S is any s-subset of X, with $0 \leq s \leq t$, then the number of blocks containing S is

$$\lambda_s = |\{B \in \mathcal{B} : S \subseteq B\}| = \lambda \tbinom{v-s}{t-s} \Big/ \tbinom{k-s}{t-s}.$$

In particular λ_s is an integer and $(X, \mathcal{B})$ is a s-(v, k, λ_s) design for all $0 \leq s \leq t$. The number of blocks of a t-(v, k, λ) design is $b = \lambda_0$.

4.9 An ordered quadruple of positive integers $(\lambda; t, k, v)$ is *admissible* if each $\lambda_s = \tbinom{v-s}{t-s} \Big/ \tbinom{k-s}{t-s}$ for $0 \leq s \leq t$ is an integer. An admissible quadruple $(\lambda; t, k, v)$ is denoted by t-(v, k, λ). An admissible t-(v, k, λ) is *realizable* if a t-(v, k, λ) design exists.

4.10 **Remark** Given integers $0 < t < k < v$, the smallest positive integer value of λ for which t-(v, k, λ) is admissible is denoted by $\lambda_{\min}$, more exactly $\lambda_{\min}(t, k, v)$. For any admissible t-(v, k, λ), $\lambda_{\min}$ divides λ. The largest value of λ for which a simple t-(v, k, λ) design exists is denoted by $\lambda_{\max}$ and is equal to $\binom{v-t}{k-t}$. The simple t-$(v, k, \lambda_{\max})$ design $\mathcal{D} = (X, \binom{X}{k})$ is the *trivial* design or the *complete* design. Here $\binom{X}{k}$ is the set of all k-subsets of X. If $k \geq v - t$, then the design is the trivial design. When $k = t + 1$, $\lambda_{\min} = \gcd(v - t, \operatorname{lcm}(1, 2, \ldots, t + 1))$ [2016].

4.11 If $\mathcal{D} = (X, \mathcal{B})$ is a t-(v, k, λ) design and I, J are disjoint subsets of X with $|I|+|J| \leq t$, then $\lambda_{|I|,|J|}$ counts the number of blocks that contain I and no point of J.

4.12 **Remark** Consider the admissible t-(v, k, λ) and let i, j be nonnegative integers. If $0 \leq i + j \leq t$, then $\lambda_{i,j} = \lambda \binom{v-i-j}{k-i} / \binom{v-t}{k-t}$ is an integer. A recursive formula for these numbers is $\lambda_{i,j+1} = \lambda_{i,j} - \lambda_{i+1,j}$. For $\lambda = 1$, see also §5.4.

4.13 **Remark** Mappings that map admissible quadruples onto admissible quadruples include:

- red: t-$(v, k, \lambda) \mapsto (t-1)$-$(v, k, \lambda_{t-1,0})$,
- der: t-$(v, k, \lambda) \mapsto (t-1)$-$(v-1, k-1, \lambda)$,
- res: t-$(v, k, \lambda) \mapsto (t-1)$-$(v-1, k, \lambda_{t-1,1})$,
- supp: t-$(v, k, \lambda) \mapsto t$-$(v, k, \lambda_{0,t})$,
- comp: t-$(v, k, \lambda) \mapsto t$-$(v, k, \lambda_{\max} - \lambda)$.

4.14 **Theorem** [226] Consider the admissible t-(v, k, λ) with $\lambda \neq \lambda_{\max}$. Then there exists a unique maximal (v', t') with t'-(v', k', λ') admissible such that t-(v, k, λ) is obtained by iteratively applying some of the mappings red, der, and res to t'-(v', k', λ').

4.15 **Remark** The unique admissible quadruple t'-(v', k', λ') in Theorem 4.14 is the *ancestor* of t-(v, k, λ). All of the admissible quadruples with this ancestor form its family. Table 5.17 lists explicit examples for $\lambda = 1$. If the ancestor is realizable, then all the quadruples of the family are realizable. The indices of the designs in a family are given by appropriate values $\lambda_{i,j}$ of the ancestor.

4.16 **Theorem** Let $\mathcal{D} = (X, \mathcal{B})$ be a t-(v, k, λ) design. Then

1. $\mathcal{D}$ is a red(t-(v, k, λ)) design, the *reduced design*,
2. If $x \in X$, then $\operatorname{der}_x(\mathcal{D}) = (X, \{B \setminus \{x\} : x \in B \in \mathcal{B}\})$ is a der(t-(v, k, λ)) design, the *derived design* at x,

3. If $x \in X$, then $\mathrm{res}_x(\mathcal{D}) = (X, \{B : x \notin B \in \mathcal{B}\})$ is a res(t-(v,k,λ)) design, the *residual design* at x,
4. $\mathrm{supp}(\mathcal{D}) = (X, \{X \setminus B : B \in \mathcal{B}\})$ is a supp(t-(v,k,λ)) design, *the supplementary design*,
5. If $\mathcal{D}$ is simple, then $\mathrm{comp}(\mathcal{D}) = (X, \binom{X}{k} \setminus \mathcal{B})$ is a comp(t-(v,k,λ)) design, the *complementary design*.

4.17 Remark In view of the last two constructions in Theorem 4.16, one usually only considers t-(v,k,λ) designs with $t < k \leq v/2$ and simple designs only for $0 < \lambda \leq \lambda_{\max}/2$.

4.18 Theorem [2069] Consider an admissible t-(v,k,λ). If der(t-(v,k,λ)) and res(t-(v,k,λ)) are realizable, then red(t-(v,k,λ)) is realizable. If t-$(2k+1,k,\lambda)$ is realizable, then t-$(2k+2,k+1,\frac{\lambda(2k+2-t)}{(k+1-t)})$ is realizable.

4.19 Remark A $(t+1)$-$(v+1,k+1,\lambda)$ design $(Y,\mathcal{A})$ is an *extension* of a t-(v,k,λ) design $(X,\mathcal{B})$ if $(X,\mathcal{B})$ is a derived design of $(Y,\mathcal{A})$. Extensions are obtained by Theorem 4.20 and by large set recursions, see §4.4.

4.20 Theorem [76] Let $\mathcal{D} = (X,\mathcal{B})$ be a t-$(2k+1,k,\lambda)$ design and ∞ a new point not in X.

1. If t is even, then $(X \cup \{\infty\}, \{B \cup \{\infty\} : B \in \mathcal{B}\} \bigcup \{X \setminus B : B \in \mathcal{B}\})$ is a $(t+1)$-$(2k+2,k+1,\lambda)$ design.
2. If $\mathcal{D}$ is simple, t odd, and $\lambda = \lambda_{\max}/2$, then $(X \cup \{\infty\}, \{B \cup \{\infty\} : B \in \mathcal{B}\} \bigcup \{X \setminus B : B \in \binom{X}{k} \setminus \mathcal{B}\})$ is a $(t+1)$-$(2k+2,k+1,\lambda)$ design.

4.21 Example Let $X = \{0,1,2,3,4,5,6,7,8,9,a,b,c\}$ and choose the 66 base blocks:

013459 014567 012457 012346 012345 012367 023567 034567 024567 012458 023468
012468 012368 012568 012378 014568 034568 013478 023578 024578 012678 024569
012469 023459 014569 014579 012579 012479 023579 013679 012589 024589 034689
013469 035678 035679 01247a 035789 034789 036789 02357a 01467a 014789 01347a
02368a 02358a 02567a 01458a 01368a 024678 023478 023479 023469 025679 024679
025689 023689 023589 012356 013467 013458 013579 015678 013578 013569 013489

Applying the automorphism $\alpha = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ a\ b\ c)$ yields 858 blocks that form a 5-$(13,6,4)$ design [1352]. By Theorem 4.20 this design is extended to a 6-$(14,7,4)$ design. This is the smallest possible 6-design. For further isomorphism types see [1292].

4.22 Remark If there is a Hadamard matrix of order $4n$, then there is a 2-$(4n-1,2n-1,n-1)$ design. By Theorem 4.20, this design can be extended to a 3-$(4n,2n,n-1)$ design, a *Hadamard* 3-design. The blocks of such a design intersect in 0 or n points.

4.23 Theorem If there is a Hadamard matrix of order $4n$, then for all integers $\ell, m \geq 0$ with $m + \ell < n$, there is a 3-$(4n, 2n+\ell-m, (n-1)\binom{2n}{\ell}\binom{2n+\ell-m}{3}\binom{2n}{m} / \binom{2n}{3})$ design.

4.24 Theorem [858] If there exists a simple t-(v,k,λ_1) design $(X,\mathcal{A})$ and a simple t-(v,k,λ_2) design $(X,\mathcal{B})$ such that $|\mathcal{B}| < \lambda_{\max}/\lambda_1$, then $\mathcal{B}$ can be chosen to be disjoint from $\mathcal{A}$, and thus a simple t-$(v,k,\lambda_1+\lambda_2)$ design exists.

4.25 Theorem [1867] If there exists a simple t-(v,k,λ) design with a group of automorphisms G and $\binom{v}{k} > (s-1)(b^2 - \frac{(b-1)|G|}{k!(v-k)!})$ for some positive integer s, then there exist s isomorphic copies of this design on the same point set with pairwise disjoint block sets.

4.26 **Theorem** [166, 1509, 2068] If there exists a simple t-(v,k,λ) design such that for some positive integer s, $\binom{v}{k} > \lambda \sum_{i=1}^{m} \binom{v}{i}\binom{s}{i}\lambda_{0,n}$ where $m = \min\{s, v-k\}$ and $n = \min\{i,t\}$, then there exists a t-$(v+s,k,\lambda\binom{v-t+s}{s})$ design.

4.27 **Remark** In [1868], more general versions of Theorems 4.25 and 4.26, employing resolvable designs, are given (see §II.7).

4.28 **Theorem** [753] If there is a t-(v,k,λ) design $(X,\mathcal{B})$ such that any two blocks intersect in at most $k-(\ell+m+1)$ points, for fixed integers $\ell, m \geq 0$, then $(X,\mathcal{A})$ is a

$$t\text{-}(v, k+\ell-m, \lambda\tbinom{v-k}{\ell}\tbinom{k+\ell-m}{t}\tbinom{k}{m}/\tbinom{k}{t}) \text{ design}$$

where $\mathcal{A} = \{(B \cup L) \setminus M : B \in \mathcal{B}, L \subseteq (X \setminus B), |L| = \ell, M \subseteq B, |M| = m\}$.

4.29 **Remark** If G is a group acting t-homogeneously on a set X and S is a k-subset of X, then the orbit S^G of S under the action of G is a t-(v,k,λ) design with $\lambda = (|G|\binom{k}{t})/(|G_S|\binom{v}{t})$ and $|G_S|$ the number of elements of G that fixes S.

4.30 **Example** Let q be a prime power and $n > 0$ be an integer. Then $G = \mathrm{PGL}(2,q^n)$ acts sharply 3-transitive on $X = \mathbb{F}_{q^n} \cup \{\infty\}$. If $S \subseteq X$ is the natural inclusion of $\mathbb{F}_q \cup \{\infty\}$, then the orbit of S under G is a 3-$(q^n+1, q+1, 1)$ design. These designs are *spherical geometries*; when $n = 2$, they are *inversive planes*, *Möbius planes*, or *circle geometries*.

4.31 **Theorem** [1152] Let B be a subgroup of the multiplicative group of nonzero elements of $\mathbb{F}_q$. Then the orbit of $S = B \cup \{0,\infty\}$ under the action of $\mathrm{PGL}(2,q)$ is the block set of one of the designs:

1. 3-$(q^n+1, q+1, 1)$ design where q is a prime power and $n \geq 2$ (a spherical geometry);
2. 3-$(q+1, k+1, k(k+1)/2)$ design if $(k-1)|(q-1)$, $k \nmid q$, and $k \notin \{3,5\}$;
3. 3-$(q+1, 4, 3)$ design for $q \equiv 1, 5 \pmod 6$;
4. 3-$(q+1, 6, 5)$ design for $q \equiv 1, 9, 13, 17 \pmod{20}$.

4.32 **Remark** The distribution of 3-designs among the orbits of k-subsets under $\mathrm{PSL}(2,q)$ for $q \equiv 3 \pmod 4$ can be found in [421].

4.33 **Remark** Several 5-designs are obtained from codes by the Assmus–Mattson Theorem, see §VII.1.4.

4.34 **Theorem** [2012] Given integers t and v with $v \equiv t \pmod{(t+1)!^{2t+1}}$ and $v \geq t+1 > 0$, then a simple t-$(v, t+1, (t+1)!^{2t+1})$ design exists. That is, simple t-designs exist for all t.

4.35 **Remark** In Theorem 4.34, v becomes very large as t grows. In contrast, Theorem 4.66, which contains a recursive construction for large sets, produces t-designs with much smaller v.

4.36 **Remark** Infinitely many infinite series of simple t-designs are obtained from large set recursion; see §4.4. There are also infinitely many infinite series of resolvable 3-designs; see §II.7 and [1403, 2072].

4.37 **Table** Some infinite families of simple t-designs with $t \geq 3$ (derived and residual families are omitted).

t-(v,k,λ)	Conditions	Ref
3-$(n,4,1)$	$n \equiv 2$ or $4 \pmod 6$	[1035]
3-$(va^d+1, q+1, 1)$	3-$(a+1, q+1, 1)$ exists, $a \geq 2$, q prime power, d sufficiently large, $v-1 \equiv 0 \pmod{(q-1)}$, $v(v-1) \equiv 0 \pmod{q(q-1)}$, $v(v^2-1) \equiv 0 \pmod{q(q^2-1)}$.	[1621]

t-(v,k,λ)	Conditions	Ref
3-$(q+1,4,2)$	$q \equiv 1 \pmod 3$	[1152]
3-$(q+1,4,3)$	odd $q \geq 5$	[1152]
3-$(3^n+1,4,\lambda)$	$\lambda = 6k$ or $6k+1$, $0 \leq k \leq (3^{n-1}-1)/2$	[753]
3-$(q+1,4,\lambda)$	odd $q \not\equiv 1 \pmod 6$, $\lambda = 6k$ or $6k+3$, $0 \leq k \leq (q-5)/6$	[753]
3-$(2^n+1,4,\lambda)$	$\lambda = 6k$, $1 \leq k \leq (2^{n-1}-1)/3$	[753]
3-$(4n,4,2n-3)$	$n \geq 2$	[753]
3-$(n,5,5(n-4)/2)$	$n \equiv 2,4 \pmod 6$	[753]
3-$(6n,6,(3n-2)(3n-4)(3n-5)/4)$	$n \equiv 0,3 \pmod 8$	[753]
3-$(2^{n+1}+2,6,5(2^n-1))$	n odd and $n \geq 5$	[2072]
3-$(2^n m,8,7(2^{n-2}m-1))$	$m = 20, 28$ and $n \geq 0$	[2072]
3-$(2^{n+j}3,2^n,(2^{n-1}-1)(2^n-1)\prod_{i=2}^{n-1}(2^{n+j-i}3-1))$	$j \geq 0$ and $n \geq 3$	[2072]
3-$(2^n,6+\ell-m,\lambda\binom{2^n-6}{\ell}\binom{6+\ell-m}{3}\binom{6}{m}/20)$	$n \geq 4$, $\ell+m \leq 2$, and $\lambda = \begin{cases}(2^n-4)/3 \text{ for } n \text{ even},\\(2^{n-1}-4)/3 \text{ for } n \text{ odd}\end{cases}$	[753]
3-$(q^f+1,q+1+\ell-m,\binom{q^f-q}{\ell}\binom{q+1+\ell-m}{3}\binom{q+1}{m}/\binom{q+1}{3})$	$f \geq 2$, and $\ell+m \leq q-2$	[753]
3-$(q+1,\frac{q+1}{2},\frac{(q+1)(q-3)}{8})$	4 divides $q+1$	[1175]
3-$(4n,2n+\ell-m,(n-1)\binom{2n}{\ell}\binom{2n+\ell-m}{3}\binom{2n}{m}/\binom{2n}{3})$	$\ell+m \leq n-1$, and H$(4n)$ exists	[753]
3-$(2n,n,n-2)$	H$(4n)$ exists and $n \geq 5$ is odd; or $2n-1$ is a prime power	[753]
3-$(6k,2k,(2k-1)\binom{3k-2}{k-2})$	$k \geq 2$	[753]
3-$(2n,k\binom{n}{s}\binom{n-s}{k-2s}2^{k-2s}\binom{k}{3}/\binom{2n}{3})$	$(2n-1)\,\vert\,\binom{k}{2}$, $2n-1 > 2k$, $s = \binom{k}{2}/(2n-1)$	[753]
4-$(2^f+1,5,\lambda)$	$\lambda \in \{5,20\}$, odd $f \geq 5$	[257]
4-$(2^f+1,6,10)$	for all odd $f \geq 5$	[252]
4-$(2^f+1,6,\lambda)$	$\lambda \in \{60,70,90,100,150,160\}$, $\gcd(f,6)=1$	[257]
4-$(2^f+1,7,70(2^f-5)/3)$	$\gcd(f,6)=1$	[257]
4-$(2^f+1,8,35)$	$\gcd(f,6)=1$	[257]
4-$(2^f+1,9,84)$	$f \geq 5$	[253]
4-$(2^f+1,9,\lambda)$	$\lambda \in \{63,147\}$, $\gcd(f,6)=1$	[257]
4-$(2^n+1,2^m,(2^m-3)\Pi_{i=2}^{m-1}\frac{2^{n-i}-1}{2^{m-i}-1})$	$2 < m < n$	[1145]
4-$(2^n+1,2^{n-1}-1,(2^{n-1}-3)(2^{n-2}-1)(2^{n-1}-4))$	$n \geq 4$	[753]
4-$(2^n+1,2^m+1,(2^m+1)\Pi_{i=2}^{m-1}\frac{2^{n-i}-1}{2^{m-i}-1})$	$2 < m < n-1$, $m \not\vert n$	[1145]
4-$(2^n+1+s,2^{n-1}-1,\binom{2^n+s-3}{s}(2^{n-1}-1)(2^{n-2}-1)(2^{n-1}-4))$	$\frac{2^{n-1}-2}{n-1} > s+6$, $s \geq 2$, $n \geq 6$	[1509]
4-$(2^n+1+s,2^m,\binom{2^n+s-3}{s}(2^m-3)\mu)$	for m sufficiently close to n, with m large enough so that $\binom{v}{k}/\binom{v+s}{s} > b_0(b_0-b_1)$ where $\mu = \Pi_{i=2}^{m-1}\frac{2^{n-i}-1}{2^{m-i}-1}$	[1509]
4-$(2^n+1+s,2^m+1,\binom{2^n+s-3}{s}(2^m+1)\mu)$	for m sufficiently close to n, with m large enough so that $\binom{v}{k}/\binom{v+s}{s} > b_0(b_0-b_1)$ where $\mu = \Pi_{i=2}^{m-1}\frac{2^{n-i}-1}{2^{m-i}-1}$	[1509]
4-$(9m+5,6,(27m^2+3m)/2)$	$m > 0$,	[1340]
5-$(2^n+2,2^{n-1}+1,(2^{n-1}-3)(2^{n-2}-1))$	$n \geq 4$,	[75]
5-$(2^n+3,2^{n-1}+1,(2^n-2)(2^{n-1}-3)(2^{n-2}-1))$	$n \geq 6$	[2069]
5-$(2^n+4,2^{n-1}+2,(2^n-1)(2^n-2)(2^{n-2}-1))$	$n \geq 6$	[2069]
5-$(2^n+5,2^{n-1}+2,2^n(2^n-1)(2^n-2)(2^{n-2}-1))$	$n \geq 6$	[2069]
5-$(2^n+6,2^{n-1}+3,2^{n-1}(2^n+1)(2^n-1)(2^n-2))$	$n \geq 6$	[2069]
5-$(2^n+2+s,2^n+1,\binom{2^n+s-3}{s}(2^{n-1}-3)(2^{n-2}-1))$	$N \geq 4$, $n \geq N$, $s > 0$, $((2^N-N)/(N-1)) > s+4$	[1509]

4.38 **Remark** Bierbrauer [256] has constructed an infinite series of nonsimple 7-designs with affine automorphism groups of characteristic 2.

4.39 **Remark** There is no known simple 4-$(4^m + 1, 5, 2)$ design for any $m > 0$. However, there exist such designs with repeated blocks for all $m > 0$ [128].

4.40 **Remark** [1333] A 6-$(17, 7, 2)$ design with repeated blocks can be constructed using orbits of 7-element subsets under the action of $G = \mathrm{PSL}(2, 16)$ on the projective line $\mathbb{F}_{16} \cup \{\infty\}$. Only one orbit is repeated. More precisely take G to be the group generated by the permutations:
(0 5 12 4 3 1 14 9 13 11 2 8 6 10 7); (0 15)(1 2)(3 4)(5 6)(7 8)(9 10)(11 12)(13 14); and (0)(1 2)(3 8)(4 6)(5 7)(9 13)(10 12)(11 14)(15 16).
Then the union of the orbits of the 3 base blocks $\{0, 1, 2, 4, 5, 6, 9\}$,$\{0,1,2,3,4,5,7\}$, and $\{0, 2, 3, 4, 6, 8, 9\}$ with the last one repeated twice form a 6-$(17, 7, 2)$ design.

4.41 **Remark** All known simple t-(v, k, λ) designs with $t \geq 6$ have $\lambda \geq 4$.

4.42 **Theorem** [2147] Given integers $0 < t \leq k \leq v$, then there is an integer $n > 0$ such that a t-(v, k, λ) design with repeated blocks exists whenever the conditions $\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}$ for $i = 0, 1, \ldots, t,$ and $\lambda > n$ are satisfied.

4.43 **Conjecture** If there exists a t-(v, k, λ) design with $\lambda \leq \lambda_{\max}/2$ having repeated blocks, then there exists such a design without repeated blocks.

4.3 Table of Simple t-Designs

4.44 **Table** Admissible but not realizable parameter quadruples [291, 1009].

t	(v, k, λ), $v \leq 30$
3	(11,5,2), (16,6,2), (22,10,6), (26,10,3)
4	(12,6,2), (12,6,6) [1574], (15,5,1), (17,7,2), (17,8,5), (18,6,1), (23,8,2), (23,11,6), (23,11,12), (24,12,15)
5	(16,6,1), (18,8,2), (18,9,5), (19,9,7), (24,12,6), (24,12,12)
6	(17,7,1),(19,9,m2) for $m \in \{1 \ldots 5\}$, (20,10,7), (20,10,14), (24,12,12), (30,15,44)
7	(18,8,1), (20,10,m2) for $m \in \{1 \ldots 5\}$, (26,11,6)
8	(19,9,1), (27,11,3), (27,12,6), (27,12,12), (27,13,18), (28,13,24)
9	(20,10,1), (28,12,3), (28,13,6), (28,13,12), (28,14,18), (29,14,24)
10	(27,12,4), (27,13,20), (29,13,3), (29,13,6), (29,13,9), (29,14,m6) for $m \in \{1 \ldots 8\}$, (30,14,15), (30,15,m24) for $m \in \{1 \ldots 4\}$
11	(28,13,4), (28,14,20), (30,14,m3) for $m \in \{1 \ldots 5\}$, (30,15,m6) for $m \in \{1 \ldots 8\}$
12	(29,14,4), (30,15,24), (31,15,m3) for $m \in \{1 \ldots 12\}$
13	(30,15,4)

4.45 **Remark** For $v < 20$, the only parameters of 3-designs for which existence is undecided are 3-$(16, 7, 5)$, 3-$(17, 7, 7)$, and 3-$(19, 9, m28)$, where $m \in \{5,$ 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, 83, 89, 92, 95, 101, 107, 113, 116, 122, 125, 128, 131, 134, 137, 143, 146, 149, 155, 161, 167, 173, 179, 185, 191, 197, 203, 209, 215, $221\}$. The designs can be found in [172, 333, 467, 1343, 1351, 1453, 1692, 2014], employing the standard constructions from Theorem 4.16, or prescribing the group $D_7 \times C_2$ for a 3-$(14, 5, 5)$ design.

4.46 **Table** Existence of simple t-(v, k, λ) designs for $t = 3, 4$ and $t < k \leq v/2$ and $v \leq 24$, $5 \leq t < k \leq v/2$ and $v \leq 40$, and $\lambda \leq \lambda_{\max}/2$.

An entry of m in the set for row t-$(v, k, m\lambda_{\min})$ indicates the existence of a t-$(v, k, m\lambda_{\min})$ design. List(t, k, v) denotes the list of these values of m. A list may be

multiplied by a factor f, meaning that each member is multiplied by f. By Theorem 4.16 some lists are easily obtained from others.

- If $\lambda_{\min}(t,k,v) = f \cdot \lambda_{\min}(t-1,k-1,v-1)$, then $f\times\text{List}(t,k,v) \subseteq \text{List}(t-1,k-1,v-1)$.
- If $\lambda_{\min}(t,k,v)\frac{v-k}{k-t+1} = f\cdot\lambda_{\min}(t-1,k,v-1)$, then $f\times\text{List}(t,k,v)\frac{v-k}{k-t+1} \subseteq \text{List}(t-1,k,v-1)$.
- If $\lambda_{\min}(t,k,v)\frac{v-t+1}{k-t+1} = f \cdot \lambda_{\min}(t-1,k,v)$, then $f\times\text{List}(t,k,v)\frac{v-t+1}{k-t+1} \subseteq \text{List}(t-1,k,v)$.

These implications are used to avoid duplications of long lists in the table. The notation $a\ldots b$ is used to indicate the set of integers from a to b. The upper limit $\lfloor\lambda_{\max}/(2\lambda_{\min})\rfloor$ on m is given by LIM. The sets are followed by prescribed automorphism groups, references, and theorems among which the constructions can be found.

If G is a permutation group on V, H a permutation group on W, then $G-$ denotes a point stabilizer, $G+$ adds a fixed point to G, G^i is a subgroup of index i in G, $G^{[2]}$ denotes the action on two element subsets, $G \oplus H$ denotes the direct product of the two groups acting on $V \cup W$, and $G \times H$ denotes the direct product of the two groups acting on the Cartesian product $V \times W$. The designs were constructed by prescribing these groups and employing `DISCRETA` [241].

3-$(20,4,m)$	$\{1\ldots8\}$ LIM $= 8$, [1337].
3-$(20,5,m2)$	$\text{List}(4,6,21) \cup \{3,\ 4\}$ LIM $= 34$, $D_{19}+$,Theorem 4.16 [1337, 1351].
3-$(20,6,m10)$	$\{1\ldots34\}$ LIM $= 34$, [1337].
3-$(20,7,m35)$	$\{1\ldots34\}$ LIM $= 34$, [1337].
3-$(20,8,m14)$	$\{1\ldots221\}$ LIM $= 221$, [1337].
3-$(20,9,m28)$	$\text{List}(4,9,21)\cup\text{List}(4,10,21) \cup \{1\ldots4,\ 6\ \ldots22,\ 24\ \ldots28,\ 30\ldots34,$ $38,\ 42\ldots46,\ 48\ldots52,\ 54\ldots58,\ 60\ldots64,\ 66\ldots70,\ 72\ldots76,\ 78\ldots82,$ $84\ldots88,\ 91,\ 93,\ 98,\ 104,\ 106,\ 110,\ 111,\ 119\ldots121,\ 140,\ 141,\ 151,$ $152,\ 156,\ 164,\ 171,\ 174,\ 181,\ 182,\ 188,\ 194,\ 196,\ 200,\ 201\}$ LIM $= 221$, $\text{PSL}(3,4)-$, $\text{PSL}(2,19)$, $\text{HOL}(C_{20})$, [1337], Theorems 4.24, 4.16, 4.18, 4.23.
3-$(20,10,m4)$	$\{1\ldots2431\}$ LIM $= 2431$, Theorem 4.20.
3-$(21,4,m6)$	$\{1\}$ LIM $= 1$, [2011].
3-$(21,5,m3)$	$\{1\ldots25\}$ LIM $= 25$, $\text{PGL}(3,2)^{[2]}$ [1335, 1351], Theorem 4.18.
3-$(21,6,m4)$	$\{3\ldots102\}$ LIM $= 102$, $\text{PGL}(3,2)^{[2]}$ [1351, 1335], Theorem 4.18.
3-$(21,7,m15)$	$4\times\text{List}(5,7,23)\cup2\times\text{List}(5,8,23)\cup\{3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 15,\ 16,\ 18,\ 20,\ 21,$ $27,\ 28,\ 30,\ 32,\ 33,\ 39,\ 42,\ 44,\ 45,\ 51,\ 52,\ 57,\ 63,\ 66,\ 69,\ 75,\ 76,\ 78,\ 81,$ $87,\ 88,\ 90\ldots93,\ 99,\ 100\}$ LIM $= 102$, $\text{PSL}(3,4)-+$, [1335], Theorem 4.18.
3-$(21,8,m84)$	$\{6,\ 8,\ 9,\ 12,\ 14,\ 15,\ 16,\ 18,\ 21,\ 22,\ 24,\ 27,\ 30,\ 32,\ 33,\ 36,\ 38,\ 39,\ 40,\ 42,$ $45,\ 46,\ 48,\ 51\}$ LIM $= 51$, $\text{PSL}(3,2)\times C_3$, [1335], Theorems 4.8, 4.18.
3-$(21,9,m42)$	$\text{List}(5,10,22)\cup\text{List}(5,11,23) \cup 13\times\text{List}(5,9,22) \cup \{1,\ 2,\ 4,\ 7,\ 10,\ 12,$ $13,\ 16,\ 17,\ 19,\ 24,\ 25,\ 31,\ 36,\ 46,\ 51,\ 61,\ 66,\ 76,\ 79,\ 106,\ 111,\ 115,$ $119,\ 120,\ 121,\ 126,\ 133,\ 141,\ 147,\ 151,\ 160,\ 165,\ 166,\ 170,\ 171,\ 177,$ $178,\ 181,\ 186,\ 187,\ 192,\ 193,\ 196,\ 201,\ 205,\ 210,\ 211,\ 214,\ 216,\ 219\}$ LIM $= 221$, Theorems 4.18, 4.8.
3-$(21,10,m72)$	$\text{List}(4,10,21) \cup \{1,\ 2,\ 4,\ 7,\ 17,\ 31,\ 51,\ 61,\ 76,\ 79,\ 91,\ 106,\ 111,\ 119,$ $141,\ 151,\ 171,\ 181,\ 196,\ 201\}$ LIM $= 221$, Theorems 4.18, 4.16.
3-$(22,4,m)$	$\{1\ldots9\}$ LIM $= 9$, Theorem 4.16.
3-$(22,5,m3)$	$\{1\ldots28\}$ LIM $= 28$, Theorems 4.18, 4.16.
3-$(22,6,m)$	$\{1\ldots484\}$ LIM $= 484$, [289, 753, 1338], Theorems 4.18, 4.16.
3-$(22,7,m)$	$2\times\text{List}(4,8,23) \cup \{5,\ 10,\ 171,\ 285,\ 513,\ 570,\ 627,\ 630,\ 726,\ 798,\ 810,$ $855,\ 969,\ 1026,\ 1197,\ 1311,\ 1386,\ 1425,\ 1482,\ 1539,\ 1653,\ 1710,\ 1881,$ $1890\}$ LIM $= 1938$, [289, 753, 1045], Theorems 4.18, 4.16, 4.24.

3-$(22, 8, m6)$	$\{m = 2n : n = 1 \ldots 484\} \cup \{m = 3n : n = 1, 2, 4 \ldots 322\}$ LIM = 969, [289, 753], Theorems 4.18, 4.16, 4.8.
3-$(22, 9, m42)$	$\{1, 2, 4 \ldots 322\}$ LIM = 323, [289, 753], Theorems 4.16.
3-$(22, 10, m6)$	List$(5, 12, 24) \cup 20\times$List$(4, 10, 23) \cup \{m = 13n, n = 2, 4 \ldots 322\} \cup \{7,$ 14, 76, 133, 190, 304, 323, 361, 475, 589, 684, 969, 1159$\}$ LIM = 4199, [289, 1045], Theorems 4.16, 4.18, 4.24.
3-$(22, 11, m9)$	$19\times$List$(4, 10, 21) \cup$List$(5, 12, 24) \cup \{1, 2, 4, 76, 133, 323, 589, 969,$ 1045, 1159$\}$ LIM = 4199, [289, 753], Theorems 4.24, 4.18, 4.16.
3-$(23, 4, m4)$	$\{1, 2\}$ LIM = 2, [467].
3-$(23, 5, m10)$	$\{1 \ldots 9\}$ LIM = 9, Theorem 4.8.
3-$(23, 6, m20)$	$\{1 \ldots 28\}$ LIM = 28, Theorems 4.18, 4.8.
3-$(23, 7, m5)$	$\{1 \ldots 484\}$ LIM = 484, Theorems 4.8, 4.18, 4.18, 4.16.
3-$(23, 8, m8)$	$\{2 \ldots 969\}$ LIM = 969, [1351].
3-(23,9,m12)	$\{4, 5, 6\} \cup \{m : m \geq 8$ and $m \equiv 0 \pmod 2\}$, [1351], Theorem 4.8.
3-$(23, 10, m120)$	List$(4, 10, 24) \cup \{323\}$ LIM = 323, Theorems 4.16, 4.18.
3-$(23, 11, m15)$	List$(5, 12, 24)$ LIM = 4199, Theorems 4.8, 4.18, 4.16.
3-$(24, 4, m3)$	$\{1, 2, 3\}$ LIM = 3, [2011].
3-$(24, 5, m30)$	$\{1, 2, 3\}$ LIM = 3, [467].
3-$(24, 6, m10)$	$\{1 \ldots 66\}$ LIM = 66, [1351].
3-$(24, 7, m105)$	$\{1 \ldots 28\}$ LIM = 28, [467].
3-$(24, 8, m21)$	$\{1 \ldots 484\}$ LIM = 484, [1351].
3-$(24, 9, m84)$	$\{1, 2, 4 \ldots 322\}$ LIM = 323, [753], Theorems 4.18, 4.8, 4.16.
3-$(24, 10, m180)$	$\{1, 2, 4, 6 \ldots 322\}$ LIM = 323, [753], Theorems 4.18, 4.8, 4.16.
3-$(24, 11, m45)$	$7\times$List$(5, 11, 24) \cup \{1, 2, 4, 66, 67, 133, 1210, 1276, 1277\}$ LIM = 2261, [753], Theorems 4.24, 4.8, 4.18, 4.16.
3-$(24, 12, m5)$	$7\times$List$(5, 12, 24) \cup \{1, 2, 4, 8, 16, 24, 32, 48, 64, 144, 145, 532, 931,$ 1330, 2128, 2261, 2527, 3325, 4123, 4356, 4357, 4500, 4501, 4788, 6517, 6783, 8113$\}$ LIM = 29393, [753, 1152], Theorems 4.24, 4.8, 4.18.
4-$(11, 5, m)$	$\{1, 2, 3\}$ LIM = 3, [333, 1342, 2159].
4-$(12, 5, m4)$	$\{1\}$ LIM = 1, [695].
4-$(12, 6, m2)$	$\{2, 4 \ldots 7\}$ LIM = 7, [1354], Theorems 4.16, 4.20, 4.18.
4-$(13, 5, m3)$	$\{1\}$ LIM = 1, Theorem 4.16.
4-$(13, 6, m6)$	$\{2, 3\}$ LIM = 3, [1343], Theorem 4.18.
4-$(14, 6, m15)$	$\{1\}$ LIM = 1, [467].
4-$(14, 7, m20)$	$\{1, 2, 3\}$ LIM = 3, [333], Theorems 4.20, 4.18.
4-$(15, 5, m)$	$\{3, 4, 5\}$ LIM = 5, [1588, 333, 1291].
4-$(15, 6, m5)$	$\{2 \ldots 5\}$ LIM = 5, [333], Theorem 4.16.
4-$(15, 7, m5)$	$\{4 \ldots 16\}$ LIM = 16, HOL$(C_5)C_3$ [333].
4-$(16, 6, m6)$	$\{1 \ldots 5\}$ LIM = 5, $(D_5 \times C_3)+$, [333], Theorems 4.18, 4.16.
4-$(16, 7, m20)$	$\{1 \ldots 5\}$ LIM = 5, [333], Theorem 4.16.
4-$(16, 8, m15)$	$\{4 \ldots 16\}$ LIM = 16, [333], Theorem 4.16.
4-$(17, 5, m)$	$\{3 \ldots 6\}$ LIM = 6, D_{17}, [1333].
4-$(17, 6, m6)$	$\{1 \ldots 6\}$ LIM = 6, Theorem 4.16.
4-$(17, 7, m2)$	$\{3, 6 \ldots 71\}$ LIM = 71, [333], Theorem 4.16.
4-$(17, 8, m5)$	$\{3, 6 \ldots 71\}$ LIM = 71, $C_{17}C_8$, [333, 1145, 1333], Theorems 4.18, 4.8, 4.16.
4-$(18, 5, m2)$	$\{1, 2, 3\}$ LIM = 3, [333].
4-$(18, 6, m)$	$\{5 \ldots 45\}$ LIM = 45, HOL$(C_{17})+$, $T(2, 3) \wr C_2$, [333, 1333, 2159].
4-$(18, 7, m28)$	$\{1 \ldots 6\}$ LIM = 6, Theorem 4.8.
4-$(18, 8, m7)$	$\{3, 5 \ldots 71\}$ LIM = 71, [333, 1333], Theorems 4.18, 4.8.
4-$(18, 9, m14)$	$\{3, 6 \ldots 71\}$ LIM = 71, [1333], Theorem 4.18.
4-$(19, 6, m15)$	$\{1, 2, 3\}$ LIM = 3, [333], Theorem 4.18.
4-$(19, 7, m35)$	$\{1 \ldots 6\}$ LIM = 6, Theorems 4.8, 4.16.
4-$(19, 8, m105)$	$\{1 \ldots 6\}$ LIM = 6, Theorems 4.8, 4.16.
4-$(19, 9, m21)$	$\{3, 6 \ldots 71\}$ LIM = 71, Theorems 4.18, 4.8, 4.16.
4-$(20, 5, m4)$	$\{1, 2\}$ LIM = 2, [1351], Theorem 4.16.

4-$(20, 6, m30)$	$\{1, 2\}$ LIM $= 2$, [1351, 1337].
4-$(20, 7, m140)$	$\{2\}$ LIM $= 2$, [1337].
4-$(20, 8, m70)$	$\{1 \ldots 13\}$ LIM $= 13$, [1337].
4-$(20, 9, m168)$	$\{2 \ldots 6, 8 \ldots 13\}$ LIM $= 13$, [1337], Theorem 4.8.
4-$(20, 10, m28)$	List$(5, 10, 20) \cup \{72, 74 \ldots 82, 84 \ldots 92, 94 \ldots 102, 104 \ldots 112, 114 \ldots 122, 124 \ldots 132, 134 \ldots 142\}$ LIM $= 143$, [1337], Theorem 4.18.
4-$(21, 5, m)$	$\{2 \ldots 8\}$LIM $= 8$, HOL$(C_7) \times C_3$, HOL(C_{21}).
4-$(21, 6, m2)$	$\{5, 6, 8 \ldots 34\}$ LIM $= 34$, PGL$(3, 2)^{[2]}$, HOL(C_{21}), [1351, 1335], Theorems 4.18, 4.8.
4-$(21, 7, m10)$	List$(5, 7, 22) \cup 2\times$List$(5, 8, 22)$ LIM $= 34$, [1335], Theorem 4.18.
4-$(21, 8, m70)$	List$(5, 9, 22)$ LIM $= 17$.
4-$(21, 9, m14)$	List$(5, 10, 22)$ LIM $= 221$, $\cup\{51, 169, 187, 192, 216\}$ LIM $= 221$, [1335], Theorems 4.18, 4.8.
4-$(21, 10, m28)$	$\{9, 10, 12, 13, 16, 18, 19, 22, 24, 25, 27, 28, 30, 33, 34, 36, 37, 39, 40, 42 \ldots 46, 48, 49, 52, 54, 55, 57, 58, 60, 63, 64, 66 \ldots 70, 72, 73, 75, 78, 82, 84, 85, 87.\ 88, 90, 93, 94, 96, 97, 99, 100, 102, 103, 105, 108, 109, 110, 112, 114, 115, 117, 118, 120, 123, 124, 126, 127, 129, 130, 132, 133, 135, 136, 138, 139, 142, 144, 145, 147, 148, 150, 153, 154, 156, 157, 158, 159, 160, 162, 163, 165, 166, 168, 169, 170, 172, 174 \ldots 178, 180, 183, 184, 186, 187, 189, 190, 192, 193, 195, 198, 199, 202, 204 \ldots 221\}$ LIM $= 221$, PSL$(2, 19)+$, [1335], Theorems 4.18, 4.8, 4.16.
4-$(22, 5, m6)$	$\{1\}$ LIM $= 1$, Theorem 4.16.
4-$(22, 6, m3)$	$3\times$List$(5, 6, 22)$ LIM $= 25$, Theorem 4.16.
4-$(22, 7, m4)$	$4\times$List$(5, 7, 23) \cup 2\times$List$(5, 8, 23)$ LIM $= 102$.
4-$(22, 8, m30)$	$3 \times$ (List$(5, 8, 22) \cup$List$(5, 9, 23))$ LIM $= 51$, Theorem 4.16.
4-$(22, 9, m252)$	List$(5, 9, 22) \cup \{11, 66\}$ LIM $= 17$, Theorem 4.16.
4-$(22, 10, m42)$	List$(5, 10, 22) \cup$List$(5, 11, 23)$ LIM $= 221$, Theorem 4.16.
4-$(22, 11, m72)$	List$(4, 10, 21)$ LIM $= 221$, Theorem 4.18.
4-$(23, 5, m)$	$\{1 \ldots 9\}$ LIM $= 9$, [1351], Theorem 4.16.
4-$(23, 6, m3)$	$\{1 \ldots 28\}$ LIM $= 28$, Theorem 4.16.
4-$(23, 7, m)$	$\{1 \ldots 484\}$ LIM $= 484$, [2159, 1338, 289, 753], Theorem 4.16.
4-$(23, 8, m2)$	$\{m = 2n,\ 1 \le n \le 484\} \cup \{3\} \cup \{m = 6n + 3,\ 3 \le n \le 160\} \cup \{969\}$ LIM $= 969$, [1783, 289], Theorems 4.16, 4.18.
4-$(23, 9, m18)$	$\{1,2,\ 4 \ldots 322\}$ LIM $= 323$, [289, 753], Theorem 4.16.
4-$(23, 10, m42)$	$\{2,4 \ldots 323\}$ LIM $= 323$, [289, 753], Theorem 4.16.
4-$(23, 11, m6)$	List$(5, 12, 24)$ LIM $= 4199$.
4-$(24, 6, m10)$	$\{1 \ldots 9\}$ LIM $= 9$, Theorem 4.8.
4-$(24, 7, m20)$	$\{1 \ldots 28\}$ LIM $= 28$, Theorem 4.8.
4-$(24, 8, m5)$	$\{1 \ldots 484\}$ LIM $= 484$, Theorem 4.16.
4-$(24, 9, m24)$	$\{1,2,\ 6 \ldots 233\}$ LIM $= 323$, Theorems 4.8, 4.16.
4-$(24, 10, m60)$	$\{2,4 \ldots 323\}$ LIM $= 323$, Theorems 4.8, 4.16.
4-$(24, 11, m120)$	List$(5, 11, 24) \cup$List$(5, 12, 25) \cup$List$(5, 11, 25)$ LIM $= 323$, Theorem 4.16.
4-$(24, 12, m15)$	List$(5, 12, 24))$ LIM $= 4199$, Theorem 4.16.
5-$(12, 6, m)$	$\{1, 2, 3\}$ LIM $= 3$, Theorem 4.20.
5-$(13, 6, m4)$	$\{1\}$ LIM $= 1$, [1352]. (See Example 4.21.)
5-$(14, 6, m3)$	$\{1\}$ LIM $= 1$, [333].
5-$(14, 7, m6)$	$\{2, 3\}$ LIM $= 3$, Theorems 4.20, 4.18.
5-$(15, 7, m15)$	$\{1\}$ LIM $= 1$, [2069].
5-$(16, 6, m)$	$\{3, 4, 5\}$ LIM $= 5$, D_{16}, [333], Theorem 4.16.
5-$(16, 7, m5)$	$\{3, 4, 5\}$ LIM $= 5$, HOL(C_{16}), HOL$(C_8) \times C_2$, [333].
5-$(16, 8, m5)$	$\{4 \ldots 16\}$ LIM $= 16$, Theorem 4.20.
5-$(17, 7, m6)$	$\{2 \ldots 5\}$ LIM $= 5$, [333, 2069].
5-$(17, 8, m20)$	$\{3, 4, 5\}$ LIM $= 5$, [2069, 1333].
5-$(18, 6, m)$	$\{4, 5, 6\}$ LIM $= 6$, [333, 1333], Theorem 4.16.
5-$(18, 7, m6)$	$\{1 \ldots 6\}$ LIM $= 6$, [1333].

5-$(18, 8, m2)$	$\{3, 7, 8, 15, 16, 20, 22, 23, 24, 30 \ldots 33, 38 \ldots 41, 46 \ldots 49, 52, 54 \ldots 57, 62 \ldots 65, 70, 71\}$ LIM $= 71$, [1333, 1504], Theorems 4.18, 4.16.
5-$(18, 9, m5)$	$\{3, 6 \ldots 71\}$ LIM $= 71$, [333, 1333], Theorems 4.16, 4.20.
5-$(19, 6, m2)$	$\{2, 3\}$ LIM $= 7$, HOL(C_{19}) [239].
5-$(19, 7, m7)$	$\{4, 5, 6\}$ LIM $= 6$, [333, 2069], Theorem 4.18.
5-$(19, 8, m28)$	$\{2 \ldots 6\}$ LIM $= 6$, [2069], Theorem 4.16.
5-$(19, 9, m7)$	$\{3, 7, 8, 15, 16, 18 \ldots 71\}$ LIM $= 71$, PSL$(2, 17)+$, [333, 1320, 2069], Theorem 4.16.
5-$(20, 8, m35)$	$\{1 \ldots 6\}$ LIM $= 6$, [1337].
5-$(20, 9, m105)$	$\{1 \ldots 6\}$ LIM $= 6$, [1337, 2069].
5-$(20, 10, m21)$	$\{3, 6 \ldots 71\}$ LIM $= 71$, [1337], Theorems 4.18, 4.20.
5-$(21, 6, m4)$	$\{1, 2\}$ LIM $= 2$, HOL(C_{21}), Theorem 4.16.
5-$(21, 7, m30)$	$\{2\}$ LIM $= 2$, Theorem 4.16.
5-$(21, 8, m280)$	$\{1\}$ LIM $= 1$, Theorem 4.16.
5-$(21, 9, m70)$	$\{2 \ldots 6, 8 \ldots 13\}$ LIM $= 13$, PSL$(2, 19)+$, Theorem 4.16, PSL$(3, 2) \times S_3$, (PΓL$(2, 9) \times id_2)+$ [2069].
5-$(21, 10, m168)$	$\{2, 4, 5, 6, 8, 10, 11, 12, 13\}$ LIM $= 13$, PGL$(2, 19)+$, PSL$(3, 2) \times S_3$, [1335, 2069], Theorem 4.18.
5-$(22, 6, m)$	$\{4 \ldots 8\}$ LIM $= 8$, Theorem 4.16.
5-$(22, 7, m2)$	$\{8, 16, 18, 20, 24, 28, 30, 34\}$ LIM $= 34$, Theorems 4.16, 4.8.
5-$(22, 8, m20)$	$\{2 \ldots 12, 14, 16, 17\}$ LIM $= 17$, PSL$(2, 19)++$, Theorem 4.8.
5-$(22, 9, m70)$	$\{3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 17\}$ LIM $= 17$, PSL$(2, 19)++$, Theorem 4.16.
5-$(22, 10, m14)$	List$(6, 11, 23) \cup \{18, 22, 27, 28, 30, 33, 34, 37, 39, 40, 42, 43, 44, 45, 48, 49, 52, 54, 57, 58, 60, 68, 69, 70, 75, 84, 88, 93, 96, 97, 102, 110, 124, 129, 136, 138, 142, 170, 174, 183, 202, 221\}$ LIM $= 221$, $M_{11} \times C_2$, PSL$(2, 19)++$, PSL$(3, 4) - \oplus C2$, PΓL$(2, 9) \times C_2 \oplus C_2$, Theorems 4.18, 4.16.
5-$(22, 11, m28)$	List$(4, 10, 21)$ LIM $= 221$, Theorem 4.20.
5-$(23, 6, m6)$	$\{1\}$ LIM $= 1$, HOL(C_{23}).
5-$(23, 7, m3)$	$\{12, 15, 18, 21, 24\}$ LIM $= 25$, Theorem 4.16.
5-$(23, 8, m8)$	$\{12, 24, 27, 30, 36, 48, 51\}$ LIM $= 51$, Theorems 4.8, 4.18, 4.16.
5-$(23, 9, m90)$	$\{3, 4, 6, 7, 9, 10, 11, 13, 16, 17\}$ LIM $= 17$, Theorems 4.8, 4.18, 4.16.
5-$(23, 10, m252)$	$\{3, 4, 6, 9, 10, 11, 12, 13, 15, 16, 17\}$ LIM $= 17$, PSL$(2, 19) \oplus C_3$, PSL$(2, 23)$, Theorems 4.8, 4.18, 4.16.
5-$(23, 11, m42)$	List$(6, 12, 24) \cup \{18, 22, 27, 28, 30, 33, 34, 37, 39, 40, 42, 43, 45, 48, 49, 52, 54, 57, 58, 60, 68, 69, 70, 75, 84, 88, 93, 102, 124, 129, 136, 138, 142, 143, 170, 174, 183\}$ LIM $= 221$, Theorems 4.8, 4.18, 4.16.
5-$(24, 6, m)$	$\{1 \ldots 9\}$ LIM $= 9$, [691, 753, 1351].
5-$(24, 7, m3)$	$\{1 \ldots 28\}$ LIM $= 28$, [753, 1351].
5-$(24, 8, m)$	$\{1 \ldots 484\}$ LIM $= 484$, [289, 753, 1338, 2159].
5-$(24, 9, m6)$	$\{1, 2, 6 \ldots 323\}$ LIM $= 323$, PSL$(2, 23)$, PGL$(2, 23)$, [120, 289, 753].
5-$(24, 10, m18)$	$\{2, 4 \ldots 323\}$ LIM $= 323$, PSL$(2, 23)$, PGL$(2, 23)$, [289, 753].
5-$(24, 11, m42)$	$19 \times$List$(6, 11, 24) \cup$List$(6, 11, 25) \cup$List$(6, 12, 25) \cup \{8, 11, 19, 22, 30, 33, 41, 44, 52, 55, 57, 63, 66, 74, 76, 77, 85, 88, 96, 99, 107, 110, 118, 121, 129, 132, 140, 143, 151, 154, 162, 165, 173, 176, 239, 323\}$ LIM $= 323$, PSL$(2, 23)$, PGL$(2, 23)$, [289, 753], Theorems 4.18, 4.16.
5-$(24, 12, m6)$	$19 \times$List$(6, 12, 24) \cup \{8, 16, 19, 27, 30, 33, 38, 41, 44, 49, 52, 55, 60, 63, 66, 71, 74, 77, 82, 85, 88, 93, 96, 99, 104, 107, 110, 115, 118, 121, 126, 129, 132, 137, 140, 143, 148, 151, 154, 159, 162, 165, 170, 173, 176, 181, 184, 187, 192, 195, 198, 203, 206, 209, 214, 217, 220, 225, 228, 231, 236, 239, 242, 247, 250, 253, 258, 261, 264, 269, 272, 275, 280, 283, 286, 291, 294, 297, 302, 305, 308, 313, 316, 319, 324, 327, 330, 335, 338, 341, 342, 346, 349, 352, 357, 360, 363, 368, 371, 374, 379, 382, 385, 390, 393, 396, 401, 404, 407, 412, 415, 418, 423, 426, 429, 434, 437, 440, 445, 448, 451, 456, 459, 462, 467, 470, 473, 478, 481, 484, 489, 492, 495, 500, 503, 506, 511, 513, 514, 517, 522, 525,

	528, 532, 533, 536, 539, 544, 547, 550, 555, 558, 561, 566, 569, 570, 572, 577, 560, 563, 568, 571, 574, 577, 580, 583, 588, 591, 594, 599, 602, 605, 610, 613, 616, 621, 624, 627, 632, 635, 638, 643, 646, 649, 654, 657, 660, 665, 668, 671, 672, 676, 679, 682, 687, 690, 693, 698, 701, 703, 704, 709, 712, 715, 720, 723, 726, 731, 734, 737, 741, 742, 745, 748, 753, 756, 759, 760, 764, 767, 770, 775, 778, 781, 786, 789, 792, 797, 798, 800, 803, 808, 811, 814, 817, 819, 822, 825, 830, 833, 836, 841, 844, 847, 852, 855, 858, 863, 866, 869, 874, 877, 880, 885, 888, 891, 896, 899, 902, 907, 910, 912, 913, 918, 921, 924, 929, 931, 932, 935, 940, 943, 946, 951, 954, 957, 962, 965, 968, 973, 976, 979, 984, 987, 988, 990, 995, 998, 1001, 1006, 1009, 1012, 1017, 1020, 1023, 1026, 1028, 1031, 1034, 1039, 1042, 1050, 1053, 1056, 1061, 1064, 1067, 1072, 1075, 1078, 1083, 1086, 1089, 1094, 1097, 1100, 1102, 1105, 1108, 1111, 1116, 1119, 1122, 1127, 1130, 1133, 1138, 1140, 1141, 1144, 1149, 1152, 1155, 1160, 1163, 1166, 1171, 1174, 1177…4199} LIM = 4199, PSL(2, 23), PGL(2, 23), [120, 289], Theorems 4.16, 4.20, 4.18.
5-(25, 7, $m10$)	{1…9} LIM = 9, Theorem 4.18.
5-(25, 8, $m20$)	{1…28} LIM = 28, PSL(2, 23), Theorems 4.16, 4.18.
5-(25, 9, $m15$)	{1, 3…161} LIM = 161, PSL(2, 23), Theorems 4.16, 4.18.
5-(25, 10, $m24$)	{2, 6…323} LIM = 323, PSL(2, 23), Theorems 4.16, 4.18.
5-(25, 11, $m60$)	List(6, 11, 25)∪List(6, 12, 26)∪List(6, 11, 26) ∪ {8, 11, 19, 22, 30, 33, 41, 44, 52, 55, 57, 66, 74, 77, 85, 88, 96, 99, 107, 110, 114, 118, 121, 129, 132, 140, 143, 151, 154, 158, 171, 173, 176, 187, 195, 206, 217, 231, 239, 242, 253, 261, 272, 273, 283, 285, 294, 305, 308, 318 … 323} LIM = 323, PSL(2, 23), Theorems 4.16, 4.18.
5-(25, 12, $m120$)	List(6, 13, 26) ∪ {8, 11, 19, 22, 30, 33, 41, 44, 52, 55, 57, 66, 74, 77, 79, 81, 85, 88, 96, 99, 106, 107, 108, 110, 118, 121, 129, 132, 133, 135, 158, 151, 154, 160, 162, 173, 176, 189, 196, 214, 226, 239, 268, 270, 288, 298, 321} LIM = 323, PSL(2, 23), Theorems 4.16, 4.18.
5-(26, 6, $m3$)	{3} LIM = 3, HOL(C_{26}).
5-(26, 8, $m70$)	{1…9} LIM = 9, PSL(2, 25), Theorems 4.16, 4.18.
5-(26, 9, $m315$)	{1…9} LIM = 9, PGL(2, 25), Theorems 4.16, 4.18.
5-(26, 10, $m63$)	{1, 3…161} LIM = 161, PGL(2, 25), Theorems 4.16, 4.18.
5-(26, 11, $m84$)	List(6, 12, 27) ∪ 2×List(6, 11, 27) ∪ {8, 11, 19, 22, 30, 33, 41, 44, 55, 57, 61, 63, 74, 76, 77, 85, 88, 96, 99, 107, 110, 114, 118, 121, 129, 132, 140, 143, 151, 154, 165, 169, 171, 173, 176, 195, 206, 209, 217, 219, 231, 239, 242, 247, 253, 261, 272, 275, 283, 285, 294, 305, 308… 323} LIM = 323, PGL(2, 25), Theorems 4.16, 4.18.
5-(26, 12, $m180$)	List(7, 14, 28)∪List(6, 12, 27) ∪ {8, 11, 19, 22, 30, 33, 41, 44, 55, 57, 66, 74, 77, 85, 88, 96, 99, 107, 110, 114, 118, 121, 129, 132, 140, 143, 151, 154, 171, 173, 176, 184, 195, 206, 217, 220, 231, 239, 242, 250, 253, 261, 264, 272, 275, 283, 285, 288, 305, 319, 321, 323} LIM = 323, Theorems 4.16, 4.18.
5-(26, 13, $m45$)	7×List(7, 14, 28) ∪ {56, 77, 133, 154, 210, 231, 287, 308, 385, 399, 462, 518, 539, 553, 567, 595, 616, 672, 693, 742, 749, 756, 770, 798, 826, 847, 903, 924, 931, 980, 1001, 1057, 1078, 1120, 1134, 1197, 1211, 1232, 1288, 1309, 1323, 1365, 1442, 1498, 1519, 1540, 1617, 1673, 1694, 1750, 1771, 1827, 1848, 1904, 1925, 1981, 1995, 2016, 2135, 2233, 2247, 2261} LIM = 2261, Theorems 4.16, 4.18.
5-(27, 6, $m2$)	{3} LIM = 11, Theorem 4.16.
5-(27, 7, $m21$)	{2…5} LIM = 5, Theorem 4.16.
5-(27, 8, $m140$)	{2…5} LIM = 5, Theorem 4.16.
5-(27, 9, $m35$)	List(6, 10, 28) ∪ {11, 22, 55, 88} LIM = 104, Theorem 4.18.
5-(27, 10, $m126$)	List(6, 10, 28) ∪ {11, 22, 55, 88} LIM = 104, Theorem 4.18.
5-(27, 11, $m231$)	List(6, 12, 28)∪List(6, 11, 27)∪{4, 11, 15, 22, 26, 37, 38, 44, 48, 55, 57, 59, 66, 70, 77, 88, 102, 103, 120, 121, 136, 147, 154, 158} LIM = 161, Theorems 4.16, 4.18.

5-$(27, 12, m264)$	$2\times$List$(6, 12, 28)\cup$List$(6, 12, 27) \cup \{8,\ 11,\ 19,\ 22,\ 30,\ 33,\ 41,\ 44,\ 55,\ 57,$ $61,\ 63,\ 66,\ 74,\ 76,\ 77,\ 85,\ 88,\ 96,\ 99,\ 102,\ 107,\ 110,\ 114,\ 118,\ 121,\ 126,$ $129,\ 132,\ 140,\ 143,\ 150,\ 151,\ 154,\ 156,\ 165,\ 169,\ 171,\ 173,\ 176,\ 184,$ $195,\ 196,\ 198,\ 206,\ 209,\ 217,\ 219,\ 220,\ 231,\ 232,\ 238,\ 239,\ 242,\ 247,$ $250,\ 253,\ 261,\ 264,\ 272,\ 275,\ 283,\ 285,\ 288,\ 294,\ 305,\ 308,\ 319,\ 321,$ $323\}$ LIM $= 323$, Theorems 4.16, 4.18.
5-$(27, 13, m495)$	List$(7, 14, 28) \cup \{8,\ 11,\ 19,\ 22,\ 30,\ 33,\ 41,\ 44,\ 55,\ 57,\ 66,\ 74,\ 77,\ 79,\ 81,$ $85,\ 88,\ 96,\ 99,\ 106,\ 107,\ 108,\ 110,\ 114,\ 118,\ 121,\ 129,\ 132,\ 133,\ 140,$ $143,\ 150,\ 151,\ 154,\ 160,\ 162,\ 171,\ 173,\ 176,\ 184,\ 187,\ 189,\ 195,\ 206,$ $214,\ 217,\ 220,\ 231,\ 239,\ 242,\ 250,\ 253,\ 261,\ 264,\ 272,\ 275,\ 283,\ 285,$ $288,\ 305,\ 319,\ 321,\ 323\}$ LIM $= 323$, Theorems 4.16, 4.18.
5-$(28, 6, m)$	$\{2 \ldots 11\}$ LIM $= 11$, [1355].
5-$(28, 7, m)$	List$(6, 8, 29) \cup \{1,\ 7,\ 8,\ 14,\ 15,\ 21,\ 22,\ 28,\ 29,\ 30,\ 33,\ 35,\ 40,\ 46,\ 50,\ 56,$ $60,\ 71,\ 73,\ 77,\ 88,\ 90,\ 92,\ 98,\ 103,\ 113,\ 119,\ 121,\ 123\}$ LIM $= 126$, $S_8^{[2]}$, PSL$(2, 13) \times C_2$ PSL$(2, 27)$, PΓL$(2, 27)$, PΓL$(2, 25) \oplus C_2$, [691, 289], Theorems 4.16, 4.18.
5-$(28, 8, m7)$	$\{3 \ldots 126\}$ LIM$= 126$, $S_8^{[2]}$, PSL$(2, 27)$, [289], Theorem 4.8. Theorems 4.16, 4.18.
5-$(28, 9, m35)$	List$(6, 9, 29) \cup \{3,\ 4,\ 10,\ 12,\ 13,\ 16,\ 19,\ 21,\ 24,\ 25,\ 27,\ 28,\ 30,\ 31,\ 33,$ $34,\ 37,\ 39,\ 40,\ 43,\ 45,\ 48,\ 49,\ 51,\ 52,\ 55,\ 57,\ 61,\ 73,\ 75,\ 79,\ 82,\ 84,\ 88,$ $91,\ 94,\ 97,\ 103,\ 106,\ 111,\ 115,\ 124\}$ LIM $= 126$, PSL$(2, 27)$, $Sp(6, 2)$, [289], Theorems 4.16, 4.18.
5-$(28, 10, m7)$	$11\times$List$(6, 11, 29) \cup 19\times$List$(6, 10, 29) \cup 23\times$List$(6, 10, 28) \cup \{253,\ 307,$ $420,\ 427,\ 506,\ 720,\ 960,\ 1080,\ 1265,\ 1440,\ 1680,\ 1800,\ 1867,\ 2024\}$ LIM $= 2392$, PSL$(2, 27)$, $Sp(6, 2)$, Theorems 4.16, 4.18.
5-$(28, 11, m231)$	$\{69,\ 138,\ 152,\ 161,\ 184,\ 207\}$ LIM $= 218$, Theorems 4.16, 4.18.
5-$(28, 12, m33)$	List$(6, 13, 29) \cup 23\times$List$(6, 12, 28) \cup \{92,\ 253,\ 345,\ 506,\ 598,\ 621,\ 759,$ $851,\ 874,\ 1012,\ 1104,\ 1173,\ 1265,\ 1311,\ 1357,\ 1449,\ 1518,\ 1610,\ 1771,$ $1794,\ 2024,\ 2116,\ 2254,\ 2277,\ 2369,\ 2530,\ 2584,\ 2668,\ 2737,\ 2760,\ 2783,$ $2875,\ 3036,\ 3128,\ 3312,\ 3381,\ 3542,\ 3634\}$ LIM $= 3714$, Theorems 4.16, 4.18.
5-$(28, 13, m33)$	List$(7, 15, 30) \cup \{184,\ 253,\ 437,\ 506,\ 690,\ 759,\ 943,\ 1012,\ 1265,\ 1311,$ $1403,\ 1449,\ 1518,\ 1702,\ 1748,\ 1771,\ 1817,\ 1863,\ 1955,\ 2024,\ 2208,\ 2277,$ $2346,\ 2438,\ 2461,\ 2484,\ 2530,\ 2622,\ 2714,\ 2783,\ 2898,\ 2967,\ 3036,\ 3059,$ $3220,\ 3289,\ 3450,\ 3473,\ 3542,\ 3588,\ 3680,\ 3726,\ 3795,\ 3887,\ 3933,\ 3979,$ $4048,\ 4232,\ 4301,\ 4347,\ 4485,\ 4508,\ 4554,\ 4738,\ 4807,\ 4922,\ 4991,\ 5037,$ $5060,\ 5313,\ 5336,\ 5474,\ 5497,\ 5566,\ 5681,\ 5750,\ 5819,\ 6003,\ 6072,\ 6256,$ $6325,\ 6509,\ 6555,\ 6624,\ 6762,\ 7015,\ 7084,\ 7337,\ 7383\}$ LIM $= 7429$, Theorems 4.16, 4.18.
5-$(28, 14, m55)$	List$(6, 14, 29) \cup 23\times$List$(6, 14, 28) \cup \{184,\ 253,\ 437,\ 506,\ 690,\ 759,\ 943,$ $1012,\ 1265,\ 1311,\ 1518,\ 1702,\ 1748,\ 1771,\ 1817,\ 1863,\ 1955,\ 2024,\ 2208,$ $2277,\ 2438,\ 2461,\ 2484,\ 2530,\ 2622,\ 2714,\ 2783,\ 2967,\ 3036,\ 3059,\ 3220,$ $3289,\ 3450,\ 3473,\ 3542,\ 3680,\ 3726,\ 3933,\ 3979,\ 4048,\ 4232,\ 4301,\ 4347,$ $4485,\ 4738,\ 4922,\ 4991,\ 5060,\ 5313,\ 5497,\ 5566,\ 5750,\ 5819,\ 6003,\ 6072,$ $6256,\ 6325,\ 6509,\ 6555,\ 6624,\ 7015,\ 7337,\ 7383\}$ LIM $= 7429$, Theorems 4.16, 4.18.
5-$(29, 6, m12)$	$\{1\}$ LIM $= 1$, Theorem 4.16.
5-$(29, 7, m6)$	$\{4,\ 6,\ 14,\ 16,\ 18,\ 22,\ 21,\ 23\}$ LIM $= 23$, PGL$(2, 27)+$, Theorems 4.16, 4.18.
5-$(29, 8, m8)$	List$(6, 9, 30) \cup$ List$(6, 8, 29) \cup \{7,\ 8,\ 14,\ 15,\ 21,\ 22,\ 28,\ 29,\ 30,\ 33,\ 35,\ 40,$ $50,\ 56,\ 71,\ 73,\ 77,\ 88,\ 90,\ 92,\ 98,\ 103,\ 113,\ 119,\ 121,\ 123\}$ LIM $= 126$, PGL$(2, 27)+$, Theorems 4.16, 4.18.
5-$(29, 9, m42)$	List$(6, 9, 29) \cup \{3,\ 4,\ 10,\ 12,\ 13,\ 16,\ 19,\ 21,\ 24,\ 25,\ 27,\ 28,\ 30,\ 31,\ 33,\ 34,$ $37,\ 39,\ 40,\ 43,\ 45,\ 48,\ 49,\ 51,\ 52,\ 55,\ 57,\ 61,\ 73,\ 75,\ 79,\ 82,\ 84,\ 88,\ 91,$ $94,\ 97,\ 103,\ 106,\ 111,\ 115,\ 124\}$ LIM $= 126$, PGL$(2, 27)+$, Theorems 4.16, 4.18.

5-$(29, 10, m168)$ List$(6, 10, 29)\cup$List$(6, 10, 30)$ LIM $= 126$, Theorem 4.16.

5-$(29, 11, m308)$ List$(6, 11, 29) \cup \{2,\ 3,\ 23,\ 36,\ 54,\ 72,\ 81,\ 108,\ 184\}$ LIM $= 218$, PΓL$(2, 27)+$, Theorem 4.16.

5-$(29, 12, m792)$ $\{69,\ 152,\ 161,\ 184\}$ LIM $= 218$, PGL$(2, 27)+$, Theorems 4.16, 4.18.

5-$(29, 13, m99)$ List$(6, 13, 29) \cup \{92,\ 253,\ 345,\ 506,\ 598,\ 759,\ 851,\ 874,\ 1012,\ 1104,\ 1173,\ 1219,\ 1242,\ 1265,\ 1311,\ 1357,\ 1449,\ 1518,\ 1610,\ 1771,\ 1794,\ 1840,\ 1863,\ 2024,\ 2116,\ 2254,\ 2277,\ 2369,\ 2461,\ 2530,\ 2668,\ 2737,\ 2760,\ 2783,\ 2875,\ 3036,\ 3128,\ 3312,\ 3381,\ 3542,\ 3634\}$ LIM $= 3714$, PGL$(2, 27)+$, Theorems 4.16, 4.18.

5-$(29, 14, m44)$ $2\times$List$(7, 15, 30) \cup \{368,\ 506,\ 874,\ 1012,\ 1380,\ 1518,\ 1886,\ 2024,\ 2530,\ 2622,\ 2806,\ 2898,\ 3036,\ 3404,\ 3496,\ 3542,\ 3634,\ 3726,\ 3910,\ 4048,\ 4416,\ 4554,\ 4692,\ 4876,\ 4922,\ 4968,\ 5060,\ 5244,\ 5428,\ 5566,\ 5796,\ 5934,\ 6072,\ 6118,\ 6440,\ 6578,\ 6900,\ 6946,\ 7084,\ 7176,\ 7360,\ 7452,\ 7590,\ 7774,\ 7866,\ 7958,\ 8096,\ 8188,\ 8464,\ 8602,\ 8694,\ 8970,\ 9016,\ 9108,\ 9476,\ 9614,\ 9844,\ 9982,\ 10074,\ 10120,\ 10488,\ 10626,\ 10672,\ 10948,\ 10994,\ 11132,\ 11362,\ 11500,\ 11638,\ 12006,\ 12144,\ 12512,\ 12650,\ 13018,\ 13110,\ 13248,\ 13524,\ 14030,\ 14168,\ 14674,\ 14766\}$ LIM $= 14858$, PGL$(2, 27)+$, Theorems 4.16, 4.18.

5-$(30, 6, m5)$ $\{1\}$ LIM $= 2$, PSL$(2, 29)$.

5-$(30, 7, m30)$ $\{3{,}5\}$ LIM $= 5$, PSL$(2, 29)$, Theorem 4.8.

5-$(30, 8, m20)$ $\{5,\ 10,\ 15,\ 24,\ 35,\ 40,\ 45,\ 52,\ 55\}$ LIM $= 57$, Theorems 4.16, 4.18.

5-$(30, 9, m10)$ $5\times$List$(6, 9, 30) \cup \{75,\ 105,\ 110,\ 140,\ 150,\ 165,\ 200,\ 215,\ 245,\ 264,\ 285,\ 365,\ 420,\ 440,\ 450,\ 455,\ 515,\ 530,\ 572,\ 605,\ 615\}$ LIM $= 632$, Theorems 4.16, 4.18.

5-$(30, 10, m42)$ $5\times$List$(6, 10, 30) \cup \{440\}$ LIM $= 632$, Theorems 4.16, 4.18.

5-$(30, 11, m1540)$ $\{40\}$ LIM $= 57$, Theorem 4.16.

5-$(30, 12, m220)$ $\{1,\ 345,\ 760,\ 805,\ 920\}$ LIM $= 1092$, Theorems 4.16, 4.18. [1504].

5-$(30, 13, m495)$ $\{345,\ 805,\ 920\}$ LIM $= 1092$, PGL$(2, 27)+$, Theorem 4.18.

5-$(30, 14, m55)$ List$(6, 15, 31) \cup \{98,\ 460,\ 1025,\ 1265,\ 1725,\ 2530,\ 2990,\ 3795,\ 4255,\ 4370,\ 5060,\ 5520,\ 5865,\ 6095,\ 6210,\ 6325,\ 6555,\ 6785,\ 7245,\ 7590,\ 8050,\ 8855,\ 8970,\ 9200,\ 9315,\ 10120,\ 10580,\ 11270,\ 11385,\ 11845,\ 12305,\ 12650,\ 13340,\ 13685,\ 13800,\ 13915,\ 14375,\ 15180,\ 15640,\ 16560,\ 16905,\ 17710,\ 18170\}$ LIM $= 18572$, PGL$(2, 27)+$, [1504] Theorems 4.16, 4.18.

5-$(30, 15, m22)$ $10\times$List$(7, 15, 30) \cup \{392,\ 1840,\ 2530,\ 4100,\ 4370,\ 5060,\ 6900,\ 7590,\ 9430,\ 10120,\ 12650,\ 13110,\ 14030,\ 14490,\ 15180,\ 17020,\ 17480,\ 17710,\ 18170,\ 18630,\ 19550,\ 20240,\ 22080,\ 22770,\ 23460,\ 24380,\ 24610,\ 24840,\ 25300,\ 26220,\ 27140,\ 27830,\ 28980,\ 29670,\ 30360,\ 30590,\ 32200,\ 32890,\ 34500,\ 34730,\ 35420,\ 35880,\ 36800,\ 37260,\ 37950,\ 38870,\ 39330,\ 39790,\ 40480,\ 42320,\ 43010,\ 43470,\ 44850,\ 45080,\ 45540,\ 47380,\ 48070,\ 49220,\ 49910,\ 50370,\ 50600,\ 53130,\ 53360,\ 53820,\ 54740,\ 54970,\ 55660,\ 56810,\ 57500,\ 58190,\ 60030,\ 60720,\ 62560,\ 63250,\ 65090,\ 65550,\ 66240,\ 67620,\ 70150,\ 70840,\ 73370,\ 73830\}$ LIM $= 74290$, Theorems 4.16, 4.18.

5-$(31, 6, m2)$ $\{3{,}5\}$ LIM $= 6$, Theorem 4.16.

5-$(31, 7, m5)$ List$(7, 33, 9) \cup \{15\}$ LIM $= 32$, Theorem 4.16.

5-$(31, 8, m40)$ List$(5, 7, 31) \cup \{18,\ 22\}$ LIM $= 32$, Theorem 4.16.

5-$(31, 9, m10)$ $13\times$List$(6, 9, 31)\cup$List$(6, 10, 32) \cup \{276,\ 299,\ 368,\ 391,\ 460,\ 520,\ 552,\ 575,\ 637,\ 644,\ 667,\ 715,\ 736\}$ LIM $= 747$, Theorems 4.16, 4.18.

5-$(31, 10, m4)$ $13\times$List$(6, 10, 31) \cup \{3795,\ 4554,\ 5313,\ 5566,\ 5720,\ 5808,\ 5850,\ 6864,\ 7029,\ 7557,\ 7865,\ 7995,\ 8096,\ 8184\}$ LIM $= 8222$, Theorems 4.16, 4.18.

5-$(31, 11, m154)$ $\{520\}$ LIM $= 747$, Theorem 4.18.

5-$(31, 12, m440)$ $\{520\}$ LIM $= 747$, Theorem 4.18.

5-$(31, 13, m715)$ $\{345,\ 805,\ 920\}$ LIM $= 1092$, Theorem 4.18.

5-$(31, 14, m1430)$ $\{345,\ 805,\ 920\}$ LIM $= 1092$, Theorem 4.18.

5-$(31, 15, m143)$	List$(6, 16, 32) \cup \{460, 1265, 1725, 2530, 2990, 3795, 4255, 4370, 5060, 5520, 5865, 6095, 6210, 6325, 6555, 6785 7245, 7590, 8050, 8855, 8970, 9200, 9315, 10120, 10580, 11270, 11385, 11845, 12305, 12650, 13340, 13685, 13800, 13915, 14375, 15180, 15640, 16560, 16905, 17710, 18170\}$ LIM $= 18572$, Theorem 4.18.
5-$(32, 6, m3)$	$\{1\}$ LIM $= 4$, PSL$(2, 31)$.
5-$(32, 7, m3)$	$\{12, 27, 45, 57\}$ LIM $= 58$, Theorems 4.16, 4.18.
5-$(32, 8, m5)$	$3\times$List$(6, 9, 33) \cup \{73, 80, 84, 85, 88, 92, 100, 101, 109, 112, 113, 116, 121, 128, 133, 135, 136, 137, 140, 213, 216, 217, 224, 241, 260, 289\}$ LIM $= 292$, AGL$(4, 2) \times C_2$, Theorems 4.16, 4.18.
5-$(32, 9, m90)$	List$(6, 9, 33) \cup \{5, 45, 54, 58, 65, 66\}$ LIM $= 97$, Theorems 4.16, 4.18.
5-$(32, 10, m18)$	$3\times$List$(6, 10, 32) \cup 23\times$List$(6, 10, 33) \cup \{1472, 1560, 2145\}$ LIM $= 2242$, Theorems 4.16, 4.18.
5-$(32, 11, m66)$	$\{1560\}$ LIM $= 2242$, Theorem 4.18.
5-$(32, 12, m198)$	$\{1560\}$ LIM $= 2242$, Theorem 4.18.
5-$(32, 14, m715)$	$\{1035, 2415, 2760\}$ LIM $= 3277$, Theorem 4.18.
5-$(32, 15, m429)$	$\{3105, 7245, 8280\}$ LIM $= 9832$, Theorem 4.18.
5-$(32, 16, m39)$	$9\times$List$(6, 15, 31) \cup \{4140, 11385, 15525, 22770, 26910, 34155, 38295, 39330, 45540, 49680, 52785, 54855, 55890, 56925, 58995, 61065, 65205, 68310, 72450, 79695, 80730, 82800, 83835, 91080, 95220, 101430, 102465, 106605, 110745, 113850, 120060, 123165, 124200, 125235, 129375, 136620, 140760, 149040, 152145, 159390, 163530\}$ LIM $= 167152$, Theorems 4.16, 4.18.
5-$(33, 6, m4)$	$\{1, 2, 3\}$ LIM $= 3$, PGL$(2, 32)$, PΓL$(2, 32)$, [1867].
5-$(33, 7, m42)$	$\{1, 3, 4\}$ LIM $= 4$, PΓL$(2, 32)$, [1867].
5-$(33, 8, m28)$	$\{5, 12, 25, 27, 32, 45, 57\}$ LIM $= 58$, PΓL$(2, 32)$, [1867], Theorems 4.16, 4.18.
5-$(33, 9, m105)$	List$(6, 10, 34) \cup \{8, 11, 12, 45, 80\}$ LIM $= 97$, PGL$(2, 32)$, PΓL$(2, 32)$, Theorems 4.16, 4.18. [1867], Theorems 4.16, 4.18.
5-$(33, 10, m504)$	List$(6, 10, 34) \cup \{5, 45, 58, 65, 66\}$ LIM $= 97$, Theorems 4.16, 4.18.
5-$(33, 11, m84)$	$\{1560, 1725\}$ LIM $= 2242$, Theorems 4.16, 4.18.
5-$(33, 12, m264)$	$\{1560\}$ LIM $= 2242$, Theorem 4.18.
5-$(33, 15, m2002)$	$\{1035, 2415, 2760\}$ LIM $= 3277$, Theorem 4.18.
5-$(33, 16, m1092)$	$\{3105, 7245, 8280\}$ LIM $= 9832$, Theorem 4.18.
5-$(34, 6, m)$	$\{4, 5, 9, 12\}$ LIM=14 , PGL$(2, 23)+$, PΓL$(2, 16) \times C_2$, PGL$(2, 16) \times C_2$ [1867].
5-$(34, 7, m14)$	$\{5, 14\}$ LIM $= 14$, PΓL$(2, 16) \times C_2$, PGL$(2, 16) \times C_2$ [1867].
5-$(34, 9, m21)$	List$(6, 10, 35) \cup \{261\}$ LIM $= 565$, Theorem 4.16.
5-$(34, 10, m21)$	$5\times$List$(6, 10, 35) \cup 29\times$List$(6, 10, 34) \cup \{1305\}$ LIM $= 2827$, Theorems 4.16. 4.18.
5-$(34, 11, m84)$	List$(6, 11, 35)$ LIM $= 2827$, Theorem 4.16.
5-$(34, 12, m12)$	$\{45240\}$ LIM $= 65032$, Theorem 4.18.
5-$(34, 16, m182)$	$\{30015, 70035, 80040\}$ LIM $= 95047$, Theorem 4.18.
5-$(34, 17, m91)$	$\{1 \ldots 40, 90045, 210105, 240120\}$ LIM $= 285142$, Theorems 4.24,4.16, 4.18.
5-$(35, 7, m15)$	$\{5\}$ LIM $= 14$, Theorem 4.18.
5-$(35, 8, m140)$	$\{11\}$ LIM $= 14$, $Sp(6, 2)_{36}$.
5-$(35, 9, m315)$	$\{33, 37\}$ LIM $= 43$, Theorem 4.18.
5-$(35, 10, m126)$	List$(6, 11, 36) \cup \{116, 261, 481, 551\}$ LIM $= 565$, Theorems 4.16, 4.18.
5-$(35, 11, m105)$	List$(6, 66, 35)$ LIM $= 2827$, Theorem 4.16.
5-$(35, 17, m455)$	$\{30015, 70035, 80040\}$ LIM $= 95047$, Theorem 4.18.
5-$(36, 6, m)$	$\{1 \ldots 15\}$ LIM $= 15$, PGL$(2, 17) \times C_2$, [1401].
5-$(36, 7, m15)$	$\{11\}$ LIM $= 15$, $S_9^{[2]}$, graphical design.
5-$(36, 8, m5)$	$\{216, 395, 440\}$ LIM $= 449$, Theorem 4.16.
5-$(36, 9, m35)$	$\{216, 341, 395, 440\}$ LIM $= 449$, $Sp(6, 2)_{36}$, Theorem 4.16.
5-$(36, 10, m63)$	$\{1147\}$ LIM $= 1348$, Theorem 4.18.

5-$(36, 11, m21)$	$31\times$List$(6, 11, 36)$ LIM $= 17530$, Theorem 4.18.
5-$(36, 12, m15)$	$\{3\}$ LIM $= 87652$, Self-dual Code.
5-$(36, 15, m143)$	$\{39\}$ LIM $= 155077$, Self-dual Code.
5-$(36, 18, m35)$	$\{5991, 930465, 2171085, 2481240\}$ LIM $= 2946472$, Self-dual Code, Theorem 4.18.
5-$(37, 6, m4)$	$\{4\}$ LIM $= 4$, Theorem 4.16.
5-$(37, 7, m2)$	$\{88, 124\}$ LIM $= 124$, Theorem 4.18, Theorem 4.65.
5-$(37, 8, m40)$	$\{36, 62\}$ LIM $= 62$, Theorem 4.16.
5-$(37, 9, m10)$	List$(6, 10, 38) \cup 4\times$List$(6, 9, 37)$ LIM $= 1798$, Theorem 4.16.
5-$(37, 10, m56)$	List$(6, 10, 38)$ LIM $= 1798$, Theorem 4.16.
5-$(37, 11, m84)$	$3\times$List$(6, 11, 38)$ LIM $= 5394$, Theorem 4.16.
5-$(37, 12, m24)$	$13\times$List$(6, 12, 38)$ LIM $= 70122$, Theorem 4.16.
5-$(38, 6, m3)$	$\{3,4\}$ LIM $= 5$, PGL$(2, 37)$, [1867].
5-$(38, 7, m6)$	$\{33, 44\}$ LIM $= 44$, PGL$(2, 37)$.
5-$(38, 8, m4)$	List$(6, 10, 39)$ LIM $= 682$, Theorem 4.16.
5-$(38, 9, m30)$	List$(6, 10, 39) \cup \{275, 374, 396, 473, 495, 594\}$ LIM$= 682$, Theorems 4.16, 4.18.
5-$(38, 10, m6)$	$11\times$List$(6, 10, 38) \cup 29\times$List$(6, 10, 39) \cup \{7975, 10846, 11044, 13717, 14355, 17226\}$ LIM $= 19778$, Theorems 4.16, 4.18.
5-$(38, 11, m308)$	List$(6, 11, 39) \cup \{1044\}$ LIM $= 1798$, Theorems 4.16, 4.18.
5-$(38, 12, m396)$	List$(6, 12, 38)$ LIM $= 5394$, Theorem 4.16.
5-$(39, 6, m2)$	$\{8\}$ LIM $= 17$, PSL$(3, 3) \times C_3$.
5-$(39, 8, m8)$	List$(6, 9, 40) \cup \{374\}$ LIM $= 374$, Theorems 4.16, 4.18.
5-$(39, 9, m2)$	List$(6, 10, 40) \cup 31\times$List$(6, 9, 40)$ LIM $= 11594$, Theorem 4.16.
5-$(39, 10, m12)$	List$(6, 10, 40) \cup 11\times$List$(6, 11, 40)$ LIM $= 11594$, Theorem 4.16.
5-$(39, 11, m22)$	$29\times$List$(6, 11, 40) \cup 17\times$List$(6, 11, 39)$ LIM $= 30566$, Theorem 4.16.
5-$(39, 12, m88)$	List$(6, 12, 40)$ LIM $= 30566$, Theorem 4.16.
5-$(40, 9, m70)$	List$(6, 9, 40)$ LIM $= 374$, Theorem 4.16.
5-$(40, 10, m14)$	List$(6, 10, 40)$ LIM $= 11594$, Theorem 4.16.
5-$(40, 11, m770)$	List$(6, 11, 40)$ LIM $= 1054$, Theorem 4.16.
5-$(40, 12, m110)$	List$(6, 12, 40)$ LIM $= 30566$, Theorem 4.16.
6-$(14, 7, m4)$	$\{1\}$ LIM $= 1$, Theorem 4.20.
6-$(19, 7, m)$	$\{4,6\}$ LIM $= 6$, [239].
6-$(19, 9, m2)$	List$(7, 10, 20)$ LIM $= 71$, Theorem 4.16.
6-$(20, 9, m28)$	$\{4\}$ LIM $= 6$, [1337].
6-$(20, 10, m7)$	$\{48, 58, 62, 63, 67, 68\}$ LIM $= 71$, PSL$(2, 19)$, PSL$(3, 4)-$.
6-$(21, 10, m105)$	$\{3,5,6\}$ LIM $= 6$, Theorem 4.16.
6-$(22, 7, m4)$	$\{2\}$ LIM $= 2$, [2014].
6-$(22, 8, m60)$	$\{1\}$ LIM $= 1$, [1350].
6-$(22, 9, m280)$	$\{1\}$ LIM $= 1$, (PSL$(3, 2) \times S_3)+$.
6-$(22, 10, m70)$	$\{5, 12\}$ LIM $= 13$, PSL$(2, 19)++$.
6-$(22, 11, m168)$	$\{5, 6, 9, 10, 11, 12, 13\}$ LIM $= 13$, PGL$(2, 19)++$, Theorems 4.18, 4.20.
6-$(23, 7, m)$	$\{4 \ldots 8\}$ LIM $= 8$, Theorem 4.18.
6-$(23, 8, m4)$	$\{8, 10, 12, 14, 16, 17\}$ LIM $= 17$, Theorems 4.16, 4.18.
6-$(23, 9, m20)$	$\{10, 12, 16, 17\}$ LIM $= 17$, (PSL$(3, 2) \times S_3)+$ Theorem 4.16.
6-$(23, 10, m70)$	$\{6, 9, 10, 12, 15, 16, 17\}$ LIM $= 17$, (PGL$(2, 19) \oplus C_3)+$, Theorem 4.16.
6-$(23, 11, m14)$	$\{55, 63, 64, 67, 72, 73, 78, 82, 85, 87, 90, 94, 99, 100, 103, 105, 108, 109, 112, 114, 117, 118, 123, 127, 130, 132, 135, 139, 144, 145, 148, 150, 152, 153, 154, 156, 157, 159, 162, 163, 168, 172, 175, 180, 184, 189, 190, 195, 198, 199, 204, 207, 208, 213, 217, 220\}$ LIM $= 221$, (PGL$(2, 19) \oplus C_3)+$, Theorems 4.16, 4.18.
6-$(24, 8, m3)$	$\{12, 15, 18, 21, 24\}$ LIM $= 25$, [239].
6-$(24, 9, m24)$	$\{10, 12, 16, 17\}$ LIM $= 17$, Theorems 4.16, 4.18.
6-$(24, 10, m90)$	$\{10, 11, 12, 16, 17\}$ LIM $= 17$, Theorems 4.16, 4.18.
6-$(24, 11, m252)$	$\{6, 9, 10, 11, 12, 15, 16\}$ LIM $= 17$, Theorems 4.16, 4.18.

6-$(24, 12, m42)$	List$(7, 12, 24)$ $\cup$ $\{155, 176, 188, 209, 210, 211, 221\}$ LIM $=$ 221, PSL$(2, 23)$.
6-$(25, 7, m)$	$\{6\}$ LIM $= 9$, Theorem 4.16.
6-$(25, 8, m3)$	$\{12, 15, 18, 21, 24, 27\}$ LIM $= 28$, [239], Theorem 4.16.
6-$(25, 9, m3)$	$\{35, 48, 60, 63, 68, 75, 80, 83, 95, 102, 108, 114, 119, 120, 123, 128, 135, 140, 143, 144, 152, 153, 155\}$ LIM $= 161$, AGL$(2, 5)$, [1867], Theorem 4.16.
6-$(25, 10, m6)$	List$(7, 11, 26) \cup \{190, 304, 323\}$ LIM $= 323$, Theorems 4.16, 4.18.
6-$(25, 11, m18)$	List$(7, 11, 26) \cup$List$(7, 12, 26) \cup \{190, 209, 304\}$ LIM $= 323$, Theorems 4.16, 4.18.
6-$(25, 12, m42)$	List$(7, 12, 26) \cup \{114, 171, 184, 187, 190, 195, 198, 206, 209, 217, 220, 231, 242, 250, 253, 261, 264, 272, 275, 283, 285, 294, 297, 304, 305, 308, 316, 319\}$ LIM $= 323$, Theorems 4.16, 4.18.
6-$(26, 8, m10)$	$\{6, 7\}$ LIM $= 9$, [239].
6-$(26, 9, m60)$	$\{1, 3 \ldots 9\}$ LIM $= 9$, PSL$(2, 25)$, Theorems 4.16, 4.18.
6-$(26, 10, m15)$	List$(7, 11, 27) \cup \{38, 48, 50, 53, 65, 68, 75, 83, 93, 95, 113, 120\}$ LIM $=$ 161, PGL$(2, 25)$, Theorems 4.16, 4.18.
6-$(26, 11, m24)$	$2\times$List$(7, 11, 27) \cup$List$(7, 12, 27) \cup \{190, 226, 316, 321\}$ LIM $= 323$, Theorems 4.16, 4.18.
6-$(26, 12, m60)$	List$(7, 13, 27) \cup$List$(7, 12, 27) \cup \{190, 209, 304, 316\}$ LIM $= 323$, Theorems 4.16, 4.18.
6-$(26, 13, m120)$	List$(6, 12, 25) \cup$List$(7, 13, 27) \cup \{323\}$ LIM $= 323$, Theorems 4.16, 4.18.
6-$(27, 9, m70)$	$\{4, 6, 7, 9\}$ LIM $= 9$, $U(4, 2)$, PΓL$(2, 25)$, [1867], Theorems 4.16, 4.18.
6-$(27, 10, m315)$	$\{3, 4, 7, 9\}$ LIM $= 9$, ASL$(3, 3)^{13}$, [1867], Theorems 4.16, 4.18.
6-$(27, 11, m63)$	List$(7, 11, 27)$ $\cup$ $\{27, 33, 42, 53, 95, 113\}$ LIM$=161$, [1867], Theorems 4.16, 4.18.
6-$(27, 12, m84)$	List$(7, 12, 27) \cup$List$(7, 13, 28) \cup \{52, 54, 135, 178, 187, 190, 234, 241, 282, 304\}$ LIM $= 323$, [1867], Theorems 4.16, 4.18.
6-$(27, 13, m180)$	List$(7, 14, 28)$ LIM $= 323$.
6-$(28, 7, m2)$	$\{3\}$ LIM $= 5$, PSU$(3, 9)$.
6-$(28, 8, m21)$	$\{2 \ldots 5\}$ LIM $= 5$. [1848].
6-$(28, 9, m140)$	$\{2, 3\}$ LIM $= 5$, PSL$(2, 25) \oplus C_2$, Theorem 4.16.
6-$(28, 10, m35)$	$\{24, 26, 27, 29, 30, 32, 33, 35, 36, 38, 39, 41, 42, 44, 45, 47, 48, 50, 54, 57, 62, 63, 66, 72, 74, 77, 80, 83, 84, 89, 90, 92, 93, 98, 99, 101, 102, 104\}$ LIM $= 104$, PΣL$(2, 27)$, PΓL$(2, 25) \oplus C_2$, [1867], Theorems 4.16, 4.18.
6-$(28, 11, m1386)$	$\{3, 6, 7, 9\}$ LIM $= 9$, Theorems 4.16, 4.18.
6-$(28, 12, m231)$	List$(7, 12, 28) \cup \{27, 53, 60, 89, 95, 105, 113, 117, 141, 150, 152, 155\}$ LIM $= 161$, Theorems 4.16, 4.18.
6-$(28, 13, m264)$	List$(7, 14, 29) \cup \{52, 150, 178, 190, 234, 268, 282, 304, 310, 323\}$ LIM $=$ 323, Theorems 4.16, 4.18, 4.65.
6-$(28, 14, m495)$	List$(7, 28, 14) \cup \{323\}$ LIM $= 323$, Theorem 4.65.
6-$(29, 7, m)$	$\{11\}$ LIM $= 11$, PSU$(3, 9)+$.
6-$(29, 8, m)$	List$(7, 9, 30) \cup \{36, 42, 43, 49, 57, 69, 70, 78, 84, 85, 91, 99, 106, 120, 126\}$ LIM $= 126$, [239], Theorems 4.16, 4.18.
6-$(29, 9, m7)$	List$(7, 10, 30) \cup$List$(7, 9, 30) \cup \{15, 18, 22, 36, 42, 46, 58, 66, 67, 69, 70, 85, 102, 112, 114, 118, 120, 126\}$ LIM $= 126$, [239], Theorems 4.16, 4.18.
6-$(29, 10, m35)$	List$(7, 10, 30) \cup \{46, 69, 88\}$ LIM $= 126$, Theorems 4.16, 4.18.
6-$(29, 11, m77)$	$\{69, 138, 152, 161, 207\}$ LIM $= 218$, Theorems 4.16, 4.18.
6-$(29, 12, m231)$	$\{152\}$ LIM $= 218$, Theorem 4.16.
6-$(29, 13, m33)$	List$(7, 14, 30) \cup \{1380, 2047, 2185, 2415, 2599, 2691, 3082, 3243, 3450, 3496, 3565\}$ LIM $= 3714$, Theorems 4.16, 4.18.
6-$(29, 14, m33)$	List$(7, 15, 30)$ LIM $= 7429$, Theorem 4.16.
6-$(30, 7, m12)$	$\{1\}$ LIM $= 1$, [2014].
6-$(30, 8, m12)$	$\{9\}$ LIM $= 11$, PΓL$(2, 27)++$.
6-$(30, 9, m8)$	List$(7, 10, 31) \cup$List$(7, 9, 30) \cup \{36, 42, 69, 70, 78, 85, 99, 120, 126\}$ LIM $= 126$, Theorems 4.16, 4.18.

6-$(30, 10, m42)$	$\mathrm{List}(7, 10, 30) \cup \{36, 42, 46, 64, 69, 85, 112, 118, 126\}$ LIM $= 126$ [239], Theorems 4.16, 4.18.
6-$(30, 11, m1848)$	$\{8\}$ LIM $= 11$, Theorem 4.16.
6-$(30, 12, m308)$	$\{6\}$ LIM $= 8$, Theorem 4.16.
6-$(30, 14, m99)$	$\mathrm{List}(6, 13, 29)$ LIM $= 3714$, Theorems 4.16, 4.18.
6-$(30, 15, m44)$	$2\times$ $\mathrm{List}(7, 15, 30)$ LIM $= 14858$, Theorem 4.16.
6-$(31, 9, m20)$	$\{10, 15, 24, 45, 52\}$ LIM $= 115$, $\mathrm{P\Gamma L}(2, 27) \oplus S_3$, $\mathrm{PGL}(3, 5)$.
6-$(31, 10, m10)$	$5\times\mathrm{List}(7, 10, 31) \cup \{180, 210, 320, 345, 390, 425, 495, 560, 630\}$ LIM $=$ 632, Theorem 4.18.
6-$(31, 15, m55)$	$5\times\mathrm{List}(7, 15, 31) \cup \{6900, 10235, 10925, 12075, 12995, 13455, 15410, 16215, 17250, 17480, 17825\}$ LIM $= 18572$, Theorem 4.18.
6-$(32, 7, m2)$	$\{3, 5\}$ LIM $= 6$, [239], Theorem 4.16.
6-$(32, 8, m5)$	$\mathrm{List}(7, 9, 33)$ LIM $= 32$, Theorem 4.16.
6-$(32, 9, m40)$	$\mathrm{List}(7, 9, 33) \cup \mathrm{List}(7, 10, 33)$ LIM $= 32$, Theorem 4.16.
6-$(32, 10, m10)$	$\{345, 414, 483, 506, 528, 585, 624, 639, 687, 744\}$ LIM $= 747$, $\mathrm{AGL}(4, 2) \times C_2$, Theorem 4.18.
6-$(32, 16, m143)$	$\mathrm{List}(6, 15, 31)$ LIM $= 18572$, Theorem 4.18.
6-$(33, 8, m3)$	$\{12, 45, 57\}$ LIM $= 58$, [1508], Theorem 4.16.
6-$(33, 9, m15)$	$\mathrm{List}(7, 10, 34) \cup 3\times\mathrm{List}(7, 9, 33) \cup \{7, 8, 11, 12, 15, 16, 19, 20, 23, 24, 27, 28, 31, 32, 80\}$ LIM $= 97$, $\mathrm{P\Gamma L}(2, 32)$, Theorem 4.16,
6-$(33, 10, m90)$	$\mathrm{List}(7, 10, 34) \cup \{5, 15, 39, 45, 54, 58, 65, 66\}$ LIM $= 97$, $\mathrm{P\Gamma L}(2, 32)$, Theorems 4.16, 4.18.
6-$(34, 9, m84)$	$\{4, 15, 19\}$ LIM $= 19$, Theorems 4.16, 4.18.
6-$(34, 10, m105)$	$\mathrm{List}(7, 10, 34) \cup \{7, 15, 16, 19, 20, 23, 24, 27, 28, 31, 32, 36, 39, 50, 51, 53, 54\}$ LIM $= 97$, $\mathrm{P\Gamma L}(2, 32)+$, Theorems 4.16, 4.18.
6-$(34, 11, m504)$	$\{75\}$ LIM $= 97$, Theorem 4.16.
6-$(35, 10, m21)$	$\mathrm{List}(7, 11, 36) \cup \{116, 551\}$ LIM $= 565$, Theorems 4.16, 4.18.
6-$(35, 11, m21)$	$5\times\mathrm{List}(7, 11, 36)$ LIM $= 2827$, Theorem 4.16.
6-$(36, 9, m140)$	$\{11\}$ LIM $= 14$, Theorem 4.16.
6-$(36, 10, m315)$	$\{37\}$ LIM $= 43$, $\mathrm{P\Gamma L}(2, 32)+$.
6-$(36, 11, m126)$	$\mathrm{List}(7, 11, 36)$ LIM $= 565$, Theorem 4.18.
6-$(37, 9, m5)$	$\{216, 395, 440\}$ LIM $= 449$, $Sp(6, 2)_{36}+$, Theorem 4.16.
6-$(38, 7, m4)$	$\{4\}$ LIM $= 4$, Theorem 4.65.
6-$(38, 8, m4)$	$\{62\}$ LIM $= 62$, Theorem 4.65.
6-$(38, 9, m40)$	$\{36\}$ LIM $= 62$, Theorem 4.16.
6-$(38, 10, m10)$	$\{648, 680, 972, 1004, 1044, 1296, 1328, 1620, 1652\}$ LIM $= 1798$, Theorem 4.16.
6-$(38, 11, m56)$	$\{648, 680, 972, 1004, 1044, 1296, 1328, 1620, 1652\}$ LIM $= 1798$, Theorem 4.16.
6-$(38, 12, m84)$	$\{1944, 2040, 2916, 3012, 3888, 3984, 4860, 4956\}$ LIM $= 5394$, Theorem 4.16.
6-$(39, 8, m12)$	$\{22\}$ LIM $= 22$, [1350].
6-$(39, 9, m4)$	$\{140, 252, 302, 324, 392, 414, 576, 626\}$ LIM $= 682$, Theorem 4.16.
6-$(39, 10, m30)$	$\mathrm{List}(7, 10, 40)$LIM $= 682$.
6-$(39, 11, m66)$	$\mathrm{List}(7, 11, 39) \cup \{725, 986, 1247, 1305, 1566\}$ LIM $= 1798$. Theorem 4.18.
6-$(39, 12, m308)$	$\mathrm{List}(8, 12, 40)$ LIM $= 1798$.
6-$(40, 9, m8)$	$\{162, 163, 180, 181, 243, 244, 262, 324, 325, 342, 343\}$ LIM $= 374$, $\mathrm{PSL}(4, 3)$.
6-$(40, 10, m2)$	$18\times\mathrm{List}(7, 10, 40) \cup \{648, 1944, 2380, 2430, 3078, 3240, 3888, 4284, 5134, 5184, 5508, 6664, 7038, 9792, 10642\}$ LIM $= 11594$, $\mathrm{PSL}(4, 3)$. Theorems 4.16, 4.18.
6-$(40, 11, m132)$	$17\times\mathrm{List}(7, 11, 40) \cup \{281, 864, 873\}$ LIM $= 1054$, $\mathrm{PSL}(4, 3)$, Theorems 4.16, 4.18.
6-$(40, 12, m22)$	$17\times\mathrm{List}(8, 12, 40)$ LIM $= 30566$, Theorem 4.18.
7-$(20, 10, m2)$	$\{58, 62, 63, 67\}$ LIM $= 71$, [239], Theorem 4.16.
7-$(22, 11, m105)$	$\{3, 5, 6\}$ LIM $= 6$, $\mathrm{PGL}(2, 19)++$ Theorem 4.20.
7-$(24, 8, m)$	$\{4 \ldots 8\}$ LIM $= 8$, [239].

7-$(24, 9, m4)$	$\{10, 12, 21\}$ LIM $= 34$, [239].
7-$(24, 10, m20)$	$\{3, 5, 6\}$ LIM $= 6$, [239].
7-$(24, 12, m14)$	List$(6, 11, 23)$ LIM $= 221$, Theorem 4.20.
7-$(25, 9, m9)$	$\{5, 6, 8\}$ LIM $= 8$, [239].
7-$(25, 10, m24)$	$\{12, 16\}$ LIM $= 17$, [239].
7-$(25, 11, m90)$	$\{11, 12\}$ LIM $= 17$, [239].
7-$(25, 12, m252)$	$\{12\}$ LIM $= 17$, Theorem 4.18.
7-$(26, 8, m)$	$\{6\}$ LIM $= 9$, [239].
7-$(26, 9, m9)$	$\{6, 7, 9\}$ LIM $= 9$, [239].
7-$(26, 10, m3)$	$\{114, 144, 152\}$ LIM $= 161$, Theorem 4.16, [239].
7-$(26, 11, m6)$	$\{180, 196, 216, 226, 228, 256, 286, 288, 316, 321, 322\}$ LIM $= 323$, PGL$(2, 25)$, PΓL$(2, 25)$, Theorems 4.16, 4.18.
7-$(26, 12, m18)$	List$(8, 13, 27) \cup \{216, 228, 322\}$ LIM $= 323$, PΓL$(2, 25)$, Theorems 4.16, 4.18.
7-$(26, 13, m42)$	List$(6, 12, 25)$ LIM $= 323$, Theorem 4.20.
7-$(27, 9, m10)$	$\{6\}$ LIM $= 9$, [239].
7-$(27, 10, m60)$	$\{4, 7, 9\}$ LIM $= 9$, $U(4, 2)$, [239].
7-$(27, 11, m15)$	$\{36, 45, 51, 54, 56, 60, 62, 63, 69, 72, 74, 78, 80, 81, 87, 89, 90, 92, 96, 98 \ldots 101, 105, 107, 108, 110, 114, 116, 117, 119, 123 \ldots 126, 128, 132, 134, 135, 137, 141, 143, 144, 146, 150, 152, 153, 155, 159, 160, 161\}$ LIM $= 161$, ASL$(3, 3)$, $U(4, 2)$, [1867].
7-$(27, 12, m24)$	List$(8, 13, 28) \cup \{79, 81, 106, 108, 133, 160, 162, 180, 189, 214, 216, 228, 256, 268, 270, 286, 322\}$ LIM $= 323$, ASL$(3, 3)$, [1867], Theorem 4.18.
7-$(27, 13, m60)$	List$(8, 13, 28) \cup$List$(8, 14, 28) \cup \{61, 63, 76, 165, 169, 216, 219, 228, 243, 247, 322\}$ LIM $= 323$, ASL$(3, 3)$, [1867], Theorems 4.16, 4.18.
7-$(28, 10, m70)$	$\{9\}$ LIM $= 9$ [239].
7-$(28, 11, m315)$	$\{7, 9\}$ LIM $= 9$, Theorem 4.18.
7-$(28, 12, m63)$	$\{54, 80, 81, 90, 107, 108, 114, 128, 134, 135, 143, 161\}$ LIM $= 161$, Theorem 4.18.
7-$(28, 13, m84)$	List$(8, 13, 28) \cup \{120, 180, 210, 216, 226, 228, 240, 256, 270, 286, 300, 316, 322\}$ LIM $= 323$, $Sp(6, 2)$, Theorems 4.16, 4.18.
7-$(28, 14, m180)$	List$(8, 14, 28) \cup \{48, 52, 61, 63, 76, 102, 115, 117, 120, 126, 128, 130, 139, 156, 165, 168, 169, 182, 190, 193, 196, 198, 209, 210, 212, 216, 219, 224, 226, 228, 232, 238, 240, 243, 247, 254, 268, 270, 273, 294 \ldots 297, 300, 304, 308, 316, 322\}$ LIM $= 323$, $Sp(6, 2)$, Theorems 4.20, 4.18.
7-$(29, 10, m140)$	$\{3\}$ LIM $= 5$ [239].
7-$(29, 11, m385)$	$\{6, 9\}$ LIM $= 9$ PΓL$(2, 27)+$.
7-$(29, 13, m231)$	$\{90, 108, 114, 128, 135, 143, 161\}$ LIM $= 161$, Theorem 4.18.
7-$(29, 14, m264)$	$\{120, 180, 210, 216, 226, 228, 240, 243, 256, 270, 286, 295, 297, 300, 316, 322\}$ LIM $= 323$, Theorem 4.18.
7-$(30, 9, m)$	$\{63, 64, 93, 100, 105, 112\}$ LIM $= 126$ PΓL$(2, 27) \oplus C_2$, Theorem 4.16.
7-$(30, 10, m7)$	List$(8, 10, 31) \cup \{54, 60, 72, 76, 78, 81, 87, 90, 96, 99, 105, 108, 109, 117, 121, 123\}$ LIM $= 126$ PΓL$(2, 27) \oplus C_2$, Theorem 4.16.
7-$(30, 11, m385)$	$\{8\}$ LIM $= 11$ Theorem 4.16.
7-$(30, 12, m77)$	$\{152\}$ LIM $= 218$ PΓL$(2, 27) \oplus C_2$, Theorem 4.16.
7-$(30, 14, m33)$	$23 \times$List$(7, 13, 29)$ LIM $= 3714$ Theorem 4.18.
7-$(30, 15, m33)$	$\{1196, 2760, 4094, 4140, 4370, 4830, 4968, 5198, 5244, 5382, 5520, 5589, 5888, 6164, 6210, 6486, 6578, 6785, 6831, 6900, 6992, 7130, 7268, 7406, 7429\}$ LIM $= 7429$ Theorems 4.65, 4.20, 4.18.
7-$(31, 10, m8)$	$\{60, 93, 100, 105\}$ LIM $= 126$ PSL$(3, 5)$, Theorem 4.18.
7-$(31, 12, m1848)$	$\{8\}$ LIM $= 11$ Theorem 4.18.
7-$(31, 15, m99)$	$\{2070, 2484, 2622, 2944, 3105, 3289, 3703\}$ LIM $= 3714$ Theorem 4.18.
7-$(32, 16, m55)$	List$(6, 15, 31)$ LIM $= 18572$, Theorem 4.20.
7-$(33, 8, m2)$	$\{5\}$ LIM $= 13$ [235].
7-$(33, 9, m5)$	$\{12, 13, 16, 17, 20, 21, 24, 25, 28, 29, 32\}$ LIM $= 32$ PΓL$(2, 32)$.

7-$(33, 10, m40)$	$\{15, 18, 21, 22\}$ LIM $= 32$ PΓL$(2, 32)$.
7-$(34, 9, m9)$	$\{15, 19\}$ LIM $= 19$ PΓL$(2, 32)+$.
7-$(34, 10, m15)$	$\{35, 40, 43, 44, 47, 48, 49, 52, 55, 56, 59, 60, 63, 64, 67, 68, 71, 72, 75, 76, 79, 83, 84, 87, 88, 91, 92, 95, 96\}$ LIM $= 97$ PΓL$(2, 32)+$.
7-$(35, 10, m84)$	$\{15, 19\}$ LIM $= 19$ Theorems 4.16, 4.18.
7-$(35, 11, m105)$	$\{75\}$ LIM $= 97$ Theorem 4.16.
7-$(36, 11, m21)$	$\{160, 200, 216, 235, 240, 251, 256, 275, 280, 291, 296, 315, 320, 336, 355, 360, 371, 376, 395, 400, 411, 416, 435, 440, 451, 456, 475, 480, 491, 496, 515, 520, 531, 555, 560\}$ LIM $= 565$ $Sp(6, 2)_{36}$, Theorem 4.18.
7-$(39, 10, m40)$	$\{36\}$ LIM $= 62$, Theorem 4.16.
7-$(39, 11, m10)$	List$(8, 12, 40) \cup \{1440\}$ LIM $= 1798$, Theorem 4.16.
7-$(39, 12, m56)$	List$(8, 12, 40)$LIM $= 1798$, Theorem 4.16.
7-$(40, 10, m4)$	$\{140, 252, 302, 324, 392, 414, 576, 626\}$ LIM $= 682$, PSL$(4, 3)$.
7-$(40, 11, m330)$	$\{25, 34, 36, 43, 45, 54\}$ LIM $= 62$ PSL$(4, 3)$, Theorem 4.18.
7-$(40, 12, m66)$	List$(8, 12, 40)$ LIM $= 1798$, Theorem 4.16.
8-$(27, 11, m3)$	$\{144\}$ LIM $= 161$, $ASL(3, 3)$.
8-$(27, 12, m6)$	$\{216, 322\}$ LIM $= 323$, $ASL(3, 3)$.
8-$(27, 13, m18)$	$\{178, 180, 256, 282, 286\}$ LIM $= 323$, $ASL(3, 3)$.
8-$(28, 13, m24)$	$\{243, 295, 297\}$ LIM $= 323$, $ASL(3, 3)+$.
8-$(28, 14, m60)$	List$(8, 13, 27) \cup \{234, 310\}$, LIM $= 323$, $ASL(3, 3)+$, Theorem 4.18.
8-$(31, 10, m)$	$\{93, 100\}$ LIM $= 126$, PSL$(3, 5)$, [1401].
8-$(31, 12, m385)$	$\{8\}$ LIM $= 11$, PSL$(3, 5)$.
8-$(36, 11, m84)$	$\{15\}$ LIM $= 19$, $Sp(6, 2)_{36}$.
8-$(40, 11, m40)$	$\{36\}$ LIM $= 62$, PSL$(4, 3)$, [1401].
8-$(40, 12, m10)$	$\{648, 680, 972, 1004, 1296, 1328, 1620, 1652\}$ LIM $= 1798$, PSL$(4, 3)$, [1406].
9-$(28, 14, m18)$	List$(8, 13, 27)$ LIM $= 323$, [1401].

4.47 Remark There are other sporadic examples of t-designs known with $3 \le t \le 5$; see §VII.1.

4.48 Examples The first 6- and small 7-designs were obtained with $G =$PΓL$(2, 32)$ as an automorphism group. This group is generated by the two permutations:

$(1\ 2\ 4\ 8\ g)(3\ 6\ c\ o\ h)(5\ a\ k\ 9\ i)(7\ e\ t\ p\ j)(b\ m\ d\ q\ \ell)(f\ v\ u\ s\ n)$ and
$(1\ i\ v)(2\ \ell\ c)(3\ a\ t)(4\ w\ x)(5\ o\ e)(6\ 7\ h)(8\ p\ s)(9\ j\ k)(b\ f\ d)(g\ n\ u)(m\ 0\ q)$.

Base blocks for one 6-$(33, 8, 36)$ design [1508]:

01234568 01235789 0123569a 1234678c 0123567a 013689ab
0124568a 0134678b 01345789 1234789a 0145678a

Base blocks of one 7-$(33, 8, 10)$ design [235]:

01234589 01234569 01234568 0123456a 01235789 01356789 01345679 0123468a 0123458b
0125679a 012469ab 1245679b 01456789 013678ab 0123567a 01346789 01235689 0123579b
012345ab 01234689 0134579a 0134569a 0125689b 01234679 01345789 01234789 0124579b
012378ab 01245789 013478ab 0124678a 014679ab 134679ac 1234568a 0145678b 0145678a

4.49 Remark Any two distinct designs with the automorphism group from Example 4.48 are pairwise nonisomorphic. There are 1179 6-$(33, 8, 36)$ designs and 4996426 7-$(33, 8, 10)$ designs with this automorphism group. Determining isomorphism types of t-designs with prescribed groups of automorphisms is treated in [1002, 1401, 1402, 1848].

4.50 Remarks Many of the designs in the Table 4.46 were constructed on the computer via a method that employs A_{tk}-matrices. A description of this method is in §VII.6.3. For general references on t-designs, see [1072, 1245].

4.4 Large Sets of t-Designs

4.51 A *large set* of t-(v,k,λ) designs of size N, denoted by $\mathrm{LS}[N](t,k,v)$, is a partition $[(X,\mathcal{B}_i)]_{i=1}^{N}$ of the complete design into N disjoint t-$(v,k,\lambda_{\max}(t,k,v)/N)$ designs. Large sets are also denoted by $\mathrm{LS}_\lambda(t,k,v)$ to emphasize the value of λ.

4.52 An ordered quadruple $(N;t,k,v)$ is *admissible* if the necessary conditions

$$N \Big| \tbinom{v-i}{k-i} \text{ for } 0 \leq i \leq t$$

are fulfilled and it is *realizable* if $\mathrm{LS}[N](t,k,v)$ exists.

4.53 **Remark** Research in large sets aims at determining which admissible quadruples are realizable.

4.54 **Remark** The large sets that are known to exist are:

- An $\mathrm{LS}_{\lambda_{\min}}(1,k,v)$ exists [158, 1059].
- An $\mathrm{LS}_{\lambda_{\min}}(2,3,v)$ exists if and only if $v \neq 7$ [1482, 1483, 1854, 1855, 2008, 2015].
- An $\mathrm{LS}_{\lambda_{\min}}(3,4,v)$ exists if $v \equiv 0 \pmod 3$ [2011].
- An $\mathrm{LS}_{\lambda_{\min}}(4,5,20u+4)$ exists if $\gcd(u,30)=1$ [2014].
- An $\mathrm{LS}_{60}(4,5,60u+4)$ exists if $\gcd(u,60)=1,2$ [2014]
- An $\mathrm{LS}_1(2,4,13)$ exists [498], and an $\mathrm{LS}_1(2,4,16)$ exists [1540].

These are the only known large sets of t-$(v,k,1)$ designs with $t \geq 2$ and $k \geq 4$. Etzion and Hartman [795] constructed $(v-5)$ disjoint 3-$(v,4,1)$ designs for $v = 5 \cdot 2^n$. This leaves only two more to go for a large set!

4.55 **Remark** The importance of large sets in design theory was revealed by Theorem 4.56, that simple t-designs exist for all t.

4.56 **Theorem** [2014] For every natural number t, let $\lambda(t) = \mathrm{lcm}(\binom{t}{m} | m = 1,2,\ldots t))$, $\lambda^*(t) = \mathrm{lcm}(1,2,\ldots t+1)$ and $\ell(t) = \prod_{i=1}^{t} \lambda(i) \cdot \lambda^*(i)$. Then for all $N > 0$, there is an $\mathrm{LS}[N](t, t+1, t+N \cdot \ell(t))$.

4.57 **Remark** The construction of infinite series of large sets mostly concerns a fixed size N and recursive constructions that start from directly constructed large sets. Direct methods mostly prescribe a group of automorphisms.

4.58 If every t-(v,k,λ) design in the large set $[(X,\mathcal{B}_i)]_{i=1}^{N}$ has the group G as an automorphism group, then the large set is a *uniformly-G* $\mathrm{LS}[N](t,k,v)$.

4.59 **Example** A uniformly-G $\mathrm{LS}[3](3,5,13)$ is given by the group

$$G = \langle (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ a\ b\ c), (2\ 4\ 9)(3\ 7\ 6)(5\ 0\ b)(8\ 9\ c) \rangle$$

and the base blocks:

Design 1: 12357 12359 1238a 1248a 1246b 1245c 12345 12468 12678 12459 1234b
Design 2: 12456 12467 12349 1235c 12347 12378 12389 1235b 1239b 1246c 12350
Design 3: 12457 12348 12478 12379 1237c 12356 12358 12368 12469 1234a 1234c

4.60 **Remark** Let a group G act on a set X with only one orbit on t-subsets of X. If the orbits on k-subsets can be combined to a_d families of size $\frac{|G|}{d}$ each for some divisors d of $|G|$ such that a natural number N divides each a_d, then an $\mathrm{LS}[N](t,k,v)$ can be constructed. This has been used with $G = \mathrm{PGL}(2,p^f)$ or $\mathrm{PSL}(2,p^f)$ when $p^f \equiv 3 \pmod 4$ to obtain infinitely many $\mathrm{LS}[N](3,k,v)$. See [625, 1404, 1405].

4.61 **Remark** The basic recursion techniques for large sets utilize the following results. For a detailed account, see [1294].

4.62 **Theorem** [1294] If an $\mathrm{LS}[N](t,k,v)$ exists, then there exists an $\mathrm{LS}[N](t-i,k-j,v-l)$ for $0 \leq j \leq l \leq i \leq t$.

4.63 Theorem [71] If an LS$[N](t,k,v)$ and an LS$[N](t,k+1,v)$ exist, then there exists an LS$[N](t,k+1,v+1)$.

4.64 Theorem [71] If LS$[N](t,i,v)$ exist for $t<i\le k$ and an LS$[N](t,k,u)$ exists, then there exist LS$[N](t,k,u+l(v-t))$ for all $l\ge 1$.

4.65 Theorem [69] Let p be a prime. If an LS$[p](t,k,v-1)$ exists, then there exists an LS$[p](t,pk+i,pv+j)$ for $-p\le j<i<p-1$.

4.66 Theorem [69] Let p be a prime. If an LS$[p](t,k,v-1)$ exists, then there exists an LS$[p](t+1,pk+i,pv+j)$ for all $0\le j<i<p-1$.

4.67 Remark For fixed p, t, and k there are finitely many admissible quadruples $(p;t,k,v)$, *root cases* [1294], such that if they are realizable, then all admissible quadruples $(p;t,k,v)$ are realizable.

4.68 Theorem [1294]

1. Let t,k,s be positive integers such that $2^{s-1}\le t<2^{s+1}-1$ and $t\le k$. Assume that LS$[2](t,2^n+j,2^{n+1}+t)$ exist for all j,n such that $0\le j\le \lfloor t/2\rfloor$ and $t+1\le 2^n+j\le k$. Then there exist LS$[2](t_1,k_1,v)$ for all $2^s-1\le t_1\le t$ and $t_1<k_1\le k$ and admissible v.
2. Let p be an odd prime and t,k,s nonnegative integers such that $p^s-1\le t<p^{s+1}-1$ and $t<k$. Let $v'=p^{s+1}+t$. Assume that LS$[p](t,k',v')$ exist for all $t<k'<min(k,v'/2)$ and LS$[p](t,ip^n+j,p^{n+1}+t)$ exist for all i,j,n such that $0\le j\le t,\ 1\le i\le (p-1)/2,\ ip^n+j\le k,\ n>s$. Then all admissible quadruples $(p;t,k,v)$, with $p^s-1\le t_1\le t$ and $t_1<k_1\le k$, are realizable.

4.69 Remark All quadruples $(5;2,3,7)$, $(7;3,4,10)$, $(14;3,5,11)$, $(7;4,5,11)$, $(11;4,5,15)$ are admissible but not realizable. Also, the admissible quadruples that would be extensions of these large sets are not realizable.

4.70 Conjecture All admissible $(2;t,k,v)$, *halvings*, are realizable (Hartman). All admissible $(3;t,k,v)$, for $t\le 4$ are realizable (Khosrovshahi). All admissible $(4;t,k,v)$ are realizable for $t\le 3$ (Khosrovshahi).

4.71 Table Parameter sets that are realizable if they are admissible ($\star$ means all admissible values).

N	t	k	v	Reference
$\star$	1	$\star$	$\star$	[158, 1059]
$\star$	2	3	$\neq 7$	[1195, 1482, 1483, 1854, 1855, 2008, 2015]
2	2	$\star$	$\star$	[70]
2	≤ 5	≤ 15	$\star$	[70, 71, 1059, 1400]
2	6	7, 8, 9	$\star$	[70, 1400]
3	2	≤ 80	$\star$	[1293]
3	3	≤ 80	$\star$	[1405]
3	4	≤ 10	$\star$	[1405]
4	2, 3	≤ 7	$\star$	[1289]
5	2	≤ 8	$\neq 7$	[1405]
5	3	≤ 6	$\neq 8$	[1405]
7	2	≤ 7	$\star$	[1405]
7	3	≤ 7	$\neq 10$	[1405]
11	2	≤ 10	$\star$	[1405]
13, 17, 19, 23	2	3, 4	$\star$	[1405]
29	2	≤ 29	$\star$	[1405]

4.72 Table Realizable parameters of large sets with $v \leq 30$. When $\{N_1, \ldots, N_r\}$ is given as $a_1 \cdot a_2 \cdots a_\ell$, the large set exists for $N = \prod_{i=1}^{\ell} a_i$, and hence also for every one of its divisors.

v	$(t, k, \{N_1, \ldots, N_r\})$
6	(2,3,{2})
8	(2,4,{5})
9	(2,3,{7}), (2,4,{7})
10	(2,3,{2}), (2,4,{2 · 7}), (2,5,{2 · 7}), (3,5,{7})
11	(2,3,{3}), (2,4,{2 · 3}), (2,5,{2 · 3 · 7}), (3,4,{2}), (3,5,{2, 7})
12	(2,3,{5}), (2,4,{3, 5}), (2,5,{2 · 3}), (2,6,{2 · 3 · 7}), (3,4,{3}), (3,5,{2 · 3}), (3,6,{2 · 3 · 7}), (4,5,{2}), (4,6,{2})
13	(2,3,{11}), (2,4,{5 · 11}), (2,5,{3, 11}), (2,6,{2 · 3, 11}), (3,4,{5}), (3,5,{3}), (3,6,{2 · 3}), (4,5,{3}), (4,6,{2, 3}), (5,6,{2})
14	(2,3,{2}), (2,4,{11}), (2,5,{11}), (2,6,{3, 11}), (2,7,{4, 2 · 3, 3 · 11, 2 · 11})$C_{13}+$, (3,6,{3}), (3,7,{2 · 3, 11}) $C_{13}+$, (4,6,{3}), (4,7,{2, 3}), (5,7,{2, 3}), (6,7,{2})
15	(2, 3, {13}), (2, 4, {13}), (2, 5, {11}), (2, 6, {11}), (2, 7, {3, 11, 13})C_{15}, (3, 7, {3}), (4, 7, {3})
16	(2, 3, {7}), (2, 4, {7 · 13}), (2, 5, {7}), (2, 6, {7, 11}), (2, 7, {11}), (3, 8, {3, 11, 13}), (4,8,{3}), (5,8,{3})
17	(2,3,{5}), (2,4,{5, 7}), (2,5,{7}), (2,6,{7}), (2,7,{11}), (2,8,{5, 11}), (3,4,{7}), (3,5,{7}), (3,6,{7})
18	(2,3,{4}), (2,4,{2, 5}), (2,5,{2, 7}), (2,6,{2, 7}), (2,7,{2}),(2,8,{2, 11}), (2,9,{2, 5, 11}), (3,4,{5}), (3,5{7}), (3,6,{7}), (3,9,{5, 11})
19	(2,3,{17}), (2,4,{4, 17}), (2,5,{4, 17}),(2,6,{7, 4, 17}), (2,7,{4, 17})$C_{19}C_3$, (2,8,{2, 13 · 17}), (2,9,{2, 11}), (3,4,{4}), (3,5,{4}), (3,6,{7, 4}), (3,7,{4}) $C_{17}C_4{+}{+}$, (3,8,{2}), (3,9,{2})
20	(2,3,{3}), (2,4,{3, 17}), (2,5,{3, 4, 17}), (2,6,{3, 4, 17}), (2,7,{3, 4, 17}), (2,8,{3, 17}), (2,10,{2, 11}), (3,5,{4}), (3,6,{4}), (3,7,{4}), (3,8,{2}), (3,9,{2}), (3,10,{2, 11}), (4,5,{2}), (4,6,{2}), (4,7,{2}), (4,8,{2}), (4,9,{2}), (4,10,{2})
21	(2,3,{19}), (2,4,{3, 19}), (2,5,{3, 17}), (2,6,{3, 17}), (2,7,{3, 4, 17}), (2,8,{3, 17}), (3,4,{3}), (3,5,{3}), (3,6,{3, 4}), (3,7,{3, 4}), (3,8,{2, 3}), (3,9,{2}), (3,10,{2}), (4,6,{2}), (4,7,{2}), (4,8,{2}), (4,9,{2}), (4,10,{2}), (5,6,{2}), (5,7,{2}), (5,8,{2}), (5,9,{2})
22	(2,3,{2, 5}), (2,4,{2, 5, 19}), (2,5,{2, 3}), (2,6,{2, 3, 17}), (2,7{2, 3, 17}), (2,8,{2, 3, 5, 17}), (2,9,{2, 5}), (2,10,{2}), (3,5,{3}), (3,6,{3}), (3,7,{3, 4}), (3,8,{2, 3}), (3,9,{2}), (3,10,{2}), (3,11,{2}), (4,5,{3}), (4,6,{3}), (4,7,{2, 3}), (4,8,{2, 3}), (4,9,{2}), (4,10,{2}), (4,11,{2}), (5,7,{2}), (5,8,{2}), (5,9,{2}), (5,10,{2}), (5,11,{2}), (6,7,{2}), (6,8,{2})
23	(2,3,{7}), (2,4,{2, 7 · 5}), (2,5,{2, 7 · 19}), (2,6,{2, 3 · 7 · 19}), (2,7,{2, 3 · 17 · 19}), (2,8,{2, 3 · 17 · 19}), (2,9,{2, 5 · 17 · 19}), (2,10,{2, 7 · 17 · 19}), (2,11,{2}), (3,4,{5}), (3,6,{3}), (3,7,{3}), (3,8,{2, 3}), (3,9,{2, 5}), (3,10,{2}), (3,11,{2}), (4,6,{3}), (4,7,{3}), (4,8,{2, 3}), (4,9,{2}), (4,10,{2}), (4,11,{2}), (5,6,{3}), (5,8,{2}), (5,9,{2}), (5,10,{2}), (5,11,{2}), (6,8,{2}), (6,9,{2}), (6,10,{2})
24	(2,3,{11}), (2,4,{7, 11}), (2,5,{2, 7, 11}), (2,6,{2, 7, 11, 19}), (2,7,{2, 3, 11, 19}), (2,8,{2, 3, 11, 17, 19}), (2,9,{2, 11, 17, 19}), (2,10,{2, 11, 17, 19}),(2,11,{2}),(2,12,{2}), (3,4,{7}), (3,5,{7}), (3,6,{7}), (3,7,{3 · 19}),(3,8,{3}), (3,9,{2}), (3,10,{2, 17 · 19}), (3,11,{2}), (3,12,{2}), (4,7,{3}), (4,8,{3}), (4,9,{2}), (4,10,{2}), (4,11,{2}), (4,12,{2}), (5,7,{3}), (5,8,{3}), (5,9,{2}), (5,10,{2}), (5,11,{2}), (5,12,{2}), (6,9,{2}), (6,10,{2}), (6,12,{2}), (7,10,{2}).
25	(2,3,{23}), (2,4,{11, 23}), (2,5,{7, 11}), (2,6,{2, 7, 11}), (2,7,{2, 3, 11, 19}), (2,8,{2, 3, 11, 19}), (2,9,{2, 11, 17, 19}), (2,10,{2, 11, 17, 19}), (2,11,{2, 17, 19, 23}), (2,12,{2}), (3,5,{7}), (3,6,{7}), (3,8,{3}), (3,10,{2}), (3,11,{2}), (3,12,{2}), (4,8,{3}), (4,10,{2}), (4,11,{2}), (4,12,{2}), (5,8,{3}), (5,10,{2}), (5,11,{2}), (5,12,{2}), (6,10,{2})

v	$(t, k, \{N_1, \ldots, N_r\})$
26	(2,4,{23}), (2,5,{11}), (2,6,{7, 11}), (2,7,{2, 11}), (2,8,{2, 11, 19}), (2,9,{2, 11, 19}), (2,10,{2, 11, 17, 19}), (2,11,{2, 17, 19}), (2,12,{2}), (2,13,{2}), (3,6,{7}), (3,11,{2}), (3,12,{2}), (3,13,{2}), (4,11,{2}), (4,12,{2}), (4,13,{2}), (5,11,{2}), (5,12,{2}), (5,13,{2}), (6,13,{2})
27	(2,3,{5}), (2,4,{2, 25}), (2,5,{2, 5 · 23, 11}), (2,6,{5, 11}), (2,7,{5 · 11 · 23}), (2,8,{25 · 11 · 23}), (2,9,{2, 11, 19}), (2,10,{2, 5 · 11 · 19 · 23}), (2,11,{2, 5 · 17 · 19 · 23}), (2,12,{2, 5}), (2,13,{2}), (3,4,{2}), (3,5,{2}), (3,6,{2}),(3,7,{2}), (3,12,{2}), (3,13,{2}), (4,12,{2}), (4,13,{2}), (5,12,{2}), (5,13,{2})
28	(2,3,{13}), (2,4,{5, 13}), (2,5,{5}), (2,6,{5}, (2,7,{5, 11},(2,8,{5, 11, 23}, (2,9,{11}), (2,10,{2, 11, 19}), (2,11,{2, 5 · 19 · 23}), (2,12,{2, 5}), (2,13,{2}), (2,14,{2}), (3,4,{5}), (3,5,{2, 5}), (3,6,{2, 5}), (3,7,{2}), (3,8,{5}), (3,11,{5 · 19 · 23}), (3,12,{5}), (3,13,{2}), (3,14,{2}), (4,5,{2}), (4,6,{2}), (4,7,{2}), (4,13,{2}), (4,14,{2}), (5,13,{2}), (5,14,{2}), (6,13,{2}), (6,14,{2})
29	(2,3,{3}), (2,4,{3, 13}), (2,5,{3, 5}), (2,6,{3, 5, 13}), (2,7,{3, 5}), (2,8,{3, 5, 11}),(2,9,{3, 11}),(2,10,{3, 5, 11, 13, 23}),(2,11,{2, 3, 5, 13, 19, 23}), (2,12,{2, 3, 5}), (2,13,{2, 3, 5}), (2,14,{2, 3}), (3,5,{5}),(3,6,{2, 5}), (3,7,{2}), (3,12,{5}),(3,14,{2}), (4,6,{2}),(4,7,{2}), (4,14,{2}), (5,6,{2}), (5,7,{2}), (5,14,{2}), (6,14,{2})
30	(2,3,{7}), (2,4,{3, 7}), (2,5,{3, 7}), (2,6,{3, 5, 7}), (2,7,{3, 5}), (2,8,{3, 5}), (2,9,{3, 11}), (2,10,{3, 11}), (2,11,{3, 5, 13, 23}), (2,12,{2, 3, 5}), (2,13,{2, 3, 5}), (2,14,{2, 3}), (2,15,{2, 3}), (3,4,{3}), (3,5,{3}), (3,6,{3, 5}), (3,7,{2, 3}), (3,8,{3}), (3,9,{3}), (3,10,{3}), (3,11,{3, 5, 13, 23}), (3,12,{3, 5}), (3,13,{3, 5}), (3,14,{3}), (3,15,{2}), (4,7,{2}), (4,15,{2}), (5,7,{2}), (5,15,{2}), (6,7,{2}), (6,15,{2})

4.73 Remark Several parameter sets in Table 4.72 are followed by a uniform automorphism group of the large set, obtained using `DISCRETA` [241]. Many LS$[N](t, k, v)$s for $t \leq 3$ are obtained by prescribing AGL$(1, q)$ and PSL$(2, q)$ as groups of automorphisms; these groups are not noted. There are some remarkable large sets not in the scope of the table. There exist LS[3]$(6, 10, 33)$ and LS[13]$(6, 10, 33)$ with uniform automorphism group PΓL$(2, 32)$. The first has been used to show that admissible LS[3]$(3, k, v)$ are realizable for $k \leq 80$.

See Also

§II.5	Steiner systems, t-designs with index one.
§II.7	Resolvable designs.
§V.1	Hadamard designs and matrices.
§VI.63	t-wise balanced designs.
§VII.1	Codes.
§VII.9	Group theory.
§VII.6.3	Computer algorithms for finding t-designs.
[241]	`DISCRETA`, a tool for constructing t-designs.
[1294]	Large sets of t-designs through partitionable sets: A survey.
[1404]	New large sets of t-designs.

References Cited: [69, 70, 71, 75, 76, 120, 128, 158, 166, 172, 226, 235, 239, 241, 252, 253, 256, 257, 289, 291, 333, 421, 467, 498, 625, 691, 695, 753, 795, 858, 1002, 1009, 1035, 1045, 1059, 1072, 1145, 1152, 1175, 1195, 1211, 1245, 1289, 1291, 1292, 1293, 1294, 1320, 1333, 1335, 1337, 1338, 1340, 1342, 1343, 1350, 1351, 1352, 1354, 1355, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1453, 1482, 1483, 1504, 1508, 1509, 1540, 1574, 1588, 1621, 1692, 1783, 1848, 1854, 1855, 1867, 1868, 2008, 2011, 2012, 2014, 2015, 2016, 2068, 2069, 2072, 2147, 2159]

5 Steiner Systems

Charles J. Colbourn
Rudolf Mathon

5.1 Basics

5.1 Given three integers t, k, v such that $2 \le t < k < v$, a *Steiner system* $S(t, k, v)$ is a v-set V together with a family $\mathcal{B}$ of k-subsets of V (*blocks*) with the property that every t-subset of V is contained in exactly one block. Equivalently, an $S(t, k, v)$ is a t-$(v, k, 1)$ design.

5.2 **Remark** The nineteenth century geometer Jakob Steiner posed the question of the existence of Steiner systems. Unaware of the earlier work of Kirkman, in 1853 Steiner first asked about $S(2, 3, v)$:

Steiner's Combinatorische Aufgabe:

Welche Zahl, N, von Elementen hat die Eigenschaft, dass sich die Elementen so zu dreien ordnen lassen, dass je zwei in einer, aber nur in einer Verbindung vorkommen?

Steiner went on to ask about $S(t, t+1, v)$ systems.

5.3 **Remark** Suppose that an $S(t, k, v)$ exists. By choosing an element x, selecting all blocks containing x, and deleting x from each, one obtains an $S(t-1, k-1, v-1)$, a *derived design*.

5.4 **Lemma** (Numerical or Divisibility Conditions) An $S(t, k, v)$ exists only if $\binom{v-i}{t-i}/\binom{k-i}{t-i}$ is an integer for every $i = 0, 1, \ldots, t-1$. When $k = t+1$, this is equivalent to requiring that $\gcd(v-t, \mathrm{lcm}(1, 2, ..., t+1)) = 1$.

5.5 **Theorem** [1684] An $S(t, k, v)$ exists only if $\binom{k}{t-1}\frac{k-t}{v-k-1} \le \left\lfloor \frac{k}{t-1} \left\lfloor \frac{k-1}{t-2} \left[\cdots \left\lfloor \frac{k-t+3}{2} \right\rfloor \cdots \right] \right\rfloor \right\rfloor$ and $\binom{k}{k-t+1}\frac{k-t}{v-k-1} \le \left\lfloor \frac{k}{k-t+1} \left\lfloor \frac{k-1}{k-t} \left[\cdots \left\lfloor \frac{t+1}{2} \right\rfloor \cdots \right] \right\rfloor \right\rfloor$.

5.6 **Theorem** [761, 1783] Let $t = 2h + \beta$ for an integer h and β equal 0 or 1. Then an $S(t, k, v)$ exists only if $\binom{v}{t} \ge \left(\frac{v}{k}\right)^{\beta} \binom{v-\beta}{h}\binom{k}{t}$. Consequently an $S(t, k, v)$ exists only if $\binom{v}{t} \ge \binom{v}{\lfloor t/2 \rfloor}\binom{k}{t}$.

5.7 **Remark** For the Steiner system $S(5, 8, 24)$, one has $h = 2$ and $\beta = 1$, and the inequality of Theorem 5.6 is attained.

5.2 Infinite Families

5.8 An $S(2, 3, v)$ is a *Steiner triple system* STS(v). See §2.

5.9 **Remark** See §II.3 and §II.1.2 for existence results and examples of small $S(2, k, v)$.

5.10 An $S(3, 4, v)$ is a *Steiner quadruple system* SQS(v). See §5.5.

5.11 Theorem Known infinite families of $S(t,k,v)$ are

1. $S(2,q,q^n)$, q a prime power, $n \geq 2$ (affine geometries, see §VII.2.4);
2. $S(3,q+1,q^n+1)$, q a prime power, $n \geq 2$ (spherical geometries);
3. $S(2,q+1,q^n+\cdots+q+1)$, q a prime power, $n \geq 2$ (projective geometries, see §VII.2.3);
4. $S(2,q+1,q^3+1)$, q a prime power (unitals, see §VII.2.12);
5. $S(2,2^r,2^{r+s}+2^r-2^s)$, $2 \leq r < s$ (Denniston designs).

5.12 Theorem (Wilson, see [281]) Let q be a prime power. If an $S(3,q+1,v+1)$ and an $S(3,q+1,w+1)$ both exist, then there exists an $S(3,q+1,vw+1)$.

5.13 Corollary [1043] If q is a prime power and an $S(3,q+1,v+1)$ exists, then an $S(3,q+1,qv+1)$ exists.

5.14 Theorem [1043] If an $S(3,6,v)$ exists, then an $S(3,6,4v-2)$ exists.

5.15 Theorem [281] Let q be a prime power, and let u be a prime power satisfying the standard divisibility conditions. Then there is a constant n_0 depending only on q and u so that, for all $\ell \geq 0$ and $n \geq n_0$, there exists an $S(3,q+1,u^\ell q^n+1)$.

5.16 Remarks

1. Only finitely many $S(t,k,v)$ with $t > 3$ are known and none are known for $t \geq 6$.
2. See [1621] for recursive constructions of Steiner 3-designs using *candelabra systems*.

5.3 Existence Table

5.17 Table Parameters for $S(t,k,t+n)$ with $n \leq 200$. The column headed $t \leq$ gives the maximum value of t for which numerical necessary conditions are met and Theorem 5.6 holds. $\exists$ gives the largest $t \geq 2$ for which a system in the family is known. $\not\exists$ gives the smallest t in the admissible range for which the system is known *not* to exist. For example, the first entry in the fourth column of the table ($n = 13, t \leq 11, \exists = 3$) indicates that there exists an $S(3,4,16)$ (hence an $S(2,3,15)$) and that it is possible according to the necessary conditions that there exists an $S(t,t+1,t+13)$ for all $t \leq 11$. The table was constructed using the infinite families and recursive constructions of §5.2, along with the following remarks:

1. For results on designs with $t = 2$, also see §II.3.
2. All designs with $t = 5$ are displayed in §5.6, and all parameters of known Steiner 4-designs are derived from the known Steiner 5-designs.
3. The nonexistence of $S(4,5,15)$ and $S(4,6,18)$ (see [225]), $S(4,10,66)$ [1011], and $S(3,13,145)$ [678] has been established.

n	$t \leq$	$\exists$	$\not\exists$	n	$t \leq$	$\exists$	$\not\exists$	n	$t \leq$	$\exists$	$\not\exists$	n	$t \leq$	$\exists$	$\not\exists$	n	$t \leq$	$\exists$	$\not\exists$
$k = t+1$																			
5	3	3		7	5	5		11	9	3	4	13	11	3		17	15	3	
19	17	5		23	21	3		25	3	3		29	27	3		31	29	5	
35	3	3		37	35	3		41	39	3		43	41	5		47	45	3	
49	5	3		53	51	3		55	3	3		59	57	3		61	59	3	
65	3	3		67	65	5		71	69	3		73	71	3		77	5	3	
79	77	3		83	81	3		85	3	3		89	87	3		91	5	3	
95	3	3		97	95	3		101	99	3		103	101	5		107	105	3	
109	107	3		113	111	3		115	3	3		119	5	3		121	9	3	
125	3	3		127	125	5		131	129	3		133	5	3		137	135	3	

n	$t \le$	$\exists$	$\not\exists$	n	$t \le$	$\exists$	$\not\exists$	n	$t \le$	$\exists$	$\not\exists$	n	$t \le$	$\exists$	$\not\exists$	n	$t \le$	$\exists$	$\not\exists$
k = t + 1 (continued)																			
139	137	3		143	9	3		145	3	3		149	147	3		151	149	3	
155	3	3		157	155	3		161	5	3		163	161	5		167	165	3	
169	11	3		173	171	3		175	3	3		179	177	3		181	179	3	
185	3	3		187	9	3		191	189	3		193	191	3		197	195	3	
k = t + 2																			
11	2	2		14	4	3	4	23	8	5		26	2	2		35	2	2	
38	16	2		47	20	2		50	2	2		59	26	2		62	28	3	
71	2	2		74	34	2		83	38	2		86	2	2		95	2	2	
98	4	3		107	50	2		110	2	2		119	4	2		122	8	2	
131	2	2		134	4	2		143	8	2		146	2	2		155	2	2	
158	76	2		167	80	2		170	2	2		179	86	2		182	4	2	
191	2	2		194	94	2													
k = t + 3																			
19	5	5		23	3	3		39	9	2		43	3	2		59	15	2	
63	3	2		79	3	2		83	5	3		99	3	3		103	13	3	
119	3	2		123	7	3		139	19	2		143	7	2		159	49	2	
163	3	2		179	55	2		183	3	2									
k = t + 4																			
29	2	2		34	3		2	44	2			49	2			59	2		
64	2	2		74	3	2		79	2			89	3	2		94	2	2	
104	3	2		109	4	2		119	2	2		124	6	2		134	2	2	
139	3			149	2	2		154	2	2		164	2	2		169	2	2	
179	3	2		184	2	2		194	3										
k = t + 5																			
41	2		2	47	3	3		83	2			89	2	2		125	5		
131	2			167	5	2		173	3										
k = t + 6																			
55	2	2		62	12	3	4	111	2			118	2	2		167	2		
174	2																		
k = t + 7																			
71	2	2		79	3	3		143	3			151	2						
k = t + 8																			
89	2	2		98	4		2	134	2			143	2			179	2		
188	2																		
k = t + 9								**k = t + 10**											
109	3		2	119	3	3		131	2	2		142	3		3	175	2		
k = t + 11								**k = t + 12**											
155	2			167	4	3		181	2	2		194	3		2				

5.4 Intersection Triangles

5.18 Let $(V, \mathcal{B})$ be an $S(t, k, v)$ and let $B \in \mathcal{B}$. Let i and j be nonnegative integers with $i+j \le k$, and let I and O be disjoint subsets of B of sizes i and j, respectively. Then the *i, j-intersection number* $\lambda_{i,j}$ is the number of blocks that contain all elements of I and no elements of O. The array $(\lambda_{i,j} : 0 \le i + j \le k)$ is the *intersection triangle* of the design.

5.19 **Construction** The definition of $\lambda_{i,j}$ does not depend on the choice of B, I, or O, because $\lambda_{i,j}$ can be computed as follows. By definition,

$$\lambda_{i,0} = \begin{cases} \binom{v-i}{t-i}/\binom{k-i}{t-i} & \text{when} \quad 0 \le i \le t \\ 1 & \text{when} \quad t < i \le k \end{cases}$$

and since $\lambda_{i,j-1} = \lambda_{i+1,j-1} + \lambda_{i,j}$, for all $j \ge 1$ and $1 \le i + j \le k$, one can calculate $\lambda_{i,j} = \lambda_{i+1,j-1} - \lambda_{i,j-1}$.

5.20 **Example** The intersection triangle for $S(5, 8, 24)$. See Table 5.37.

759	506	330	210	130	78	46	30	30
253	176	120	80	52	32	16	0	
77	56	40	28	20	16	16		
21	16	12	8	4	0			
5	4	4	4	4				
1	0	0	0					
1	0	0						
1	0							
1								

5.21 **Remark** The number x_i of blocks that intersect a fixed block B in exactly i elements is $\binom{k}{i}\lambda_{i,k-i}$, and hence does not depend on B. Thus, for example, in an $S(5, 8, 24)$, for every block B, one finds 30 disjoint blocks, 448 blocks intersecting B in two elements, and 280 blocks intersecting B in four elements.

5.22 **Theorem** [988] For an $S(t, k, v)$, if $x_i = 0$ and $0 \le i < t$, then

1. $i = 0$ and the design is one of $S(4, 7, 23)$, $S(t, t + 1, 2t + 3)$ when $t + 3$ is prime, or a projective plane $S(2, q + 1, q^2 + q + 1)$;
2. $i = 1$ and the design is one of $S(3, 6, 22)$, $S(5, 8, 24)$, or $S(t, t + 1, 2t + 2)$ when $t + 2$ is prime;
3. $i = 2$ and the design is $S(4, 7, 23)$; or
4. $i = 3$ and the design is $S(5, 8, 24)$.

5.23 **Remark** An analogous definition of intersection triangles can be made for t-designs with $\lambda > 1$; however, in that case, because the intersection numbers $\lambda_{i,0}$ for $i > t$ may depend on the block B and sets I and O chosen, one cannot guarantee that $\lambda_{i,j}$ for $t < i + j \le k$ is a constant. However, when $i + j \le t$, the intersection numbers for t-designs in general are again independent of the block and sets chosen.

5.5 Steiner Quadruple Systems

5.24 **Theorem** An SQS(v) (a 3-$(v, 4, 1)$ design) exists if and only if $v \equiv 2, 4 \pmod 6$.

5.25 **Remark** Theorem 5.24 can be proved using six recursive constructions: If there is an SQS(v), then SQS($2v$), SQS($3v - 2$), SQS($4v - 6$), and SQS($12v - 10$) all exist. If, in addition, $v \equiv 2 \pmod{12}$, then an SQS($3v - 8$) also exists. If instead $v \equiv 10 \pmod{12}$, then an SQS($3v - 4$) exists. These constructions, together with an SQS(14) and a certain SQS(38), suffice to prove existence. See [1063].

5.26 **Example** The unique SQS(10) is a graphical design. See Table §VI.26.7. A SQS(16) is given by Construction VI.63.49.

5.27 Let $V = \mathbb{Z}_2^n$, $n \ge 3$. Let $\mathcal{B}$ be the set of all sets of four distinct elements of V whose (vector) sum is zero. Then $(V, \mathcal{B})$ is an SQS(2^n), the *boolean quadruple system* of order 2^n.

5.28 **Example** The boolean quadruple system of order 8; the unique SQS(8).

000 001 010 011	000 001 100 101	000 001 110 111	000 010 100 110
000 010 101 111	000 011 100 111	000 011 101 110	100 101 110 111
010 011 110 111	010 011 100 101	001 011 101 111	001 011 100 110
001 010 101 110	001 010 100 111		

5.29 **Example** An SQS(14) (also a (14,4,6) BIBD). Let $V = \{x_i : x \in \mathbb{Z}_7,\ i \in \mathbb{Z}_2\}$. The blocks are obtained by applying the automorphisms $x_i \mapsto (x+1)_i$ and $x_i \mapsto (3x)_{i+1}$ to the five base blocks:

$$0_0, 1_0, 2_0, 4_0 \quad 0_0, 1_1, 2_1, 4_1 \quad 3_0, 4_0, 3_1, 4_1 \quad 4_0, 5_0, 2_1, 3_1 \quad 5_0, 6_0, 1_1, 2_1$$

5.30 **Theorem** There are 4 nonisomorphic SQS(14)s [1588] and 1054163 nonisomorphic SQS(16)s [1273].

5.31 **Theorem** For $v \leq 100$, an SQS(v) whose automorphism group contains a (cyclic) automorphism of order v exists when $v \equiv 2, 4 \pmod 6$, except when $v \in \{8, 14, 16\}$ and possibly when $v \in \{46, 56, 62, 70, 86, 94\}$.

5.32 **Theorem** Every Steiner triple system of order $v \leq 15$ is the derived system of some SQS($v+1$).

5.33 An SQS(v) is *resolvable* if its blocks can be partitioned into *parallel classes*, each of which is a set of blocks that partition the set of elements.

5.34 **Theorem** [1198] A resolvable SQS(v) exists for all $v \equiv 4, 8 \pmod{12}$.

5.6 Steiner 5-Designs

5.35 **Remark** All but one of the known Steiner 5-designs are of order $q+1$, where $q \equiv 3 \pmod 4$ is a prime power, and have automorphism group $\mathrm{PSL}_2(q)$; the $S(5, 8, 24)$ has the larger Mathieu group M_{24} as its automorphism group, and the unique $S(5, 6, 12)$ has the Mathieu group M_{12}. The $S(5, 8, 24)$ and its derived $S(4, 7, 23)$ are the *Witt designs*.

5.36 **Remark** Representations of the groups used to construct the designs in Table 5.37. For $q \in \{11, 23, 47, 71, 83, 107, 131, 167\}$, employ the representation of $\mathrm{PSL}_2(q)$ acting on $\mathbb{Z}_q \cup \{\infty\}$ that contains the permutations generated by (1) $x \mapsto x+1 \pmod q$, (2) $x \mapsto \alpha x \pmod q$ where $\alpha = 2$ for $q \in \{23, 47, 71, 167\}$ and $\alpha = 3$ for $q \in \{11, 83, 107, 131\}$; and (3) $x \mapsto -\frac{1}{x}$.

For $\mathrm{PSL}_2(27)$, an explicit set of five generators is:

(0 1 2)(3 4 5)(6 7 8)(9 10 11)(12 13 14)(15 16 17)(18 19 20)(21 22 23)(24 25 26)
(0 3 6)(1 4 7)(2 5 8)(9 12 15)(10 13 16)(11 14 17)(18 21 24)(19 22 25)(20 23 26)
(0 9 18)(1 10 19)(2 11 20)(3 12 21)(4 13 22)(5 14 23)(6 15 24)(7 16 25)(8 17 26)
(1 9 15 13 20 12 11 6 7 16 22 8 25)(2 18 21 26 10 24 19 3 5 23 17 4 14)
(0 ∞)(1 2)(3 11)(4 15)(5 12)(6 19)(7 24)(8 21)(9 14)(10 16)(13 17)(18 25)(20 23)(22 26)

The only known example [240] not admitting $\mathrm{PSL}_2(q)$ on $q+1$ points is an $S(5, 6, 36)$ admitting $\mathrm{PGL}(2, 17) \times C_2$; use the representation:

(0 17)(1 16)(2 8)(3 11)(5 10)(6 14)(7 12)(9 15)(18 35)(19 34)(20 26)(21 29)(23 28)(24 32)(25 30)(27 33)
(0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16)(18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34)
(1 3 9 10 13 5 15 11 16 14 8 7 4 12 2 6)(19 21 27 28 31 23 33 29 34 32 26 25 22 30 20 24)
(0 18)(1 19)(2 20)(3 21)(4 22)(5 23)(6 24)(7 25)(8 26)(9 27)(10 28)(11 29)(12 30)(13 31)(14 32)(15 33)(16 34)(17 35)

For $P\Sigma L(2, 243)$ the generators are

(1 217 241 80 195 104 38 111 175 153 17 191 131 41 31 140 42 84 172 236 133 68 34 57 169 72 8 190 238 160 71 197 211 157 151 70 61 60 89 199 239 53 192 184 154 231 105 91 227 132 94 144 16 55 223 78 88 63 7 54 6 83 119 120 176 46 219 187 74 115 66 170 208 237 186 100 225 25 56 116 202 156 177 99 11 108 12 164 128 121 147 179 209 130 148 150 96 90 10 218 134 201 185 47 112 149 43 58 143 205 76 142 69 87 92 117 13 135 15 81 9) (2 110 122 40 138 178 73 222 107 198 22 136 232 79 62 196 75 168 101 118 230 52 59 33 86 36 4 137 125 203 49 139 152 206 212 50 32 30 166 155 124 67 141 98 200 129 174 182 127 228 188 207 23 29 113 39 167 45 5 27 3 163 235 240 106 65 114 95 37 221 51 85 146 123 93 173 126 14 28 220 161 204 102 171 19 216 24 82 226 242 213 103 145 233 215 210 183 180 20 109 229 159 97 64 224 214 77 35 193 158 44 194 48 165 181 234 26 189 21 162 18)

(0 90 56 55 156 75 240 168 148 117 207 150 91 233 3) (1 160 2 110 182 57 105 104 15 122 180 92 43 196 186) (4 69 242 162 151 ∞ 118 66 20 38 48 152 145 119 169) (5 95 29 31 106 183 214 171 47 11 128 100 174 197 218) (6 154 213 226 195 238 89 84 136 81 191 79 134 205 203) (7 65 13 27 121 12 200 36 185 124 158 201 108 230 26) (8 10 228 232 99 21 166 78 19 37 101 212 146 30 188) (9 239 131 45 127 194 24 18 221 80 53 97 87 40 204) (14 149 83 184 52 241 113 224 217 88 163 25 59 23 58) (16 42 175 135 44 39 86 172 41 189 187 129 61 132 161) (17 227 216 72 165 225 177 206 123 210 126 64 190 120 202) (22 125 143 223 111 33 237 181 139 32 144 153 103 173 159) (28 193 199 209 236 140 142 234 222 192 198 96 102 54 114) (34 116 141 229 46 167 109 63 219 107 208 176 60 74 138) (35 235 231 112 71 133 73 67 50 94 179 70 137 170 98) (49 220 178) (51 147 215 82 130 115 62 77 164 93 76 157 155 211 85)

5.37 Table Parameters of known $S(5, k, v)$, and an example of each. The $S(5, 8, 24)$ is unique; for $S(5, 6, 24)$ and $S(5, 7, 28)$, all examples having the PSL group as a group of automorphisms are listed. See [238, 240, 691, 943, 1611, 2158] for further discussion.

$S(5, 6, 12)$			
∞,0,1,2,3,5			
$S(5, 8, 24)$			
∞,0,1,2,3,5,14,17			
$S(5, 6, 24)$ (three nonisomorphic solutions)			
∞,0,1,2,3,12	∞,0,1,2,5,14	∞,0,1,3,7,10	
∞,0,1,2,3,12	∞,0,1,2,5,14	∞,0,1,3,7,21	
∞,0,1,2,3,13	∞,0,1,2,5,18	∞,0,1,3,4,16	
$S(5, 7, 28)$			
∞,0,1,2,3,4,5	∞,0,1,3,7,10,18		
$S(5, 6, 36)$			
0,1,2,21,24,32	0,1,2,18,21,31	0,1,2,3,6,32	0,1,2,7,18,25
0,1,2,18,22,29	0,1,2,18,26,28	0,1,2,18,27,33	0,1,2,21,22,35
0,1,2,21,25,27	0,1,2,21,30,33	0,1,2,3,10,35	0,1,2,3,23,27
0,1,2,3,4,20	0,1,2,3,5,30	0,1,2,4,27,34	
$S(5, 6, 48)$			
∞,0,1,2,3,40	∞,0,1,2,5,8	∞,0,1,2,10,27	∞,0,1,2,13,26
∞,0,1,3,4,18	∞,0,1,3,8,14	∞,0,1,3,12,39	∞,0,1,4,20,41
$S(5, 6, 72)$			
∞,0,1,2,3,14	∞,0,1,2,5,17	∞,0,1,2,6,67	∞,0,1,2,7,46
∞,0,1,2,8,56	∞,0,1,2,9,68	∞,0,1,2,10,18	∞,0,1,2,27,31
∞,0,1,3,7,8	∞,0,1,3,10,51	∞,0,1,3,11,67	∞,0,1,3,12,46
∞,0,1,3,13,66	∞,0,1,3,17,38	∞,0,1,3,20,42	∞,0,1,3,31,65
∞,0,1,4,9,21	∞,0,1,6,10,49	∞,0,1,6,14,31	

	$S(5,6,84)$ – every orbit is a 3-design		
∞,0,1,2,3,32	∞,0,1,2,5,66	∞,0,1,2,6,20	∞,0,1,2,7,13
∞,0,1,2,8,57	∞,0,1,2,10,80	∞,0,1,2,11,46	∞,0,1,3,4,40
∞,0,1,3,7,61	∞,0,1,3,11,17	∞,0,1,3,12,65	∞,0,1,3,13,15
∞,0,1,3,14,53	∞,0,1,3,18,24	∞,0,1,3,22,23	∞,0,1,3,34,44
∞,0,1,3,37,68	∞,0,1,3,50,51		
	$S(5,6,108)$		
∞,0,1,2,3,55	∞,0,1,2,5,28	∞,0,1,2,6,103	∞,0,1,2,7,19
∞,0,1,2,8,101	∞,0,1,2,9,68	∞,0,1,2,10,13	∞,0,1,2,11,98
∞,0,1,2,12,97	∞,0,1,2,14,95	∞,0,1,2,16,93	∞,0,1,2,22,87
∞,0,1,2,25,59	∞,0,1,3,4,9	∞,0,1,3,7,21	∞,0,1,3,8,24
∞,0,1,3,10,90	∞,0,1,3,12,86	∞,0,1,3,13,102	∞,0,1,3,14,42
∞,0,1,3,15,67	∞,0,1,3,16,94	∞,0,1,3,17,77	∞,0,1,3,19,64
∞,0,1,3,20,60	∞,0,1,3,26,91	∞,0,1,3,27,30	∞,0,1,3,28,45
∞,0,1,3,31,72	∞,0,1,3,33,62	∞,0,1,3,35,40	∞,0,1,3,44,71
∞,0,1,3,48,51	∞,0,1,3,56,98	∞,0,1,3,74,96	∞,0,1,3,88,100
∞,0,1,4,5,92	∞,0,1,4,11,69	∞,0,1,4,15,90	∞,0,1,4,17,31
∞,0,1,4,20,80	∞,0,1,4,21,32	∞,0,1,4,28,50	∞,0,1,4,35,44
∞,0,1,4,38,45	∞,0,1,4,46,60	∞,0,1,4,47,57	∞,0,1,4,51,63
∞,0,1,4,68,84	∞,0,1,4,76,83	∞,0,1,5,6,25	∞,0,1,5,8,80
∞,0,1,5,18,70	∞,0,1,5,26,62	∞,0,1,5,35,46	∞,0,1,6,26,30
∞,0,1,6,33,78	∞,0,1,6,39,66	∞,0,1,6,50,77	∞,0,1,7,23,85
∞,0,1,8,11,38	∞,0,1,9,15,73	∞,0,1,9,22,91	∞,0,1,9,30,99
	$S(5,6,132)$		
∞,0,1,2,3,68	∞,0,1,2,5,99	∞,0,1,2,7,126	∞,0,1,2,8,33
∞,0,1,2,9,18	∞,0,1,2,10,105	∞,0,1,2,11,24	∞,0,1,2,12,22
∞,0,1,2,13,121	∞,0,1,2,15,118	∞,0,1,2,16,25	∞,0,1,2,17,74
∞,0,1,2,28,31	∞,0,1,2,32,94	∞,0,1,2,34,43	∞,0,1,2,36,51
∞,0,1,2,38,65	∞,0,1,2,40,48	∞,0,1,2,58,100	∞,0,1,2,60,112
∞,0,1,2,64,95	∞,0,1,3,4,9	∞,0,1,3,7,41	∞,0,1,3,8,63
∞,0,1,3,10,62	∞,0,1,3,11,52	∞,0,1,3,12,91	∞,0,1,3,13,55
∞,0,1,3,14,92	∞,0,1,3,15,69	∞,0,1,3,16,90	∞,0,1,3,17,124
∞,0,1,3,18,83	∞,0,1,3,19,27	∞,0,1,3,20,65	∞,0,1,3,21,100
∞,0,1,3,22,24	∞,0,1,3,23,51	∞,0,1,3,25,115	∞,0,1,3,28,106
∞,0,1,3,29,31	∞,0,1,3,33,43	∞,0,1,3,34,111	∞,0,1,3,40,57
∞,0,1,3,42,127	∞,0,1,3,61,84	∞,0,1,3,72,117	∞,0,1,3,98,110
∞,0,1,4,5,103	∞,0,1,4,11,102	∞,0,1,4,13,128	∞,0,1,4,14,84
∞,0,1,4,15,106	∞,0,1,4,19,48	∞,0,1,4,22,46	∞,0,1,4,23,114
∞,0,1,4,24,92	∞,0,1,4,26,112	∞,0,1,4,28,34	∞,0,1,4,29,81
∞,0,1,4,35,77	∞,0,1,4,39,63	∞,0,1,4,52,108	∞,0,1,4,61,62
∞,0,1,4,64,107	∞,0,1,4,93,125	∞,0,1,5,6,98	∞,0,1,5,11,83
∞,0,1,5,12,31	∞,0,1,5,14,70	∞,0,1,5,16,40	∞,0,1,5,19,30
∞,0,1,5,22,107	∞,0,1,5,24,35	∞,0,1,5,43,82	∞,0,1,5,52,60
∞,0,1,5,55,64	∞,0,1,5,79,95	∞,0,1,6,7,36	∞,0,1,6,10,53
∞,0,1,6,13,51	∞,0,1,6,20,49	∞,0,1,6,38,97	∞,0,1,7,8,83
∞,0,1,7,18,91	∞,0,1,7,24,97	∞,0,1,8,20,42	∞,0,1,8,35,94
∞,0,1,9,10,90	∞,0,1,9,19,97	∞,0,1,9,101,118	∞,0,1,9,107,114
∞,0,1,11,12,73	∞,0,1,11,53,117	∞,0,1,15,37,92	∞,0,1,16,54,68

$S(5,6,168)$			
∞,0,1,2,3,85	∞,0,1,2,5,113	∞,0,1,2,7,162	∞,0,1,2,8,25
∞,0,1,2,9,16	∞,0,1,2,10,131	∞,0,1,2,11,20	∞,0,1,2,12,92
∞,0,1,2,13,24	∞,0,1,2,14,78	∞,0,1,2,18,60	∞,0,1,2,19,150
∞,0,1,2,21,40	∞,0,1,2,22,94	∞,0,1,2,28,69	∞,0,1,2,31,75
∞,0,1,2,34,72	∞,0,1,2,36,107	∞,0,1,2,43,164	∞,0,1,2,45,106
∞,0,1,2,47,70	∞,0,1,2,56,86	∞,0,1,2,59,118	∞,0,1,3,4,83
∞,0,1,3,8,41	∞,0,1,3,10,30	∞,0,1,3,11,95	∞,0,1,3,12,68
∞,0,1,3,13,39	∞,0,1,3,14,135	∞,0,1,3,15,81	∞,0,1,3,17,147
∞,0,1,3,18,134	∞,0,1,3,19,132	∞,0,1,3,20,109	∞,0,1,3,21,51
∞,0,1,3,22,115	∞,0,1,3,23,123	∞,0,1,3,24,117	∞,0,1,3,25,156
∞,0,1,3,27,116	∞,0,1,3,28,131	∞,0,1,3,31,90	∞,0,1,3,33,69
∞,0,1,3,37,44	∞,0,1,3,40,45	∞,0,1,3,43,54	∞,0,1,3,48,110
∞,0,1,3,49,89	∞,0,1,3,52,73	∞,0,1,3,57,162	∞,0,1,3,61,153
∞,0,1,3,62,118	∞,0,1,3,63,99	∞,0,1,3,64,107	∞,0,1,3,65,100
∞,0,1,3,67,87	∞,0,1,3,70,76	∞,0,1,3,77,146	∞,0,1,3,79,165
∞,0,1,3,94,128	∞,0,1,3,98,119	∞,0,1,4,5,20	∞,0,1,4,13,45
∞,0,1,4,14,131	∞,0,1,4,15,59	∞,0,1,4,17,46	∞,0,1,4,18,98
∞,0,1,4,19,31	∞,0,1,4,21,95	∞,0,1,4,23,60	∞,0,1,4,24,130
∞,0,1,4,25,115	∞,0,1,4,26,104	∞,0,1,4,27,37	∞,0,1,4,29,148
∞,0,1,4,30,125	∞,0,1,4,32,97	∞,0,1,4,34,92	∞,0,1,4,39,73
∞,0,1,4,40,81	∞,0,1,4,41,48	∞,0,1,4,43,138	∞,0,1,4,47,124
∞,0,1,4,49,91	∞,0,1,4,50,63	∞,0,1,4,52,82	∞,0,1,4,55,152
∞,0,1,4,62,157	∞,0,1,4,64,99	∞,0,1,4,68,113	∞,0,1,4,71,143
∞,0,1,4,77,135	∞,0,1,4,79,149	∞,0,1,4,87,100	∞,0,1,4,136,142
∞,0,1,5,6,148	∞,0,1,5,11,34	∞,0,1,5,12,60	∞,0,1,5,16,108
∞,0,1,5,19,146	∞,0,1,5,21,48	∞,0,1,5,24,87	∞,0,1,5,37,141
∞,0,1,5,39,131	∞,0,1,5,41,49	∞,0,1,5,44,74	∞,0,1,5,66,163
∞,0,1,6,7,138	∞,0,1,6,13,75	∞,0,1,6,14,33	∞,0,1,6,15,65
∞,0,1,6,17,142	∞,0,1,6,20,64	∞,0,1,6,22,154	∞,0,1,6,23,104
∞,0,1,6,25,157	∞,0,1,6,35,131	∞,0,1,6,39,145	∞,0,1,6,43,139
∞,0,1,6,52,100	∞,0,1,6,66,78	∞,0,1,6,108,134	∞,0,1,6,147,159
∞,0,1,7,11,123	∞,0,1,7,12,128	∞,0,1,7,15,110	∞,0,1,7,20,71
∞,0,1,7,22,54	∞,0,1,7,23,107	∞,0,1,7,41,95	∞,0,1,7,50,78
∞,0,1,7,60,66	∞,0,1,7,73,159	∞,0,1,7,77,102	∞,0,1,7,82,119
∞,0,1,7,98,149	∞,0,1,7,115,133	∞,0,1,8,10,58	∞,0,1,8,13,124
∞,0,1,8,20,141	∞,0,1,8,34,44	∞,0,1,8,55,131	∞,0,1,8,63,77
∞,0,1,9,23,40	∞,0,1,9,39,159	∞,0,1,9,47,117	∞,0,1,9,53,155
∞,0,1,9,59,107	∞,0,1,9,89,157	∞,0,1,9,90,121	∞,0,1,9,96,131
∞,0,1,10,81,103	∞,0,1,11,15,149	∞,0,1,12,30,86	∞,0,1,13,40,142
∞,0,1,13,79,152	∞,0,1,15,31,119	∞,0,1,18,34,58	∞,0,1,33,34,81
$S(5,6,244)$			
∞,0,1,2,3,241	∞,0,1,2,9,59	∞,0,1,3,4,86	∞,0,1,3,7,167
∞,0,1,3,10,64	∞,0,1,3,11,33	∞,0,1,3,12,36	∞,0,1,3,13,58
∞,0,1,3,14,28	∞,0,1,3,15,240	∞,0,1,3,16,165	∞,0,1,3,17,188
∞,0,1,3,18,83	∞,0,1,3,19,59	∞,0,1,3,20,184	∞,0,1,3,23,87
∞,0,1,3,25,226	∞,0,1,3,26,66	∞,0,1,3,27,217	∞,0,1,3,31,102
∞,0,1,3,32,136	∞,0,1,3,34,166	∞,0,1,3,35,97	∞,0,1,3,39,128
∞,0,1,3,40,50	∞,0,1,3,42,79	∞,0,1,3,43,173	∞,0,1,3,44,45
∞,0,1,3,51,216	∞,0,1,3,52,119	∞,0,1,3,53,118	∞,0,1,3,62,178

∞,0,1,3,67,129	∞,0,1,3,68,155	∞,0,1,3,75,154	∞,0,1,3,76,234
∞,0,1,3,84,98	∞,0,1,3,88,152	∞,0,1,3,103,208	∞,0,1,3,109,197
∞,0,1,3,121,190	∞,0,1,3,123,214	∞,0,1,3,153,201	∞,0,1,3,164,215
∞,0,1,3,185,220	∞,0,1,4,5,145	∞,0,1,4,9,170	∞,0,1,4,17,83
∞,0,1,4,20,208	∞,0,1,4,30,221	∞,0,1,4,31,101	∞,0,1,4,34,138
∞,0,1,4,36,96	∞,0,1,4,37,64	∞,0,1,4,43,234	∞,0,1,4,45,143
∞,0,1,4,54,85	∞,0,1,4,72,176	∞,0,1,4,87,144	∞,0,1,4,204,219
∞,0,1,5,16,41	∞,0,1,5,32,139	∞,0,1,5,33,143	∞,0,1,5,35,72
∞,0,1,5,51,205	∞,0,1,5,100,212	∞,0,1,9,49,135	

5.38 **Remark** The number N of nonisomorphic $S(5,6,q+1)$ that are invariant under $\mathrm{PSL}_2(q)$ [238, 944]; for $v \in \{108, 132, 168\}$, only systems using short orbits are considered:

$q+1$	48	72	84	108	132	168	244
N	459	926299	348512	≥ 71	≥ 55	≥ 4	≥ 6450

Omitting the restriction to short orbits, Laue (unpublished) reports that there are at least 719,144 nonisomorphic $S(5,6,108)$s and at least 945 nonisomorphic $S(5,6,132)$s.

See Also

§II.3	Steiner 2-designs are BIBDs with index one.
§II.4	$S(t,k,v)$ are t-designs with index one.
§VI.63	t-wise balanced designs are generalizations of Steiner systems.
§VII.2	Finite geometries furnish many examples of $S(t,k,v)$.
[225]	Textbook covering most of the material in this chapter.
[578]	A comprehensive monograph on triple systems.
[1403]	Resolvable t-designs.
[1063]	A comprehensive survey of SQS.
[1439]	Necessary conditions for Steiner systems.
[1951]	Asymptotically most efficient known isomorphism algorithm for $S(2,k,v)$s.

References Cited: [225, 238, 240, 281, 578, 678, 691, 761, 943, 944, 988, 1011, 1043, 1063, 1198, 1273, 1403, 1439, 1588, 1611, 1621, 1684, 1783, 1951, 2158]

6 Symmetric Designs

Yury J. Ionin
Tran van Trung

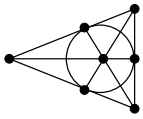
6.1 Preliminaries

6.1 A BIBD with $b = v$ (or equivalently, $r = k$) is a *symmetric* (v,k,λ) design or simply a *symmetric design*. A symmetric design with $k = 1$ or $k = v-1$ is *trivial*. The value $n = k - \lambda$ is the *order* of the design.

6.2 **Remark** This chapter deals only with nontrivial symmetric designs, those with $1 < k < v-1$.

6.3 **Proposition** In a symmetric (v,k,λ) design every two distinct blocks have λ points in common (the design is *linked*).

6.4 **Example** The paradigmatic example of a symmetric design is the $(7, 3, 1)$ design.



This is the *Fano plane*. The point set is $X = \{0, \cdots, 6\}$ and the block set is $\mathcal{B} = \{013, 124, 235, 346, 450, 561, 602\}$. The seven blocks are presented by six lines and one circle.

6.5 The *complement* of a symmetric (v, k, λ) design $\mathcal{D}$ is a symmetric $(v, v-k, v-2k+\lambda)$ design, whose blocks are the complements of blocks of $\mathcal{D}$.

6.6 **Remarks** In any symmetric design, the parameter v satisfies $4n-1 \le v \le n^2+n+1$.

1. The lower bound on v corresponds to a symmetric design $\mathcal{D}$ with parameters $(v = 4n-1, k = 2n-1, \lambda = n-1)$ or its complement; and $\mathcal{D}$ is a *Hadamard design* of order n. See §V.1.
2. The upper bound on v corresponds to a symmetric design $\mathcal{D}$ with parameters $(v = n^2+n+1, k = n+1, \lambda = 1)$ or its complement; and $\mathcal{D}$ is a *finite projective plane* of order n. See §VII.2.1.

6.7 Let $\mathcal{D} = (V, \mathcal{B})$ be a BIBD, then the *dual* of $\mathcal{D}$ is $\mathcal{D}^* = (\mathcal{B}, V)$ where $b \in \mathcal{B}$ is contained in $v \in V$ if and only if v is contained in b in $\mathcal{D}$.

6.8 **Remark** The dual of a BIBD is a BIBD if and only if the BIBD is symmetric. Also, the parameters of a symmetric design and its dual are the same, yet they are not necessarily isomorphic.

6.9 A *polarity* of a symmetric design $\mathcal{D}$ is an isomorphism π from $\mathcal{D}$ to $\mathcal{D}^*$ that has order 2 (π^2 is the identity mapping on $\mathcal{D}$).

6.2 The Bruck–Ryser–Chowla Theorem

6.10 **Remark** For a symmetric (v, k, λ) design to exist the arithmetic condition $\lambda(v-1) = k(k-1)$ must be satisfied. The most fundamental necessary condition on the existence of symmetric designs is due to Bruck, Ryser, and Chowla [356, 503].

6.11 **Theorem** (*Bruck–Ryser–Chowla*) Let v, k, and λ be integers with $\lambda(v-1) = k(k-1)$ for which there exists a symmetric (v, k, λ) design.

1. If v is even, then $n = k - \lambda$ is a square.
2. If v is odd, then the equation $z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2$ has a solution in integers x, y, z not all zero.

6.12 **Remarks** The Bruck–Ryser–Chowla theorem implies that if a projective plane of order $n \equiv 1$ or $2 \pmod 4$ exists, then n is the sum of two squares of integers. The smallest orders of projective planes whose existence is still undecided are $n = 12$, 15, 18, 20, 24, 26, 28.

At one time it was conjectured that the necessary conditions of the Bruck–Ryser–Chowla theorem are sufficient for the existence of symmetric designs. This conjecture is now known to be false: A symmetric (111,11,1) design cannot exist [1378]. See Remark VII.6.27.

6.13 **Conjecture** For every $\lambda > 1$, there exist only finitely many symmetric (v, k, λ) designs.

6.14 **Remarks** If $\lambda = 2$, the only values of k for which symmetric $(v, k, 2)$ designs (*biplanes*) are known are $k = 4$, 5, 6, 9, 11, 13. The values of k of the known symmetric designs with $\lambda = 3$ are $k = 6$, 7, 9, 10, 12, 15. Arasu [107] shows the finiteness of the number of symmetric designs for a given λ, when v is of a special form.

6.3 Automorphisms of Symmetric Designs

6.15 An *automorphism* of a design is a permutation of the point set that preserves the block set. A group obtained under composition of automorphisms is an *automorphism group*. The group of *all* automorphisms of a design $\mathcal{D}$ is the *full automorphism group* of $\mathcal{D}$, denoted by $Aut(\mathcal{D})$.

6.16 **Theorem** An automorphism of a symmetric design fixes the same number of points as blocks.

6.17 **Theorem** [114] Let $\mathcal{D}$ be a symmetric (v, k, λ) design and let p be a prime divisor of the order of $Aut(\mathcal{D})$. Then either p divides v or $p \leq k$.

6.18 **Theorem** [1874] If f is the number of fixed points of an automorphism of a symmetric (v, k, λ) design, then $f \leq k + \sqrt{n}$, where $n = k - \lambda$.

6.19 **Theorem** (Multiplier theorem) [1019]) Suppose that there exists a symmetric (v, k, λ) design having an abelian group G of order v as a regular automorphism group. Suppose that p is a prime such that $p > \lambda$, p divides $n = k - \lambda$, and p is relatively prime to v. Then the mapping $g \to pg$, $g \in G$, is also an automorphism of the design. (See also §VI.18.2.)

6.20 **Theorem** [1256] Let $\mathcal{D}$ be a symmetric (v, k, λ) design with $k < v/2$ such that $Aut(\mathcal{D})$ acts doubly transitively on points. Then $\mathcal{D}$ is one of the following:

1. a point-hyperplane design with $v = \frac{q^{m+1}-1}{q-1}$, $k = \frac{q^m-1}{q-1}$, and $\lambda = \frac{q^{m-1}-1}{q-1}$ (§VII.2),
2. the unique Hadamard design with $v = 11$, $k = 5$, and $\lambda = 2$ (§V.1);
3. a unique design with $v = 176$, $k = 50$, and $\lambda = 14$ admitting the Higman–Sims group; or
4. a unique design with $v = 2^{2m}$, $k = 2^{m-1}(2^m - 1)$, and $\lambda = 2^{m-1}(2^{m-1} - 1)$, for each $m \geq 2$.

6.21 **Theorem** [681, 682] Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric (v, k, λ) design and $G \leq Aut(\mathcal{D})$. Assume that G acts as a primitive rank 3 group on points and blocks.

A. If G has a nontrivial socle T, then T is simple and one of the following holds:
   1. $v = \frac{q^{2n}-1}{q-1}, k = \frac{q^{2n-1}-1}{q-1}, \lambda = \frac{q^{2n-2}-1}{q-1}, n \geq 2$, q a prime power. $T \simeq PSp(2n, q)$ and $\mathcal{D}$ is the point-hyperplane design on a $2n$-dimensional space over $\mathbb{F}_q$.
   2. $v = \frac{q^{2n}-1}{q-1}, k = \frac{q^{2n-1}-1}{q-1}, \lambda = \frac{q^{2n-2}-1}{q-1}, n \geq 2$, q is a prime power, and q is odd if $n \geq 3$. $T \simeq P\Omega(2n+1, q)$ and $\mathcal{P}$ is the set of isotropic points in a nondegenerate, $(2n+1)$-dimensional, orthogonal space over $\mathbb{F}_q$. Blocks have the form $b(P) = \{Q \in \mathcal{P} | P \perp Q\}$, $P \in \mathcal{P}$.
   3. $v = \frac{3^n(3^n-1)}{2}, k = \frac{3^{n-1}(3^n+1)}{2}, \lambda = \frac{3^{n-1}(3^{n-1}+1)}{2}, n \geq 2$. $T \simeq P\Omega(2n+1, 3)$ and $\mathcal{P}$ is the set of anisotropic points $P =< p >$, $(p, p) = -1$ in a nondegenerate, $(2n+1)$-dimensional, orthogonal space over $\mathbb{F}_3$ with discriminant $(-1)^n$. Blocks have the form $b(P) = \{Q \in \mathcal{P} | P \perp Q\}$, $P \in \mathcal{P}$.
   4. $v = \frac{3^n(3^n+1)}{2}, k = \frac{3^{n-1}(3^n-1)}{2}, \lambda = \frac{3^{n-1}(3^{n-1}-1)}{2}, n \geq 2$. $T \simeq P\Omega(2n+1, 3)$ and $\mathcal{P}$ is the set of anisotropic points $P =< p >$, $(p, p) = 1$ in a nondegenerate, $(2n+1)$-dimensional, orthogonal space over $\mathbb{F}_3$ with discriminant $(-1)^n$. Blocks have the form $b(P) = \{Q \in \mathcal{P} | P \perp Q\}$, $P \in \mathcal{P}$.
   5. $v = 15, k = 7, \lambda = 3$. $T \simeq A_6$, $\mathcal{P} = \binom{X}{2}$, $|X| = 6$. Blocks have the form $b(P) = \{P\} \cup \{Q \in \binom{X}{2} | P \cap Q = \emptyset\}$, $P \in \binom{X}{2}$.

6. $v = 35, k = 17, \lambda = 8$. $T \simeq A_8 \simeq GL(4,2)$ and points are the lines in a 4-dimensional space over $\mathbb{F}_2$. Blocks have the form $b(P) = \{P\} \cup \{Q \in \mathcal{P} | P \cap Q = 0\}$, $P \in \mathcal{P}$.
7. $v = 36, k = 15, \lambda = 6$. $T \simeq U_3(3)$, $G \simeq G_2(2)$. A point and block stabilizer is a $PGL(2,7)$.
8. $v = 56, k = 11, \lambda = 2$. $T \simeq L_3(4)$. A point and block stabilizer is an A_6.
9. $v = 176, k = 50, \lambda = 14$. $T \simeq M_{22}$. Point and block stabilizers are A_7 belonging to different conjugacy classes.
10. $v = 351, k = 126, \lambda = 45$. $T \simeq G_2(3)$. A point and block stabilizer is an $U_3(3).2$.
11. $v = 14080, k = 1444, \lambda = 148$. $T \simeq Fi(22)$. Point and block stabilizers are $P\Omega(7,3)$ belonging to different conjugacy classes.

B. If G is a primitive affine rank 3 group of degree p^m, p a prime, then one of the following holds:

12. $p > 2$ and $\mathcal{D}$ is the Paley design with parameters $v = p^m, k = \frac{(p^m-1)}{2}, \lambda = \frac{(p^m-3)}{4}$, $p^m \equiv 3 \pmod 4$.
13. $p^m = 2^{2a}$ and $\mathcal{D} = \mathcal{S}_{2a}$ is the unique design with parameters $v = 2^{2a}$, $k = 2^{a-1}(2^a - 1)$, $\lambda = 2^{a-1}(2^{a-1} - 1)$ and $Aut(\mathcal{S}_{2a}) \simeq V(2a,2).Sp(2a,2)$.

6.22 Remarks

1. For further results about automorphisms of symmetric designs, see [1397].
2. For any given finite group G, for all sufficiently large d, and for each $q > 3$, there are symmetric designs with the same parameters as the point-hyperplane symmetric designs $PG(d,q)$ having G as full automorphism group [1260].
3. See [1553] for a study of symmetric designs having unitals or unitary polarities.

6.4 Quasi-Residual Designs and their Embedding

6.23 Let $\mathcal{D}$ be a symmetric (v,k,λ) design and let B be a block of $\mathcal{D}$. Remove B and all points in B from the other blocks. The result is a BIBD$(v-k, k-\lambda, \lambda)$, a *residual design*.

6.24 Remark If a design with parameters (v,b,r,k,λ) is a residual design of a symmetric design, then $r = k + \lambda$.

6.25 A BIBD with $r = k + \lambda$ is a *quasi-residual design*. If such a design is a residual design, then it is *embeddable* or *residual*; otherwise, *nonembeddable*.

6.26 Remark A quasi-residual design with $\lambda = 1$ is an affine plane and is embeddable in a projective plane.

6.27 Theorem (Hall–Connor [1017]) A quasi-residual design with $\lambda = 2$ is embeddable.

6.28 Theorem [310] For every $\lambda \geq 3$, there is a function $f(\lambda)$ such that any quasi-residual (w,k,λ) design with $k > f(\lambda)$ is embeddable. The function f is given by

$$f(\lambda) = \begin{cases} 76 & : \quad \lambda = 3, \\ \frac{1}{2}(\lambda-1)(\lambda^4 - 2\lambda^2 + \lambda + 2) & : \quad 4 \leq \lambda \leq 9, \\ \frac{1}{2}(\lambda-1)(\alpha + \sqrt{\alpha^2 + 4(\lambda-1)}) - (\lambda-1) & : \quad 10 \leq \lambda, \end{cases}$$

where $\alpha = (\lambda-1)(\lambda^2 - 3\lambda + 3)$.

6.29 Remarks

1. No example of a quasi-residual (w,k,λ) design with $k > f(\lambda)$ of Theorem 6.28 is known.

2. Example 6.30 gives the nonembeddable quasi-residual design with parameters $(16, 6, 3)$ [250]. For more information on the existence of nonembeddable quasi-residual designs, see [2070].
3. See [1169] for sufficient conditions for nonembeddability of quasi-residual designs and constructions of infinite families of designs satisfying these conditions.
4. See [2089] for a sufficient condition for nonembeddability of quasi-derived designs and constructions of designs satisfying this condition.

6.30 **Example** A nonembeddable quasi-residual (16,6,3) design. (Look at the block intersection sizes to verify nonembeddability.)

1 2 3 4 5 6	1 2 3 4 7 8	1 2 9 10 12 13	1 3 10 11 12 15
1 4 9 13 14 16	1 5 7 10 14 15	1 5 7 11 13 16	1 6 8 9 11 14
1 6 8 12 15 16	2 3 9 10 11 16	2 4 12 13 14 15	2 5 6 9 15 16
2 5 8 11 13 15	2 6 7 11 12 14	2 7 8 10 14 16	3 4 11 14 15 16
3 5 6 10 13 14	3 5 8 9 12 14	3 6 7 12 13 16	3 7 8 9 13 15
4 5 7 9 11 12	4 5 8 10 12 16	4 6 7 9 10 15	4 6 8 10 11 13

6.31 **Remark** [1946] All four 2-(8,4,3) designs are residual; of 18,920 nonisomorphic quasi-residual 2-(16,6,3) designs, only 1305 are residual; all 3809 nonisomorphic 2-(21,7,3) designs are residual.

6.5 Extensions of Symmetric Designs

6.32 If a t-design $\mathcal{D}^*$ is the derived design of some $(t+1)$-design $\mathcal{D}$, then $\mathcal{D}$ is an *extension* of $\mathcal{D}^*$, and $\mathcal{D}^*$ is *extendible*.

6.33 **Example** Every Hadamard $(4n-1, 2n-1, n-1)$ design $\mathcal{D}$ is extendible to a 3-$(4n, 2n, n-1)$ design $\mathcal{E}$, a *Hadamard 3-design*. See Construction V.1.7.

6.34 **Theorem** [413] If a symmetric (v, k, λ) design $\mathcal{D}$ is extendible, then one of the following holds:

1. $v = 4\lambda + 3$, $k = 2\lambda + 1$; that is, $\mathcal{D}$ is a Hadamard design,
2. $v = (\lambda + 2)(\lambda^2 + 4\lambda + 2)$, $k = \lambda^2 + 3\lambda + 1$, or
3. $v = 495$, $k = 39$, $\lambda = 3$.

6.35 **Remarks** The known symmetric designs in the three cases of Theorem 6.34 are the known Hadamard designs in case 1, the projective plane of order 4, and the biplanes with parameters (56,11,2) in case 2. The Hadamard designs and the projective plane of order 4 are extendible. In 1988, Bagchi claimed that no (56,11,2) biplane is extendible; however, there was a fatal error in the proof. None of the five known (56,11,2) biplanes can be extended to a 3-(57,12,2) design [1283]. In case 2, see [1840] for a connection between extendability and existence of maximal arcs.

6.6 λ-Designs and the λ-Design Conjecture

6.36 For integers λ and v with $0 < \lambda < v$, a *λ-design* D on v *points* (also known as a *Ryser design*) is a pair $(X, \mathcal{B})$, where X is a set of cardinality v and $\mathcal{B}$ is a set of v distinct subsets (*blocks*) of X, such that

1. for all blocks $A, B \in \mathcal{B}$, $A \neq B$, $|A \cap B| = \lambda$, and
2. there exist blocks $A, B \in \mathcal{B}$ with $|A| \neq |B|$.

6.37 Construction A λ-design can be constructed from a symmetric design with parameters (v, k, μ) (when $\mu \neq k/2$) as follows. Let $(X, \mathcal{A})$ be such a symmetric design and let $A \in \mathcal{A}$. Put $\mathcal{B} = \{A\} \cup \{A \triangle B \mid B \in \mathcal{A},\ |B| \neq |A|\}$, where $\triangle$ denotes the symmetric difference of sets. Then $(X, \mathcal{B})$ is a λ-design on v points with $\lambda = k - \mu$. This procedure is *complementation* with respect to the block A.

6.38 A *type-1* λ-design is any λ-design arising from Construction 6.37.

6.39 Conjecture (Ryser (1968), Woodall (1970)) Every λ-design is of type 1.

6.40 Remarks The λ-design conjecture was proved for $\lambda = 1$ by de Bruijn and Erdős (1948), for $\lambda = 2$ by Ryser (1968), for $3 \leq \lambda \leq 9$ by Bridges and Kramer (1970), for $\lambda = 10$ by Seress (1990), for $\lambda = 14$ by Bridges and Tsaur (1996), and for all other values of $\lambda \leq 34$ by Weisz (1995). Singhi and S. S. Shrikhande (1976) proved the conjecture for prime λ, and Seress (2001) proved it when λ is twice a prime.

Investigating the conjecture as a function of v rather than λ, Ionin and M. S. Shrikhande (1996) proved the conjecture for $v = p + 1,\ 2p + 1,\ 3p + 1$ and $4p + 1$, where p is any prime. Hein and Ionin (2002) proved it for $v = 5p + 1$ with any prime $p \not\equiv 2$ or 8 (mod 15). Fiala (2002) proved it for $v = 6p + 1$ where p is any prime. Fiala [812] proved it for $v = 8p + 1$ with any prime $p \equiv 1$ or 7 (mod 8). References can be found in [812, 1170]. This is all summarized in Theorems 6.41.

6.41 Theorems The λ-design conjecture is true when $\lambda \leq 34$ and when λ is a prime or twice a prime. It is also true when $v = np + 1$ where p is a prime and $n = 1, 2, 3, 4$, or 6; for $v = 5p + 1$ where $p \not\equiv 2$ or 8 (mod 15) is a prime and for $v = 8p + 1$ where $p \not\equiv 5$ or 11 (mod 24) is a prime.

6.42 Given a λ-design $D = (X, \mathcal{B})$ and a point $x \in X$, the *replication number* of x is the number of blocks in $\mathcal{B}$ that contain x.

6.43 Proposition If $D = (X, \mathcal{B})$ is a λ-design on v points, then there exist distinct integers $r, r^* > 1$ such that every point $x \in X$ has replication number r or r^*. Furthermore $r + r^* = v + 1$ and $\frac{1}{\lambda} + \sum_{A \in \mathcal{B}} \frac{1}{|A| - \lambda} = \frac{(v-1)^2}{(r-1)(r^*-1)}$.

6.7 Generic Constructions of Symmetric Designs

6.44 Theorem [1163, 1170] Let $\mathcal{M}$ be a nonempty finite set of incidence matrices of symmetric (v, k, λ)-designs such that $q = k^2/(k - \lambda)$ is a prime power. Suppose there exists a permutation σ of $\mathcal{M}$ satisfying (i) σ^{q-1} is the identity permutation, (ii) for all $M, N \in \mathcal{M}$, $(\sigma M)(\sigma N)^T = MN^T$; and (iii) for all $M \in \mathcal{M}$, $\sum_{i=1}^{q-1} \sigma^i M = (k(q-1)/v)J$. Then, for any positive integer m, there exists a symmetric design with parameters

$$(v(q^m - 1)/(q - 1), kq^{m-1}, \lambda q^{m-1}).$$

6.45 Theorem [1164, 1170] Let $\mathcal{M}$ be a nonempty finite set of incidence matrices of quasi-residual 2-(v, k, λ) designs, such that $r = k + \lambda$ is a prime power, and let L be an incidence matrix of a quasi-derived 2-$(r, \lambda, \lambda - 1)$ design. Suppose there exists a permutation σ of $\mathcal{M}$ satisfying (i) σ^{r-1} is the identity permutation; (ii) for all $M, N \in \mathcal{M}$, $(\sigma M)(\sigma N)^T = MN^T$ and $(\sigma M)L^T = \lambda J$; and (iii) for all $M \in \mathcal{M}$, $\sum_{i=1}^{r-1} \sigma^i M = (k(r-1)/v)J$. Then, for any positive integer m, there exists a symmetric design with parameters

$$(1 + (v + r - 1)(r^m - 1)/(r - 1), r^m, \lambda r^{m-1}).$$

6.46 Remark See §V.6, Theorems 6.49 and 6.53, for a more general form of Theorems 6.44 and 6.45.

6.8 Known Symmetric Designs

Family 1 (Point-hyperplane designs)
$v = \frac{q^{m+1}-1}{q-1}$, $k = \frac{q^m-1}{q-1}$, $\lambda = \frac{q^{m-1}-1}{q-1}$, $n = q^{m-1}$, q a prime power and $m \geq 2$. Points and blocks of the designs are points and hyperplanes of the projective geometries $\mathrm{PG}(m, q)$. (See §VII.2.)

Family 2 (Hadamard designs)
$v = 4n-1$, $k = 2n-1$, $\lambda = n-1$. (See §V.1.)

Family 3 (Chowla [501])
$v = 4t^2+1$, $k = t^2$, $\lambda = (t^2-1)/4$, $n = (3t^2+1)/4$, t an odd positive integer, v a prime. Designs are constructed via a difference set consisting of biquadratic residues modulo v. (See Example VI.18.48.)

Family 4 (Lehmer [1421]) (See Construction VI.18.48.)
a. $v = 4t^2+9$, $k = t^2+3$, $\lambda = (t^2+3)/4$, $n = 3(t^2+3)/4$, t an odd positive integer, v a prime. Designs are constructed via a difference set consisting of 0 and biquadratic residues modulo v.
b. $v = 8t^2+1 = 64u^2+9$, $k = t^2$, $\lambda = u^2$, $n = t^2-u^2$, t, u odd positive integers, v a prime. Designs are constructed via a difference set of octic residues modulo v.
c. $v = 8t^2+49 = 64u^2+441$, $k = t^2+6$, $\lambda = u^2+7$, $n = t^2-u^2-1$, t an odd positive integer, u an even integer, v a prime. Designs are constructed via a difference set consisting of 0 and octic residues modulo v.

Family 5 (Whiteman [2136])
$v = pq$, $k = (pq-1)/4$, $\lambda = (pq-5)/16$, $n = (3pq+1)/16$, p and $q = 3p+2$ primes, k an odd square. Designs are constructed via a difference set modulo v. However, the only known examples are $p = 17$, $q = 53$, and $p = 46817$, $q = 140453$.

Family 6 (Menon [1591])
$v = 4t^2$, $k = 2t^2-t$, $\lambda = t^2-t$, $n = t^2$. A symmetric design with these parameters exists if and only if there exists a regular Hadamard matrix of order $4t^2$. The existence of such matrices is known whenever (i) there is a Hadamard matrix of $2t$ or (ii) $2t-1$ and $2t+1$ are both prime powers or (iii) n is an odd square or (iv) there exists a Hadamard difference set and in other cases. It is conjectured that designs exist for all values of t. See §VI.18.6 and §V.1.)

Family 7 (Wallis [2104])
$v = q^{m+1}(q^m+\cdots+q+2)$, $k = q^m(q^m+\cdots+q+1)$, $\lambda = q^m(q^{m-1}+\cdots+q+1)$, $n = q^{2m}$, q a prime power, m a positive integer. The construction is based on the existence of affine designs with parameters $(q^{m+1}, q^m, \frac{q^m-1}{q-1})$. A different construction due to McFarland [1564] is based on noncyclic difference sets. (See §VI.18.5.)

Family 8 (Wilson (unpublished); Shrikhande and Singhi [1908])
$v = m^3+m+1$, $k = m^2+1$, $\lambda = m$, $n = m^2-m+1$, where both $m-1$ and m^2-m+1 are prime powers. The construction is based on symmetric group divisible designs and projective planes of order $m-1$.

Family 9 (Spence [1939])
$v = 3^m(3^m-1)/2$, $k = 3^{m-1}(3^m+1)/2$, $\lambda = 3^{m-1}(3^{m-1}+1)/2$, $n = 3^{2(m-1)}$. Designs are constructed via a noncyclic difference set. (See §VI.18.5.)

Family 10 (Rajkundlia [1773] and Mitchell [1616] for $d = 2$; Ionin [1164])
$v = 1+qr(r^m-1)/(r-1)$, $k = r^m$, $\lambda = r^{m-1}(r-1)/q$, $n = r^{m-1}q^{d-1}$, where q and $r = (q^d-1)/(q-1)$ are prime powers. The construction is based on Theorem 6.45 using affine and projective geometries.

Family 11 (Wilson (unpublished); Brouwer [339])
$v = 2(q^m + q^{m-1} + \cdots + q) + 1$, $k = q^m$, $\lambda = q^{m-1}(q-1)/2$, $n = (q^m + q^{m-1})/2$, q an odd prime power, m a positive integer. The construction is based on symmetric group divisible designs using projective geometries and Hadamard designs.

Family 12 (Spence [1942], Jungnickel and Pott [1234], Ionin [1163])
$v = q^{d+1}(r^{2m}-1)/(r-1)$, $k = r^{2m-1}q^d$, $\lambda = (r-1)r^{2m-2}q^{d-1}$, $n = r^{2m-2}q^{2d}$, whenever q and $r = (q^{d+1}-1)/(q-1)$ are prime powers. The construction is based on Theorem 6.44 using McFarland difference sets.

Family 13 (Davis and Jedwab [635])
$v = 2^{2d+4}(2^{2d+2}-1)/3$, $k = 2^{2d+1}(2^{2d+3}+1)/3$, $\lambda = 2^{2d+1}(2^{2d+1}+1)/3$, $n = 2^{4d+2}$. The designs are constructed via noncyclic difference sets.

Family 14 (Chen [486])
$v = 4q^{2d}(q^{2d}-1)/(q^2-1)$, $k = q^{2d-1}(1+2(q^{2d}-1)/(q+1))$, $\lambda = q^{2d-1}(q-1)(q^{2d-1}+1)/(q+1)$, $n = q^{4d-2}$, whenever q is the square of an odd prime or a power of 2 or 3. The designs are constructed via noncyclic difference sets.

Family 15 (Ionin [1163])
$v = q^d(r^{2m}-1)/((q-1)(q^d+1))$, $k = q^d r^{2m-1}$, $\lambda = q^d(q^d+1)(q-1)r^{2m-2}$, $n = q^{2d}r^{2m-2}$, where q and $r = q^{d+1}+q-1$ are prime powers. The construction is based on Theorem 6.44 using the complements of McFarland difference sets.

Family 16 (Ionin [1163])
$v = 2\cdot 3^d(q^{2m}-1)/(3^d+1)$, $k = 3^d q^{2m-1}$, $\lambda = 3^d(3^d+1)q^{2m-2}/2$, $n = 3^{2d}q^{2m-2}$, where $q = (3^{d+1}+1)/2$ is a prime power. The construction is based on Theorem 6.44 using Spence difference sets.

Family 17 (Ionin [1163])
$v = 3^d(q^{2m}-1)/(2(3^d-1))$, $k = 3^d q^{2m-1}$, $\lambda = 2\cdot 3^d(3^d-1)q^{2m-2}$, $n = 3^{2d}q^{2m-2}$, where $q = 3^{d+1}-2$ is a prime power. The construction is based on Theorem 6.44 using the complements of Spence difference sets.

Family 18 (Ionin [1163])
$v = 2^{2d+3}(q^{2m}-1)/(q+1)$, $k = 2^{2d+1}q^{2m-1}$, $\lambda = 2^{2d-1}(q+1)q^{2m-2}$, $n = 2^{4d+2}q^{2m-2}$, where $q = (2^{2d+3}+1)/3$ is a prime power. The construction is based on Theorem 6.44 using Davis–Jedwab difference sets.

Family 19 (Ionin [1163])
$v = 2^{2d+3}(q^{2m}-1)/(3q-3)$, $k = 2^{2d+1}q^{2m-1}$, $\lambda = 3\cdot 2^{2d-1}(q-1)q^{2m-2}$, $n = 2^{4d+2}q^{2m-2}$, where $q = 2^{2d+3}-3$ is a prime power. The construction is based on Theorem 6.44 using the complements of Davis–Jedwab difference sets.

Family 20 (Ionin [1164])
$v = 1 + pq(q^{e+1}-1)/(q-1)$, $k = r^{m+1}$, $\lambda = p^d(p^{d-1}q^e-1)/(p-1)$, whenever p, $q = (p^d-1)/(p-1)$, and $r = p^d(q^{e+1}-1)/(q-1)$ are prime powers. The construction is based on Theorem 6.45 using residual and derived designs of the complements of designs of Family 10. The only known realization of these parameters occurs when $p = 2$, $q = 2^d-1$ is a Mersenne prime, and $r = 2^{2d}$. This gives parameters $v = 1 + 2^{d+1}(2^{dm}-1)/(2^d+1)$, $k = 2^{2dm}$, $\lambda = 2^{2dm-d-1}(2^d+1)$, $n = 2^{2dm-d-1}(2^d-1)$.

Family 21 (Kharaghani [1285], Ionin and Kharaghani [1168])
$v = 4t^2(q^{m+1}-1)/(q-1)$, $k = (2t^2-t)q^m$, $\lambda = (t^2-t)q^m$, $n = t^2q^m$, whenever $q = (2t-1)^2$ is a prime power and there exists a productive regular Hadamard matrix with row sum $2t$. A regular Hadamard matrix H with row sum $2t$ is *productive* if there is a set $\mathcal{H}$ of regular Hadamard matrices with row sum $2t$ and a permutation σ of $\mathcal{H}$ such that $H \in \mathcal{H}$, σ^{4t} is the identity permutation, $(\sigma X)(\sigma Y)^T = XY^T$ for all $X, Y \in \mathcal{H}$, and $H + \sigma H + \sigma^2 H + \cdots + \sigma^{4|t|-1}H = \pm 2J$. All Bush-type Hadamard matrices (§V.1) are productive; for any d there exists a productive regular Hadamard

matrix with row sum $\pm 2 \cdot 3^d$; the Kronecker product of a Bush-type matrix and a productive regular Hadamard matrix is productive [1165]. The construction is based on Theorem 6.44.

Special constructions

(133,33,8) via a difference set [1013].
(176,50,14) from the Higman–Sims group [1099]. The latter acts on the design as a 2-transitive automorphism group.
(56,11,2) constructed in terms of the rank-3 group PSL(3, 4) and its associated strongly regular graph [1018].
(79,13,2) by using an automorphism group of order 110 [114].
(71,15,3) obtained from embedding a quasi-residual 2-(56,70,15,12,3) design [179, 1005]. The latter is constructed using eigenvalue techniques.
(41,16,6) via coding theory and an automorphism group of order 15 [326].
(66,26,10) using an automorphism group of order 55 [2067].
(49,16,5) via an automorphism group of order 15 [352].
(70,24,8) via automorphism group of order 42 [1185].
(78,22,6) using an automorphism group of order 39 [1186]; also via embedding of the Witt–Mathieu 3-(22,6,1) design [2045].
(71,21,6) via automorphism group of order 21 [1187].
(160,54,18) using the incidence matrix of the point-hyperplane design of PG(3, 3) and 4×4-circulant matrices [1949].
(189,48,12) using an automorphism group $G = F_{21}$ wr $\mathbb{Z}_2$, the wreath product of Frobenius group F_{21} and cyclic group $\mathbb{Z}_2$ [1182].
(105,40,15) using an automorphism group $G = F_{20} \times \mathbb{Z}_5$, the direct product of Frobenius group F_{20} and cyclic group $\mathbb{Z}_5$ [1183].
(14080,1444,148) using the sporadic simple Fischer group $Fi(22)$, which acts as a primitive rank 3 permutation group on points and blocks [681].

6.9 Symmetric Designs with n ≤ 25

6.47 Table A listing of symmetric (v, k, λ) designs with $n = k - \lambda \le 25$, $k \le v/2$, and $4n - 1 < v < n^2 + n + 1$ satisfying $(v - 1)\lambda = k(k - 1)$ and the Bruck–Ryser–Chowla condition. If a design is known to exist, one solution is given. Parameters for which existence is undecided are marked by a question mark.

n	v	k	λ	Solution
4	16	6	2	Base block: 0000 1000 0100 0010 0001 1111 (mod (2, 2, 2, 2)).
6	25	9	3	Points: $A, B, C, D, E, F, G, 1_i, 2_i, 3_i, 4_i, 5_i, 6_i$, $i = 0, 1, 2$ (mod 3), Automorphisms: $\rho = (A)(B)(C)(D)(E)(F)(G)(I_0\ I_1\ I_2)$, $I = 1, \ldots, 6$, $\tau_1 = (A\ D)(B\ C)(E)(F)(G)(1_i)(2_i)(3_i\ 6_{i+1})(4_i\ 5_{i+1})$, $\tau_2 = (A\ C)(B\ D)(E)(F)(G)(1_i)(2_i)(3_i\ 5_{i+1})(4_i\ 6_{i+1})$, Base blocks: $1_0 1_1 1_2 3_0 3_1 3_2 5_0 5_1 5_2$, $2_0 2_1 2_2 3_0 3_1 3_2 6_0 6_1 6_2$, $EFG1_0 1_1 1_2 2_0 2_1 2_2$, $EFG3_0 3_1 3_2 4_0 4_1 4_2$, $ABE1_0 2_0 3_0 4_0 5_0 6_0$, $ACF1_0 2_2 3_1 4_0 5_2 6_1$, $ADG1_2 2_0 3_1 4_0 5_1 6_2$.
7	37	9	2	Base block: 1 7 9 10 12 16 26 33 34 (mod 37).

n	v	k	λ	Solution
7	31	10	3	Points: A, B, C, $1_i, 2_i, 3_i, 4_i$, $i = 0, 1, 2, 3, 4, 5, 6 \pmod 7$, Automorphisms: $\rho = (A)(B)(C)(I_0\ I_1\ I_2\ I_3\ I_4\ I_5\ I_6)$, $I = 1, 2, 3, 4$, $\sigma = (A\ B\ C)(1_i\ 2_i\ 3_i)(4_i)$, Base blocks: $A1_11_62_22_53_33_44_14_24_4$, $1_31_61_52_32_62_53_33_63_54_0$, $ABC1_01_11_21_31_41_51_6$.
9	56	11	2	Points: $1_i, 2_i, 3_i, 4_i, 5_i, 6_i, 7_i, 8_i$, $i = 0, 1, \ldots, 6 \pmod 7$, Automorphisms: $\rho = (I_0\ I_1\ I_2\ I_3\ I_4\ I_5\ I_6)$, $I = 1, 2, 3, 4, 5, 6, 7, 8$, $\sigma = (1_i\ 2_{2i}\ 3_{4i})(4_i\ 5_{2i}\ 6_{4i})(7_i\ 7_{2i}\ 7_{4i})(8_i\ 8_{2i}\ 8_{4i})$, $\tau = (1_i\ 4_{6i})(2_i\ 5_{6i})(3_i\ 6_{6i})(7_i\ 8_{6i})$, Base blocks: $1_12_23_34_15_26_47_07_37_67_58_0$, $1_21_52_22_53_13_64_04_14_67_18_6$.
9	45	12	3	Base block: 000 001 002 100 110 120 200 211 222 300 312 321 $\pmod{(5, 3, 3)}$.
9	40	13	4	Base block: 1 2 3 5 6 9 14 15 18 20 25 27 35 $\pmod{40}$.
9	36	15	6	Base block: 11 22 33 44 55 01 02 03 04 05 10 20 30 40 50 $\pmod{(6, 6)}$.
10	41	16	6	Points: A, $1_i, 2_i, 3_i, 4_i, 5_i, 6_i, 7_i, 8_i$, $i = 0, 1, 2, 3, 4 \pmod 5$, Automorphisms: $\rho = (A)(I_0\ I_1\ I_2\ I_3\ I_4)$, $I = 1, 2, 3, 4, 5, 6, 7, 8$, $\sigma = (A)(1_i\ 2_i\ 3_i)(4_i\ 5_i\ 8_i)(6_i)(7_i)$, Base blocks: $A1_01_11_21_31_42_02_12_22_32_43_03_13_23_33_4$, $A1_11_42_22_33_04_14_24_34_46_16_47_27_35_08_0$, $1_21_32_22_33_23_34_04_24_35_05_25_38_08_28_36_0$, $1_11_42_12_43_13_47_17_27_37_44_24_35_25_38_28_3$, $3_03_23_32_02_12_46_06_16_44_24_38_18_47_17_45_0$.
11	79	13	2	Points: $A, B, 1_i, 2_i, 3_i, 4_i, 5_i, 6_i, 7_i$, $i = 0, 1, \ldots, 10 \pmod{11}$, Automorphisms: $\rho = (A)(B)(I_0\ I_1\ \cdots\ I_{10})$, $I = 1, 2, \ldots, 7$, $\sigma = (A)(B)(1_i\ 2_{4i}\ 3_{5i}\ 4_{9i}\ 5_{3i})\ (6_i\ 6_{4i}\ 6_{5i}\ 6_{9i}\ 6_{3i})(7_i\ 7_{4i}\ 7_{5i}\ 7_{9i}\ 7_{3i})$, $\tau = (A\ B)(1_i\ 1_{10i})(2_i\ 2_{10i})(3_i\ 3_{10i})$ $(4_i\ 4_{10i})(5_i\ 5_{10i})(6_i\ 6_{10i})(7_i\ 7_{10i})$, Base blocks: $AB6_06_16_26_36_46_56_66_76_86_96_{10}$, $AB7_07_17_27_37_47_57_67_77_87_97_{10}$, $A1_11_42_42_53_53_94_94_35_35_16_07_0$, $B1_{10}1_72_72_63_63_24_24_85_85_{10}6_07_0$, $1_02_22_92_42_73_53_65_45_76_26_97_57_6$.
11	49	16	5	Points: $A, B, C, D, 1_i, 2_i, 3_i, 4_i, 5_i, 6_i, 7_i, 8_i, 9_i$, $i = 0, 1, 2, 3, 4 \pmod 5$, Automorphisms: $\rho = (A)(B)(C)(D)(I_0\ I_1 \cdots\ I_4)$, $I = 1, 2, \ldots, 9$, $\sigma = (A)(B\ C\ D)(1_i\ 2_i\ 3_i)(4_i\ 5_i\ 6_i)(7_i\ 8_i\ 9_i)$, Base blocks: $A7_07_17_27_37_48_08_18_28_38_49_09_19_29_39_4$, $B4_04_14_24_34_45_05_15_25_35_49_09_19_29_39_4$, $AB1_01_12_02_23_04_04_15_25_46_37_07_18_08_3$, $BC1_01_22_33_03_14_14_36_26_37_37_48_29_29_4$, $1_01_11_21_32_03_44_45_05_46_26_47_28_28_39_19_4$.

n	v	k	λ	Solution
12	71	15	3	Points: $A, 1_i, 2_i, \ldots, 10_i$, $i = 0, 1, \ldots, 6 \pmod 7$, Automorphisms: $\rho = (A)(I_0\ I_1\ \cdots\ I_6)$, $I = 1, 2, \ldots, 10$, $\tau = (A)(1_i)(2_i)(3_i\ 4_i)(5_i\ 6_i)(7_i\ 8_i)(9_i\ 10_i)$, $\sigma = (A)(K_0)(K_1\ K_2\ K_4)(K_3\ K_6\ K_5)(3_i\ 5_{2i}\ 7_{4i})(4_i\ 6_{2i}\ 8_{4i})$, $K = 1, 2, 9, 10$, Base blocks: $A1_01_11_21_31_41_51_62_02_12_22_32_42_52_6$, $A1_02_03_23_45_15_47_17_24_36_68_59_19_29_4$, $1_11_21_43_13_35_25_67_47_54_14_36_26_68_48_5$, $1_11_21_43_05_07_04_06_08_09_19_29_410_110_210_4$, $1_02_12_35_15_37_04_14_24_56_06_26_69_59_610_1$.
12	61	16	4	Points: $A, 1_i, 2_i, \ldots, 20_i$, $i = 0, 1, 2 \pmod 3$, Automorphisms: $\rho = (A)(I_0\ I_1\ I_2)$, $I = 1, \ldots, 20$, $\sigma = (A)(1_i\ 2_i\ 3_i\ 4_i\ 5_i)(6_i\ 7_i\ 8_i\ 9_i\ 10_i)$ $(11_i\ 12_i\ 13_i\ 14_i\ 15_i)(16_i\ 17_i\ 18_i\ 19_i\ 20_i)$, Base blocks $A1_01_11_22_02_12_23_03_13_24_04_14_25_05_15_2$, $A1_01_11_26_07_18_19_011_012_113_114_016_017_118_119_0$, $1_02_13_14_010_110_28_18_26_07_011_111_212_112_220_018_0$, $1_02_13_14_015_115_213_113_211_012_016_116_217_117_210_08_0$, $1_02_13_14_020_120_218_118_216_017_06_16_27_17_215_013_0$.
13	81	16	3	?
13	69	17	4	Points: $A, B, C, D, 1_i, 2_i, \ldots, 5_i$, $i = 0, \ldots, 12 \pmod{13}$, Automorphisms: $\rho = (A)(B)(C)(D)(I_0\ I_1\ \cdots\ I_{12})$, $I = 1, 2, \ldots, 5$, $\tau = (A\ B\ C\ D)(1_i\ 2_i\ 3_i\ 4_i)(5_i)$, Base blocks: $ABCD1_01_11_21_31_41_51_61_71_81_91_{10}1_{11}1_{12}$, $A1_11_31_92_22_62_53_43_{12}3_{10}4_84_{11}4_75_05_45_{12}5_{10}$, $1_01_11_31_92_02_12_32_93_03_13_33_94_04_14_34_95_0$.
14	121	16	2	?
15	71	21	6	Points: $A, 1_i, \ldots, 10_i$, $i = 0, 1, \ldots, 6 \pmod 7$, Automorphisms: $\rho = (A)(I_0\ I_1\ \cdots\ I_6)$, $I = 1, 2, \ldots, 10$, $\sigma = (A)(K_0)(K_1\ K_2\ K_4)(K_3\ K_6\ K_5)(4_i\ 5_{2i}\ 6_{4i})$ $(7_i\ 8_{2i}\ 9_{4i})$, $K = 1, 2, 3, 10$, Base blocks: $1_01_11_21_31_41_51_62_02_12_22_32_42_52_63_03_13_23_33_43_53_6$, $1_02_03_03_13_23_34_04_05_06_07_07_27_38_08_48_69_09_19_510_110_210_4$, $2_12_22_43_13_23_34_34_44_55_65_15_36_56_26_67_37_68_68_59_59_3$, $1_01_31_61_52_03_04_14_55_25_36_46_67_37_47_58_68_18_39_59_29_6$, $1_31_61_53_13_23_34_14_34_65_25_65_56_46_56_37_08_09_010_310_610_5$, $A1_31_52_12_43_23_33_40_42_43_46_50_52_71_74_76_82_83_95_10_110_2$, $1_11_42_02_12_53_34_04_14_55_25_66_08_38_59_09_39_49_510_410_510_6$.
15	61	25	10	Points: $A, 1_i, \ldots, 12_i$, $i = 0, 1, \ldots, 4 \pmod 5$, Automorphisms: $\rho = (A)(I_0\ I_1\ \cdots\ I_4)$, $I = 1, 2, \ldots, 12$, $\tau = (A)(1_i\ 2_i\ 3_i\ 4_i\ 5_i)(6_i\ 7_i\ 8_i\ 9_i\ 10_i)(11_i)(12_i)$, Base blocks: $1_01_11_21_31_42_02_12_22_32_43_03_13_23_33_44_04_14_24_34_45_05_15_25_35_4$, $A1_11_42_02_12_43_03_23_34_24_36_07_17_48_28_39_010_110_210_310_411_111_412_212_3$, $1_02_12_43_23_34_05_15_25_35_46_26_37_08_09_19_410_110_210_310_411_211_312_012_212_3$, $1_11_42_12_43_13_44_14_45_15_46_06_16_47_07_17_48_08_18_49_09_19_410_010_110_4$, $1_21_32_22_33_23_34_24_35_25_36_16_47_17_48_18_49_19_410_110_411_011_111_211_311_4$.

n	v	k	λ	Solution
16	154	18	2	?
16	115	19	3	?
16	96	20	4	Base block: 00000 01000 10000 11000 00001 00101 00011 00111 00002 01102 10012 11112 00003 01013 11103 10113 00004 10104 01114 11014 (mod $(2,2,2,2,6)$).
16	85	21	5	Base block: 0 1 2 4 7 8 14 16 17 23 27 28 32 34 43 46 51 54 56 64 68 (mod 85).
16	78	22	6	Points: $1_i,\ldots,6_i$, $i=0,1,\ldots,12$ (mod 13), Automorphisms: $\rho=(I_0\ I_1\ \cdots\ I_{12})$, $I=1,2,\ldots,6$, $\tau=(1_i)(6_i)(2_i\ 3_i)(4_i\ 5_i)$, Base blocks: $1_01_11_31_91_41_{12}1_{10}2_22_62_53_23_63_54_44_{12}4_{10}5_45_{12}5_{10}6_46_{12}6_{10}$, $2_02_22_62_52_72_82_{11}1_11_31_93_43_{12}3_{10}4_24_64_55_75_85_{11}6_76_86_{11}$, $4_04_24_64_54_74_84_{11}1_71_81_{11}2_22_62_53_73_83_{11}5_15_35_96_46_{12}6_{10}$, $6_06_16_36_96_46_{12}6_{10}1_11_31_92_12_32_93_13_33_94_24_64_55_25_65_5$.
16	70	24	8	Points: $1_i,\ldots,10_i$, $i=0,1,\ldots,6$ (mod 7), Automorphisms: $\rho=(I_0\ I_1\ \cdots\ I_6)$, $I=1,2,\ldots,10$, $\sigma=(K_0)(K_1\ K_2\ K_4)(K_3\ K_6\ K_5)(4_i\ 5_{2i}\ 6_{4i})$ $(7_i\ 8_{2i}\ 9_{4i})$, $K=1,2,3,10$, $\tau=(3_i)(10_i)(1_i\ 2_i)(4_i\ 7_i)(5_i\ 8_i)(6_i\ 9_i)$, Base blocks: $1_01_11_21_42_02_12_22_43_03_33_63_54_14_65_25_56_36_47_17_68_28_59_39_4$, $10_010_310_610_51_01_31_61_52_02_32_62_54_04_15_05_26_06_47_07_18_08_29_09_4$, $10_010_310_610_52_02_12_22_43_03_13_23_44_04_65_05_56_06_37_27_58_48_39_19_6$, $10_010_21_31_42_02_53_03_14_04_14_34_55_15_25_35_56_26_37_07_37_47_69_19_5$.
16	66	26	10	Points: $1_i,\ldots,6_i$, $i=0,1,\ldots,10$ (mod 11), Automorphisms: $\rho=(I_0\ I_1\ \cdots\ I_{10})$, $I=1,2,\ldots,6$, $\sigma=(6_i)(1_i\ 2_i\ 3_i\ 4_i\ 5_i)$, Base blocks: $1_11_31_41_51_92_22_62_72_82_{10}3_23_63_73_83_{10}4_14_34_44_54_96_16_36_46_56_95_0$, $1_21_61_71_81_{10}2_22_62_72_82_{10}3_23_63_73_83_{10}4_24_64_74_84_{10}5_25_65_75_85_{10}6_0$.
16	64	28	12	Base block: 0000 0001 0002 0003 0004 0005 0006 0010 0012 0013 0100 0101 0104 0110 0115 0116 1001 1002 1005 1012 1014 1016 1101 1103 1106 1113 1114 1115 (mod $(2,2,2,8)$).
18	191	20	2	?
18	79	27	9	Points: $A,1_i,\ldots,6_i$, $i=0,1,\ldots,12$ (mod 13), Automorphisms: $\rho=(A)(I_0\ I_1\ \cdots\ I_{12})$, $I=1,2,\ldots,6$, $\tau_1=(A)(1_i)(2_i)(3_i\ 4_i)(5_i\ 6_i)$, $\tau_2=(A)(1_i)(2_i)(3_i\ 5_i)(4_i\ 6_i)$, Base blocks: $A1_01_11_21_31_41_51_61_71_81_91_{10}1_{11}1_{12}2_02_12_22_32_42_52_62_72_82_92_{10}2_{11}2_{12}$, $A1_01_11_31_92_02_12_32_93_13_33_93_43_{12}3_{10}4_24_64_55_15_35_95_45_{12}5_{10}6_26_66_65$, $1_11_31_92_44_{12}2_{10}2_82_{11}2_73_13_33_93_83_{11}3_74_24_64_55_25_65_65_61_63_69_68_61_67$, $1_41_{12}1_{10}1_81_{11}1_72_12_32_93_13_33_93_83_{11}3_74_14_34_94_84_{11}4_75_25_65_65_62_66_65$.
19	211	21	2	?
19	155	22	3	?
19	101	25	6	Base block: 1 5 16 19 24 25 31 36 37 52 54 56 58 68 71 78 79 80 81 84 87 88 92 95 97 (mod 101).

n	v	k	λ	Solution
19	85	28	9	?
20	139	24	4	?
20	121	25	5	Points: $A, B, C, D, E, \infty_1, \ldots, \infty_{16}, 1_i, \ldots, 20_i$, $i = 0, \ldots, 4 \pmod 5$, Automorphisms: $\rho = (A)(B)(C)(D)(E)(\infty_i)(I_0\ I_1\ \cdots\ I_4)$, $i = 1, \ldots, 16$, $I = 1, 2, \ldots, 20$, $\sigma = (\infty_1)(\infty_2\ \infty_5\ \infty_6\ \infty_7\ \infty_8)(\infty_3\ \infty_9\ \infty_{10}\infty_{11}\ \infty_{12})$ $(\infty_4\ \infty_{13}\ \infty_{14}\ \infty_{15}\ \infty_{16})(A\ 1_3\ 2_3\ 3_3\ 4_3)(B\ 1_4\ 2_4\ 3_4\ 4_0)$ $(C\ 1_2\ 2_2\ 3_0\ 4_4)(D\ 1_1\ 2_0\ 3_2\ 4_2)(E\ 1_0\ 2_1\ 3_1\ 4_1)$ $(5_i)(6_i\ 9_i\ 10_i\ 11_i\ 12_i)(7_i\ 13_i\ 14_i\ 15_i\ 16_i)(8_i\ 17_i\ 18_i\ 19_i\ 20_i)$, Base blocks: $ABCDE1_01_11_21_31_42_02_12_22_32_43_03_13_23_33_34_04_14_24_34_4$, $ABCDE5_05_15_25_35_46_06_16_26_36_47_07_17_27_37_48_08_18_28_38_4$, $ABCDE9_09_19_29_39_412_012_112_212_312_414_014_114_214_314_4$ $15_015_115_215_315_4$, $ABCDE13_013_113_213_313_416_016_116_216_316_4$ $18_018_118_218_318_419_019_119_219_319_4$, $ABCDE17_017_117_217_317_420_020_120_220_320_4$ $10_010_110_210_310_411_011_111_211_311_4$, $A1_02_03_04_09_112_114_115_113_216_218_219_25_36_37_38_3$ $17_420_410_411_4\infty_1\infty_2\infty_3\infty_4$, $A1_02_03_04_013_116_118_119_117_220_210_211_29_312_314_315_3$ $5_46_47_48_4\infty_5\infty_8\infty_{10}\infty_{11}$, $A1_02_03_04_017_120_110_111_15_26_27_28_213_316_318_319_3$ $9_412_414_415_4\infty_9\infty_{12}\infty_{14}\infty_{15}$, $A1_02_03_04_05_16_17_18_19_212_214_215_217_320_310_311_3$ $13_416_418_419_4\infty_{13}\infty_{16}\infty_6\infty_7$.
21	131	26	5	?
21	109	28	7	Base block: 0 1 3 5 7 9 15 16 21 22 25 26 27 35 38 45 48 49 63 66 73 75 78 80 81 89 97 105 (mod 109).
21	85	36	15	?
22	201	25	3	?
22	127	28	6	?
22	97	33	11	?
23	301	25	2	?
23	103	34	11	?
25	352	27	2	?
25	253	28	3	?
25	204	29	4	?
25	175	30	5	Base block: 000 100 200 300 400 001 011 021 031 041 002 112 222 332 442 003 123 243 313 433 004 134 214 344 424 005 145 235 325 415 (mod $(5, 5, 7)$).
25	156	31	6	Base block: 0 1 5 11 13 25 28 39 46 55 58 65 68 74 76 86 87 91 111 117 118 119 122 123 125 127 134 140 142 143 147 (mod 156).
25	133	33	8	Base block: 1 4 5 14 16 19 20 21 25 38 54 56 57 64 66 70 76 80 83 84 91 93 95 98 100 101 105 106 114 123 125 126 131 (mod 133).

n	v	k	λ	Solution
25	120	35	10	?
25	112	37	12	?
25	105	40	15	Points: $\infty_1, \ldots, \infty_5$, $6_i, \ldots, 25_i$, $i = 0, 1, 2, 3, 4 \pmod 5$, Automorphisms: $\rho = (\infty_1)(\infty_2)(\infty_3)(\infty_4)(\infty_5)$ $(6_0, 6_1, 6_2, 6_3, 6_4) \ldots (25_0, 25_1, 25_2, 25_3, 25_4)$, $\gamma = (\infty_1, \infty_2, \infty_3, \infty_4, \infty_5)(6_i, 7_i, 8_i, 9_i, 10_i)$ $(11_i, 12_i, 13_i, 14_i, 15_i)(16_i, 17_i, 18_i, 19_i, 20_i)(21_i, 22_i, 23_i, 24_i, 25_i)$, $i = 0, 1, 2, 3, 4$, $\kappa = (\infty_1)(\infty_2, \infty_3, \infty_5, \infty_4)(6_i, 11_i)(7_i, 13_i, 10_i, 14_i)$ $(8_i, 15_i, 9_i, 12_i)(16_i, 21_i)(17_i, 23_i, 20_i, 24_i)(18_i, 25_i, 19_i, 22_i)$, $i = 0, 1, 2, 3, 4$. Base blocks: $6_0 6_1 6_2 6_3 6_4\ 7_0 7_1 7_2 7_3 7_4\ 10_0 10_1 10_2 10_3 10_4\ 11_0 11_1 11_2 11_3 11_4$ $13_0 13_1 13_2 13_3 13_4\ 14_0 14_1 14_2 14_3 14_4\ 16_0 16_1 16_2 16_3 16_4$ $21_0 21_1 21_2 21_3 21_4$, $\infty_1\ 6_1\ 7_0 7_3\ 8_2 8_4\ 9_2 9_4\ 10_0 10_3\ 11_0 11_1 11_4\ 12_2\ 13_3 13_4\ 14_3 14_4\ 15_2$ $16_3\ 17_0 17_1 17_4\ 18_0 18_1 18_2\ 19_0 19_1 19_2\ 20_0 20_1 20_4\ 21_1 21_4$ $22_1 22_3 22_4\ 25_1 25_3 25_4$, $\infty_1 \infty_3 \infty_4\ 6_0 6_1 6_3 6_4\ 7_2 7_3\ 8_1 8_2\ 9_1 9_2\ 10_2 10_3\ 11_0 11_2 11_3\ 12_0 12_3$ $15_0 15_3\ 16_4\ 17_0 17_2\ 18_1 18_3\ 19_1 19_3\ 20_0 20_2\ 21_0 21_1 21_4\ 22_3$ $23_1 23_2\ 24_1 24_2\ 25_3$.
25	100	45	20	Points: $A, 1_i, \ldots, 9_i$, $i = 0, 1, \ldots, 10 \pmod{11}$, Automorphisms: $\rho = (A)(I_0\ I_1\ \cdots\ I_{10})$, $I = 1, 2, \ldots, 9$, $\sigma = (A)(1_i\ 2_i\ 3_i\ 4_i)(5_i\ 6_i\ 7_i\ 8_i)(9_i)$, Base blocks: $A 1_0 1_1 1_2 1_3 1_4 1_5 1_6 1_7 1_8 1_9 1_{10} 2_0 2_1 2_2 2_3 2_4 2_5 2_6 2_7 2_8 2_9 2_{10}$ $3_0 3_1 3_2 3_3 3_4 3_5 3_6 3_7 3_8 3_9 3_{10} 4_0 4_1 4_2 4_3 4_4 4_5 4_6 4_7 4_8 4_9 4_{10}$, $A 1_0 1_2 1_6 1_7 1_{10} 1_8 2_0 2_1 2_3 2_9 2_5 2_4 3_0 3_2 3_6 3_7 3_{10} 3_8 4_0 5_2 5_6 5_7$ $5_{10} 5_8 6_1 6_3 6_9 6_5 6_4 7_1 7_3 7_9 7_5 7_4 8_2 8_6 8_7 8_{10} 8_8 9_2 9_6 9_7 9_{10} 9_8$, $1_1 1_3 1_9 1_5 1_4 2_1 2_3 2_9 2_5 2_4 3_2 3_6 3_7 3_{10} 3_8 4_2 4_6 4_7 4_{10} 4_8 5_0 5_1 5_3$ $5_9 5_5 5_4 6_0 6_2 6_6 6_7 6_{10} 6_8 7_0 7_1 7_3 7_9 7_5 7_4 8_0 9_0 9_2 9_6 9_7 9_{10} 9_8$, $1_2 1_6 1_7 1_{10} 1_8 2_2 2_6 2_7 2_{10} 2_8 3_2 3_6 3_7 3_{10} 3_8 4_2 4_6 4_7 4_{10} 4_8 5_0 5_2$ $5_6 5_7 5_{10} 5_8 6_0 6_2 6_7 6_{10} 6_8 7_0 7_2 7_6 7_7 7_{10} 7_8 8_0 8_2 8_6 8_7 8_{10} 8_8 9_0$.

See Also

§V.1	Hadamard designs are an important class of symmetric designs.
§VI.18	Symmetric designs are often constructed from difference sets.
§VI.65	Youden squares are an arrangement of the blocks of a symmetric design.
§VII.2	Projective planes are another important class of symmetric designs.
§VII.3	Divisible semiplanes are symmetric group divisible designs.
[225]	A comprehensive book for combinatorial designs.
[1016]	This second edition contains more results on symmetric designs.
[2141]	*Semibiplanes* are connected incidence structures of points and lines, in which every two points lie on 0 or two common lines, and every two lines meet in 0 or two points. A semibiplane has the same number of points as lines; every line has k points, and every point lies on k lines.

References Cited: [107, 114, 179, 225, 250, 310, 326, 339, 352, 356, 413, 486, 501, 503, 635, 681, 682, 812, 1005, 1013, 1016, 1017, 1018, 1019, 1099, 1163, 1164, 1165, 1168, 1169, 1170, 1182, 1183, 1185, 1186, 1187, 1234, 1256, 1260, 1283, 1285, 1378, 1397, 1421, 1553, 1564, 1591, 1616, 1773, 1840, 1874, 1908, 1939, 1942, 1946, 1949, 2045, 2067, 2070, 2089, 2104, 2136, 2141]

7 Resolvable and Near-Resolvable Designs

R. Julian R. Abel
Gennian Ge
Jianxing Yin

7.1 Definitions and Examples

7.1 A *parallel class* or *resolution class* in a design is a set of blocks that partition the point set. A *partial parallel class* is a set of blocks that contain no point of the design more than once.

7.2 A *resolvable balanced incomplete block design* is a BIBD(v, k, λ) whose blocks can be partitioned into parallel classes. The notation RBIBD(v, k, λ) is commonly used.

7.3 **Example** An RBIBD$(9, 3, 1)$. (Each column is a parallel class.)

{1,2,3}	{1,4,7}	{1,5,9}	{1,6,8}
{4,5,6}	{2,5,8}	{2,6,7}	{2,4,9}
{7,8,9}	{3,6,9}	{3,4,8}	{3,5,7}

7.4 An *affine design* (or *affine resolvable design*) is an RBIBD with the property that any two blocks in different parallel classes intersect in a constant number of points.

7.5 A (K, λ)-*frame* is a (K, λ)-GDD $(X, \mathcal{G}, \mathcal{A})$ whose blocks can be partitioned into partial parallel classes each of which contains exactly the points of $X \backslash G$ for some $G \in \mathcal{G}$. The group type of the frame is the group type of the underlying GDD.

7.6 **Example** A (3,1) frame of type 2^4.

groups	{2,3}	{4,7}	{5,9}	{6,8}
blocks	{4,5,6}	{2,5,8}	{2,6,7}	{2,4,9}
	{7,8,9}	{3,6,9}	{3,4,8}	{3,5,7}

7.7 A *near parallel class* is a partial parallel class missing a single point. A *near-resolvable design*, NRB$(v, k, k-1)$, is a BIBD$(v, k, k-1)$ with the property that the blocks can be partitioned into near parallel classes. For such a design, every point is absent from exactly one class.

7.8 **Example** An NRB$(7, 3, 2)$.

missing point	{ 0 }	{ 1 }	{ 2 }	{ 3 }	{ 4 }	{ 5 }	{ 6 }
blocks	{1,2,4}	{2,3,5}	{3,4,6}	{4,5,0}	{5,6,1}	{6,0,2}	{0,1,3}
	{3,5,6}	{4,6,0}	{5,0,1}	{6,1,2}	{0,2,3}	{1,3,4}	{2,4,5}

7.9 **Remark** Necessary conditions for the existence of an RBIBD(v, k, λ) are $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ and $v \equiv 0 \pmod{k}$. The necessary condition for the existence of an NRB$(v, k, k-1)$ is $v \equiv 1 \pmod{k}$.

7.10 Theorem [965] If v and k are both powers of the same prime, then the necessary conditions for the existence of an RBIBD(v, k, λ) are sufficient.

7.11 Theorem The following equivalencies are known.

1. An RBIBD$(v, k, 1)$ is equivalent to a $(k, 1)$-frame of type $(k-1)^r$ where $r = \frac{v-1}{k-1}$.
2. An RBIBD$(k^2, k, 1)$ is equivalent to an affine plane. (See §VII.2.2.)
3. An RBIBD$(4n, 2n, 2n-1)$ is equivalent to a Hadamard matrix of order $4n$ or a $(4n-1, 2n-1, n-1)$-Hadamard design. Also, an NRB$(2n+1, 2n, 2n-1)$ is equivalent to a conference matrix of order $4n+2$. (See §V.1.)
4. An NRB$(v, k, k-1)$ is equivalent to a $(k, k-1)$-frame of type 1^v.

7.12 Remark An RBIBD$(v, 3, 1)$ is a Kirkman triple system; see §2.8.

7.2 Basic Recursive Constructions

7.13 A *basic factorization* $BF_\lambda(2h, m)$ is a resolvable design $(X, \mathcal{A})$ where X contains m points and each block in $\mathcal{A}$ has size h or $2h$ that satisfies the properties: (1) each point of X is contained in exactly λ blocks of size h and (2) $2\lambda_h(x, y) + \lambda_{2h}(x, y) = \lambda$ for each pair $\{x, y\}$ of distinct points of X. The notation $\lambda_k(x, y)$ stands for the number of blocks of size k that contain $\{x, y\}$.

7.14 A basic factorization $BF_\lambda(2h, m)$ is *uniform* if all blocks in each parallel class have the same size.

7.15 Remark [144, 964] A uniform $BF_{k-1}(k, k)$ is equivalent to a $(k, k/2, (k-2)/2)$ RBIBD with an extra block consisting of the entire point set. A uniform $BF_{k-1}(k, m)$ exists if either (1) $k - 1 \equiv 3 \pmod 4$ is a prime power and $m = k$ or (2) k and m are both powers of 2, and $k \le m < k^2$.

7.16 Theorem [144] Let k be even. Suppose that there exist (1) $\frac{k-2}{2}SOLSSOM(n)$, where the symmetric mate is unipotent if n is even and idempotent otherwise, (2) a $BF_\lambda(k, m)$, and (3) an RBIBD(m, k, λ). Then there exists an RBIBD(mn, k, λ) containing n pairwise disjoint RBIBD(m, k, λ)s as subdesigns.

7.17 Theorem Suppose that a resolvable (k, λ)-GDD having u groups of size g and an RBIBD(g, k, λ) both exist. Then there exists an RBIBD(gu, k, λ) containing u disjoint RBIBD(g, k, λ)s as subdesigns.

7.18 Theorem [1967] Let $(X, \mathcal{G}, \mathcal{A})$ be a (k, λ)-frame. Suppose that for each group $G \in \mathcal{G}$, there exists an RBIBD$(|G| + w, k, \lambda)$ containing an RBIBD(w, k, λ) as a subdesign. Then there exists an RBIBD$(|X| + w, k, \lambda)$ containing an RBIBD(w, k, λ) as a subdesign.

7.19 Theorem [2213] Suppose that there exist (1) an RBIBD(u, k, λ), (2) a resolvable TD(k, v), and (3) a BIBD(v, k, λ) whose blocks can be partitioned into s partial parallel classes. If $s \le \lambda[(u-1) + (v-1)]/(k-1)$, then there exists an RBIBD(uv, k, λ) with v disjoint RBIBD(u, k, λ)s as subdesigns.

7.20 Theorem [2193] Let u, g, w and k be positive integers with $1 \le w \le g$. Suppose that there exist (1) a $(g, u+1; 1)$-difference matrix over an abelian group G, (2) a $(g, k, k-1)$ difference family over G containing $(g-1)/k$ pairwise disjoint base blocks, (3) an NRB$(m, k, k-1)$ for each $m \in \{u+1, w\}$, and (4) an RBIBD$(u, k, k-1)$. Then there exists an NRB$(gu + w, k, k-1)$.

7.21 Theorem [848] Let u, g, w and k be positive integers with $1 \le w \le g$. Suppose that there exist (1) a $(g, u+1; 1)$-difference matrix over an abelian group G, (2) an

RBIBD$(g+1,k,k-1)$ over $G\cup\{\infty\}$ that can be generated by $(g+1)/k$ pairwise disjoint base blocks under the action of G (with ∞ fixed), (3) an $(m,k,k-1)$ RBIBD for each $m\in\{u,w+1\}$, and (4) an NRB$(u+1,k,k-1)$. Then there exists an RBIBD$(gu+w+1,k,k-1)$.

7.22 **Remark** Theorems 7.16 through 7.21 are adapted from the constructions in the references. Detailed information and further techniques for construction can be found in [848].

7.23 **Remark** [1782] A block disjoint (v,k,λ) difference family yields a BIBD(v,k,λ) whose blocks can be partitioned into v partial parallel classes. If q is a prime power and a block disjoint (q,k,λ) difference family over $\mathbb{F}_q$ exists, then so does an RBIBD$(kq,k,1)$.

7.24 **Theorem** [848, 1246] Suppose that a resolvable TD(n,λ',n) and an RBIBD(kn,k,λ) both exist. Then an RBIBD(kn^2,kn,μ) also exists where $\mu=\lambda\lambda'\frac{kn-1}{k-1}$.

7.25 **Theorem** [848, 1246] For any prime power q, when $q(nq-1)/(q-1)\le(kq-1)/(k-1)$, the existence of an RBIBD(kq,k,μ) and an RBIBD(nq,q,λ) implies the existence of an RBIBD$(knq^2,kq,\lambda r_\mu)$ with $r_\mu=\mu(kq-1)/(k-1)$.

7.26 **Corollary** For any prime power q, the existence of an RBIBD$(kq,k,k-1)$ implies the existence of an RBIBD$(kq^2,kq,kq-1)$.

7.3 Nonexistence and Asymptotic Existence Results

7.27 **Remark** All parameter sets for which an RBIBD is known not to exist are multiples of parameter sets of affine designs. The theorems in this section are useful for establishing nonexistence results.

7.28 **Theorem** If an RBIBD(v,k,λ) exists, then $b\ge v+r-1$ where b is the number of blocks. When $b=v+r-1$ (or equivalently, $r=k+\lambda$) the RBIBD is an affine design and any two nonparallel lines intersect in exactly $\frac{k^2}{v}$ points.

7.29 **Remark** The condition that $b\ge v+r-1$ is known as *Bose's condition*.

7.30 **Theorem** Consider a (v,k,λ) affine design with replication number r whose nonparallel blocks intersect in $\mu=k^2/v$ points.

1. If $v=tk$ and $k\not\equiv 0 \pmod t$, then no RBIBD$\left(tk,k,\frac{k-1}{t-1}\right)$ exists.
2. If v and r are odd, then k is a perfect square.
3. If v is odd and r is even, then μ is a perfect square.
4. If $r\equiv 2 \pmod 4$ or $r\equiv 3 \pmod 4$, then the square free factor of $\frac{v}{k}$ has no prime divisor $p\equiv 3 \pmod 4$.
5. If $\lambda\in\{1,2\}$, then the affine design is a residual design. See §II.6.4.

7.31 **Theorem** If both k and t are odd, then no RBIBD$(2k,k,t(k-1))$ exists.

7.32 **Theorem** [968] If k is even, then no NRB$(2k+1,k,(k-1))$ exists if $2k+1$ is not the sum of two squares. In particular, no NRB$(21,10,9)$ or NRB$(33,16,15)$ exists.

7.33 **Theorem** Given any positive integers k and λ, there exists an integer $c(k,\lambda)$ such that an RBIBD(v,k,λ) exists whenever $v>c(k,\lambda)$ and the necessary conditions are satisfied.

7.34 **Theorem** For k a positive integer, there exists $n(k)\in\mathbb{Z}^+$ such that an NRB$(v,k,k-1)$ exists whenever $v>n(k)$ and $v\equiv 1 \pmod k$.

7.4 Existence Results for RBIBDs for Specific k and λ

7.35 Table A summary of existence results. Entries shown in the tables referenced are definite exceptions.

k	λ	Exceptions	Possible Exceptions	Largest Possible Exception
3	1	none	none	
3	2	6	none	
4	1	none	none	
4	3	none	none	
5	1		see Table 7.37	645
5	2	15	see Table 7.38	395
5	4	10, 15	see Table 7.39	195
6	5	none	none	
7	1		[961]; no explicit enumeration	294427
7	6		see Table 7.40	462
8	1		see Table 7.41	24480
8	7		see Table 7.42	1488
12	11		explicit enumeration in [1419]	108768
16	15		[964]; no explicit enumeration	83840

7.36 Remark [451] An RBIBD$(v, k, 1)$ exists if $v > exp\{exp\{k^{12k^2}\}\}$ and the necessary conditions are satisfied. However, no specific bounds have been computed for any other pairs of k and λ not specifically mentioned in Table 7.35.

7.37 Table Values of $v \equiv 5 \pmod{20}$ for which no RBIBD$(v, 5, 1)$ is known [7, 40, 41, 848, 2213].

45 345 465 645

7.38 Table Values of $v \equiv 5 \pmod{10}$ for which no RBIBD$(v, 5, 2)$ is known [40, 1600].

15 45 115 130 195 215 235 295 315 335 345 395

7.39 Table Values of $v \equiv 0 \pmod{5}$ for which no RBIBD$(v, 5, 4)$ is known [7, 40, 848].

10 15 135 160 190 195

7.40 Table Values of $v \equiv 0 \pmod{7}$ for which no RBIBD$(v, 7, 6)$ is known [43, 848].

14 84 119 126 133 175 182 189 210 231
238 259 266 287 413 420 427 434 462

7.41 Table Values of $v \equiv 8 \pmod{56}$ for which no RBIBD$(v, 8, 1)$ is known [966].

176	624	736	1128	1240	1296	1408	1464	1520	1576
1744	2136	2416	2640	2920	2976	3256	3312	3424	3760
3872	4264	4432	5216	5720	5776	6224	6280	6448	6896
6952	7008	7456	7512	7792	7848	8016	9752	10200	10704
10760	10928	11040	11152	11376	11656	11712	11824	11936	12216
12328	12496	12552	12720	12832	12888	13000	13280	13616	13840
13896	14008	14176	14232	21904	24480				

7.42 Table Values of $v \equiv 0 \pmod{8}$ for which no RBIBD$(v, 8, 7)$ is known [36, 847, 1631].

24 160 168 192 224 240 312
336 440 552 560 744 1464 1488

7.5 Existence Results for NRBs for Specific k

7.43 **Theorem** [7, 34, 43, 848, 2193] The necessary condition, $v \equiv 1 \pmod{k}$, for the existence of an NRB$(v, k, k-1)$ is sufficient for $k \leq 7$. For $k = 8$, it is sufficient, except possibly for $v = 385$ or 553.

7.44 **Table** Bounds on the existence of NRB$(v, k, k-1)$s. N denotes the number of unknown NRBs.

k	$n(k) \leq$	N
9	973	26
10	2681	43
12	6289	37
15	126331	1116

k	$n(k) \leq$	N
16	10033	151
17	464373	2647
18	103609	463
22	716057	2643

k	$n(k) \leq$	N
24	58105	290
26	1238849	4530
28	121073	651
30	490141	1197

7.6 Some Explicit Constructions

7.45 **Construction** Suppose p is a prime power, x is a primitive element in $\mathbb{F}_p$, and $u = (p-1)/k$. Then developing the following base blocks over $\mathbb{F}_p$ gives an NRB$(p, k, k-1)$: $\{x^i, x^{u+i}, x^{2u+i} \ldots, x^{(k-1)u+i}\}$ for $0 \leq i < (p-1)/k$. For prime v, the NRBs in Table 7.46 have this structure.

7.46 **Table** Some NRB$(v, k, k-1)$s. In each case, develop the blocks given over $\mathbb{Z}_v$ to obtain the v parallel classes. Adding the element 0 to each block prior to the development gives a $(v, k+1, k+1)$-design.

v, k	Base Near Parallel Classes
19,6	{1,7,8,11,12,18}, {2,3,5,14,16,17}, {4,6,9,10,13,15}
21,5	{1,2,3,5,10}, {4,8,11,15,16}, {6,12,14,17,20}, {7,9,13,18,19}
26,5	{1,4,8,18,22}, {2,9,11,19,24}, {3,6,16,17,23}, {5,7,10,21,25}, {12,13,14,15,20}
29,4	{1,12,17,28}, {2,5,24,27}, {4,10,19,25}, {8,9,20,21}, {11,13,16,18}, {3,7,22,26}, {6,14,15,23}
31,6	{1,5,6,25,26,30}, {3,13,15,16,18,28}, {8,9,14,17,22,23}, {4,7,11,20,24,27}, {2,10,12,19,21,29}
31,10	{1,2,4,8,15,16,23,27,29,30}, {3,6,7,12,14,17,19,24,25,28}, {5,9,10,11,13,18,20,21,22,26}
33,4	{1,8,18,19}, {2,3,24,31}, {4,13,21,23}, {5,11,17,20}, {6,10,26,29}, {7,12,15,16}, {9,22,28,30}, {14,25,27,32}
33,8	{1,11,12,15,20,22,26,28}, {2,5,9,14,17,18,19,29}, {3,4,16,21,23,24,27,31}, {6,7,8,10,13,25,30,32}
36,7	{1,13,18,24,28,32,34}, {2,12,14,25,30,31,33}, {3,6,9,10,15,23,35}, {4,5,8,16,17,19,26}, {7,11,20,21,22,27,29}
37,12	{1,6,8,10,11,14,23,26,27,29,31,36}, {2,9,12,15,16,17,20,21,22,25,28,35}, {3,4,5,7,13,18,19,24,30,32,33,34}
41,4	{1,9,32,40}, {6,13,28,35}, {4,5,36,37}, {11,17,24,30}, {16,20,21,25}, {3,14,27,38}, {2,18,23,39}, {12,15,26,29}, {8,10,31,33}, {7,19,22,34}
41,8	{1,3,9,14,27,32,38,40}, {2,6,13,18,23,28,35,39}, {4,5,12,15,26,29,36,37}, {8,10,11,17,24,30,31,33}, {7,16,19,20,21,22,25,34}
41,10	{1,4,10,16,18,23,25,31,37,40}, {6,14,15,17,19,22,24,26,27,35}, {2,5,8,9,20,21,32,33,36,39}, {3,7,11,12,13,28,29,30,34,38}

7.47 **Example** An NRB$(22, 7, 6)$ over $\mathbb{Z}_{21} \cup \{\infty\}$. Twenty-one near parallel classes are obtained by developing $\{\infty$,1,5,6,7,15,18$\}$, $\{2,3,4,8,10,13,17\}$, and $\{9,11,12,14,16,19,20\}$ mod 21. The last near parallel class consists of the three distinct translates of $\{0,3,6,9,12,15,18\}$.

7.48 Example An NRB$(28, 9, 8)$ over $\mathbb{Z}_{27} \cup \{\infty\}$. Twenty-seven near parallel classes are obtained by developing the blocks {∞,1,2,5,7,14,16,23,24}, {9,12,13,15,17,19,20,25,26} and {3,4,6,8,10,11,18,21,22} mod 27. The last near parallel class consists of the three distinct translates of {0,3,6,9,12,15,18,21,24}.

7.49 Example A RBIBD$(21, 7, 6)$ over $\mathbb{Z}_{20} \cup \{\infty\}$. Develop the following blocks by adding the even residues (mod 20): $B_1 = \{0, 4, 16, 11, 13, 17, 19\}$, $B_2 = \{\infty, 6, 14, 1, 3, 7, 9\}$, $B_3 = \{2, 8, 10, 12, 18, 5, 15\}$, $B_4 = \{0, 10, 1, 9, 11, 15, 19\}$, $B_5 = \{\infty, 2, 4, 16, 18, 3, 7\}$, $B_6 = \{6, 8, 12, 14, 5, 13, 17\}$. Both $\{B_1, B_2, B_3\}$ and $\{B_4, B_5, B_6\}$ form a parallel class.

7.50 Example A RBIBD$(288, 8, 1)$. The point set is $(\mathbb{Z}_7 \times \mathbb{Z}_{41}) \cup \{\infty\}$. Obtain the first parallel class as

$$\{(0, 9t), (0, 32t), (1, 3t), (1, 38t), (2, t), (2, 40t), (4, 14t), (4, 27t)\}$$

for $t = 1, 37, 16, 18, 10$, developing modulo $(7, -)$; then append the block

$$\{\infty, (0, 0), (1, 0), (2, 0), (3, 0), (4, 0), (5, 0), (6, 0)\}$$

to complete the first parallel class. Develop this parallel class modulo $(-, 41)$ to obtain the resolution.

7.51 Remark [24, 848] $(p, p-1)$-frames of type p^q are frequently used to construct NRB$(pq+1, p, p-1)$s. In particular, if p and q are odd prime powers, then such a frame is known to exist when

1. $p \equiv 3 \pmod 4$ and $q > p$, and
2. $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$, and $q > p$, except possibly when $q = p + 2$, $p \equiv 5, 9$, or $13 \pmod{16}$ and $p \geq 25$.

See Theorem IV.5.24. There are also known upper bounds on p for such a frame to exist when both p and $q \equiv 1 \pmod 4$. For $q \leq 433$, these bounds are tabulated in [24].

7.52 Examples

1. For $z = 3^i$, $0 \leq i \leq 4$, the blocks $\{(0, z), (1, 4z), (1, 7z), (4, 2z), (4, 9z)\}$ and $\{(0, 10z), (3, 2z), (3, 9z), (2, 4z), (2, 7z)\}$ generate a $(5, 4)$-frame of type 5^{11} over $\mathbb{F}_5 \times \mathbb{F}_{11}$.
2. For $z = 3^i$, $0 \leq i \leq 4$, the blocks $\{(0, z), (1, 2z), (1, 9z), (2, 4z), (2, 7z), (4, 3z), (4, 8z)\}$ and $\{(0, 10z), (6, 2z), (6, 9z), (5, 4z), (5, 7z), (3, 5z), (3, 6z)\}$ generate a $(7, 6)$-frame of type 7^{11} over $\mathbb{F}_7 \times \mathbb{F}_{11}$.
3. If x is any primitive element of $\mathbb{F}_9$, then for $z = x^{2i}$, $0 \leq i \leq 3$, the blocks $\{(0, z), (1, x^4z), (1, x^7x), (2, x^2z), (2, x^3z), (4, x^6z), (4, x^5z)\}$ and $\{(0, xz), (6, x^5z), (6, z), (5, x^3z), (5, x^4z), (3, x^7z), (3, x^6z)\}$ generate a $(7, 6)$-frame of type 7^9 over $\mathbb{F}_7 \times \mathbb{F}_9$.

7.7 Orthogonal Resolutions

7.53 Let $(V, \mathcal{B})$ be a design. Let $\mathcal{P} = \{P_1, \ldots, P_s\}$ and $\mathcal{Q} = \{Q_1, \ldots, Q_t\}$ be partitions of $\mathcal{B}$ into partial parallel classes. Partitions $\mathcal{P}$ and $\mathcal{Q}$ are *orthogonal* if $|P_i \cap Q_j| \leq 1$ for all $1 \leq i \leq s$ and $1 \leq j \leq t$.

7.54 Remark The situations most explored are when $\mathcal{P}$ and $\mathcal{Q}$ are both resolutions, or both near resolutions. When a design has two orthogonal resolutions, it is *doubly resolvable*; when it has two orthogonal near resolutions, it is *doubly near-resolvable*.

7.55 **Example** [585] A doubly near-resolvable BIBD(10,3,2). One near resolution is the rows, the second is the columns.

		3,4,8	1,6,7				2,5,9		
			4,0,9	2,7,8				3,6,5	
3,8,9				0,1,5					4,7,6
1,2,6	4,9,5				0,8,7				
	2,3,7	0,5,6				1,9,8			
		1,7,9					4,6,8		0,2,3
			2,8,5		1,3,4			0,7,9	
				3,9,6		2,4,0			1,8,5
4,5,7					2,9,6		3,0,1		
	0,6,8					3,5,7		4,1,2	

7.56 **Example** A doubly near-resolvable BIBD(16,3,2) over $\mathbb{Z}_{16}$. Develop (mod 16) the following base blocks, which form a near parallel class: $B_1 = \{8, 9, 12\}$, $B_2 = \{10, 13, 2\}$, $B_3 = \{1, 3, 7\}$, $B_4 = \{14, 15, 5\}$, $B_5 = \{4, 6, 11\}$. Near parallel classes in the second near resolution are translates of $B_1 + 6 = \{14, 15, 2\}$, $B_2 + 15 = \{9, 12, 1\}$, $B_3 + 4 = \{5, 7, 11\}$, $B_4 + 5 = \{3, 4, 10\}$, and $B_5 + 2 = \{6, 8, 13\}$.

7.57 **Theorems**

1. [45, 560] For any $v \equiv 3 \pmod 6$ there exists a doubly resolvable BIBD$(v, 3, 1)$, except for $v \in \{9, 15\}$ and possibly for $v \in \{21, 141, 153, 165, 177, 189, 231, 249, 261, 267, 285, 351, 357\}$.
2. [45, 1386] A doubly resolvable BIBD$(v, 3, 2)$ exists if and only if $v \equiv 0 \pmod 3$ and $v \notin \{6, 9\}$.
3. [45, 1385] A doubly near-resolvable BIBD$(v, 3, 2)$ exists if and only if $v \equiv 1 \pmod 3$ and $v \geq 10$.

7.58 **Remark** Asymptotic existence of doubly near-resolvable BIBD(v, k, λ)s and of doubly resolvable BIBD$(v, k, 1)$s is established in [1391]. One known infinite class consists of doubly resolvable BIBD$(p^n, p, 1)$s for p a prime power and n an integer ≥ 3 [843]. Another is given by Theorem 7.59.

7.59 **Theorem** [1383] A doubly resolvable BIBD$(k(k+1), k, k-1)$ exists if either k or $k+1$ is a prime power and $k \geq 3$.

7.8 α-Resolvable Designs

7.60 Let α be a positive integer. An *α-parallel class* or *α-resolution class* in a design is a set of blocks containing every point of the design exactly α times.

7.61 **Example** A 2-resolvable BIBD(10,4,6) over $\mathbb{Z}_9 \cup \{\infty\}$. Its blocks are obtained by developing (mod 9) the following base blocks that consist of a 2-parallel class.

$$\{0, 1, 2, 3\}, \quad \{0, 2, 5, 6\}, \quad \{1, 4, 5, 7\}, \quad \{3, 7, 8, \infty\}, \quad \{4, 6, 8, \infty\}$$

7.62 **Theorem** Necessary conditions for the existence of an α-resolvable BIBD(v, k, λ) are (1) $\lambda(v-1) \equiv 0 \pmod{(k-1)\alpha}$ and (2) $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$; (3) $\alpha v \equiv 0 \pmod k$.

7.63 **Theorem** [1233] The necessary conditions for existence of an α-resolvable BIBD$(v, 3, \lambda)$ are sufficient, except for $v = 6$, $\alpha = 1$ and $\lambda \equiv 2 \pmod 4$.

7.64 **Theorem** [2096] The necessary conditions for existence of an α-resolvable BIBD$(v, 4, \lambda)$ are sufficient, with the exception of $(\alpha, v, \lambda) = (2, 10, 2)$.

7.65 **Remark** An RBIBD(v, k, λ) is an α-resolvable BIBD(v, k, λ) with $\alpha = 1$. Several concepts and constructions for RBIBDs can be carried over to α-resolvable designs. For instance, a doubly α-resolvable BIBD is one with two α-resolutions, such that any α-parallel class in the first α-resolution has at most one block in common with each α-parallel class in the second α-resolution.

7.66 **Theorem** [45, 1389] A doubly 2-resolvable BIBD$(v, 3, 4)$ exists for all $v \equiv 0 \pmod 3$.

7.9 Uniformly Resolvable Designs

7.67 A parallel class in a pairwise balanced design is *uniform* if all blocks in the parallel class have the same size.

7.68 A *uniformly resolvable design*, URD(v, K, λ, R), is a resolvable PBD(v, K, λ) such that all of the parallel classes are uniform. R is a multiset, where $|R| = |K|$ and for each $k \in K$ there corresponds a positive $r_k \in R$ such that there are exactly r_k parallel classes of size k.

7.69 **Remark** While this definition requires that $r_k > 0$, one could allow $r_k = 0$. In this case there are no blocks of size k and the design is *k-free*; otherwise, it is *k-essential*.

7.70 **Remark** If $K = \{g, k\}$ and $R = \{r_g, r_k\}$ write k-URD(v, g, λ, r), where $r = r_g$ and, hence, $r_k = \frac{\lambda(v-1)-r(g-1)}{k-1}$.

7.71 **Example** A URD$(12, \{2, 3\}, 1, \{5, 3\})$ (also a 2-URD(12,3,1,3) or 3-URD(12,2,1,5)) over $\mathbb{Z}_3 \times \mathbb{Z}_4$. The parallel classes are shown.

$[\{(0,0),(0,1)\},\ \{(0,2),(0,3)\}] \bmod (3,-)$
$[\{(0,0),(0,2)\},\ \{(0,1),(0,3)\}] \bmod (3,-)$
$[\{(0,0),(0,3)\},\ \{(0,1),(0,2)\}] \bmod (3,-)$
$[\{(0,j),(1,j+2)\},\ \{(0,j+1),(1,j+3)\},$
$\{(0,j+2),(2,j+3)\},\ \{(0,j+3),(2,j)\},$
$\{(1,j),(2,j+1)\},\ \{(1,j+1),(2,j+2)\}]\ j = 0, 2$

$[\{(0,0),(1,0),(2,0)\}] \bmod (-,4)$
$[\{(0,0),(1,1),(2,3)\}] \bmod (-,4)$
$[\{(0,0),(1,3),(2,2)\}] \bmod (-,4)$

7.72 **Theorem** Necessary conditions for the existence of a URD(v, K, λ, R) are (1) $v \equiv 0 \pmod k$ for each $k \in K$ and (2) $\lambda(v-1) = \sum_{k \in K} r_k(k-1)$. In addition, if $\lambda = 1$ and $r_k > 1$, then $v \geq k^2$.

7.73 **Theorem** [1787] A 3-URD$(v, 2, 1, r)$ with $r \geq 1$ exists if and only if $v \equiv 0 \pmod 6$, $r \equiv 1 \pmod 2$, $1 \leq r \leq v - 3$ and $(v, r) \notin \{(6, 1), (12, 1)\}$. If $r = 1$, such a design is a *Nearly Kirkman Triple System*, denoted as NKTS(v).

7.74 **Theorem** [628] Suppose that $k = 2$, or that $k = 3$ and g is odd. Let $\epsilon_{k,g} = 1$ when $g \equiv 0 \pmod k$ and $\epsilon_{k,g} = k$ when $g \not\equiv 0 \pmod k$. Then

1. If n and $u \equiv 0 \pmod{k-1}$ and there exists a resolvable TD$(\epsilon_{k,g}g, u)$, then there exists a k-URD$(\epsilon_{k,g}gnu, g, \lambda, r)$ for all $1 \leq r \leq \lambda n$.
2. There is a k-URD$(\epsilon_{k,g}qg, g, \lambda, r)$ for all odd prime powers $q \geq g$ and all $1 \leq r \leq \frac{\lambda(q-1)}{k-1}$ except possibly when $k = 3$ and $q \equiv 5 \pmod 6$.

7.75 **Theorem** [627] A 4-URD$(v, 3, 1, \frac{v}{2} - 5)$ exists for all $v \equiv 12 \pmod{24}$, $v \neq 12$, except possibly when $v = 84$ or 156.

7.76 Theorem [627] Suppose that $t \equiv 3 \pmod 6$, $t \notin \{3, 21, 39\}$ and $v \equiv 4t \pmod{8t}$. Then

1. If $\frac{v}{4t}$ is a prime power congruent to 1 modulo 6, then a 4-URD$(v, 3, 1, \frac{v}{2} - 3s - 2)$ exists for all $s \leq \frac{(v-4t)}{8t}$.
2. If $\frac{v}{4t}$ is composite and there exists a resolvable TD$(t, \frac{v}{4tq})$, where q is the smallest proper factor of $\frac{v}{4t}$, then there exists a 4-URD$(v, 3, 1, \frac{v}{2} - 3s - 2)$ for all $s \leq \frac{v}{4tq}$.

7.77 Remark There is another large class of resolvable pairwise balanced designs, *class-uniformly resolvable designs* (CURDs), in which any two parallel classes have the same number of blocks of each size. For the existence of CURDs, see [1280] and references therein.

7.78 Proposition

1. If $K = \{k\}$ then a URD(v,K,λ,r_k) is equivalent to an RBIBD(v,k,λ), where $r_k = \frac{\lambda(v-1)}{k-1}$. An RBIBD$(v,k,\lambda)$ is also a CURD.
2. A k-URD$(v,g,1,1)$ is equivalent to a k-RGDD of type $g^{v/g}$. A 3-URD$(v,2,1,1)$ is equivalent to a Nearly Kirkman Triple System, NKTS(v). See §IV.5.
3. A k-URD$(kn, n, 1, 1)$ is equivalent to a resolvable TD(k,n). See §III.3.

See Also

§II.6	Some affine designs exist only as residual designs of symmetric designs. See Theorem 7.30.
§III.3	Resolvable TDs are a class of URDs.
§III.5	SOLSSOMs can be utilized in constructions of RBIBDs via Theorem 7.16.
§IV.2	Resolvable PBDs are the underlying block set of URDs.
§IV.4	Known results and techniques on resolvable GDDs and frames can be used in constructions of RBIBDs via Theorems 7.17 and 7.18.
§IV.5	Resolvable GDDs are a class of URDs.
§V.1	Hadamard designs are related via Theorem 7.11.
§VI.16	Block disjoint difference families and 1-rotational difference families are related to constructions of RBIBDs.
§VI.50	Room squares are equivalent to doubly RBIBD$(v, 2, 1)$s.
§VII.2	Affine geometries are the source of many RBIBDs.
[577]	A survey of orthogonal resolutions of triple systems and related cubical arrays.
[848]	Contains existence tables for RBIBDs with $10 \leq v \leq 200$, and an extensive bibliography.
[1420]	English translation of Lu's asymptotic existence results together with a more modern treatment.
[1782]	Contains first asymptotic proof covering all k. Deals with $\lambda = 1$.

References Cited: [7, 24, 34, 36, 40, 41, 43, 45, 144, 451, 560, 577, 585, 627, 628, 843, 847, 848, 961, 964, 965, 966, 968, 1233, 1246, 1280, 1383, 1385, 1386, 1389, 1391, 1419, 1420, 1600, 1631, 1782, 1787, 1967, 2096, 2193, 2213]

Part III

Latin Squares

1 Latin Squares

Charles J. Colbourn
Jeffrey H. Dinitz
Ian M. Wanless

1.1 Definitions and Examples

1.1 A *latin square* of *side* n (or *order* n) is an $n \times n$ array in which each cell contains a single symbol from an n-set S, such that each symbol occurs exactly once in each row and exactly once in each column.

1.2 A latin square of side n (on the symbol set $1, 2, \ldots, n$ or on the symbol set $0, 1, \ldots, n-1$) is *reduced* or in *standard form* if in the first row and column the symbols occur in natural order.

1.3 **Example** A reduced latin square of side 8 on the symbols $0, 1, \ldots, 7$.

0	1	2	3	4	5	6	7
1	0	3	4	5	6	7	2
2	3	5	0	6	7	4	1
3	4	0	7	1	2	5	6
4	5	6	1	7	0	2	3
5	6	7	2	0	3	1	4
6	7	4	5	2	1	3	0
7	2	1	6	3	4	0	5

1.4 Let L be an $n \times n$ latin square on symbol set E_3, with rows indexed by the elements of the n-set E_1 and columns indexed by the elements of the n-set E_2. Let $\mathcal{T} = \{(x_1, x_2, x_3) : L(x_1, x_2) = x_3\}$. Let $\{a, b, c\} = \{1, 2, 3\}$. The (a, b, c)-*conjugate* of L, $L_{(a,b,c)}$, has rows indexed by E_a, columns by E_b, and symbols by E_c, and is defined by $L_{(a,b,c)}(x_a, x_b) = x_c$ for each $(x_1, x_2, x_3) \in \mathcal{T}$.

1.5 **Example** A latin square of side 4 and its six conjugates.

1	4	2	3
2	3	1	4
4	1	3	2
3	2	4	1

(1,2,3)-conjugate

1	2	4	3
4	3	1	2
2	1	3	4
3	4	2	1

(2,1,3)-conjugate

1	3	2	4
2	4	1	3
4	2	3	1
3	1	4	2

(3,2,1)-conjugate

1	2	4	3
3	4	2	1
2	1	3	4
4	3	1	2

(2,3,1)-conjugate

1	3	4	2
3	1	2	4
2	4	3	1
4	2	1	3

(1,3,2)-conjugate

1	3	2	4
3	1	4	2
4	2	3	1
2	4	1	3

(3,1,2)-conjugate

1.6 **Remark** Any latin square has 1, 2, 3, or 6 distinct conjugates.

1.7 The *transpose* of a latin square L, denoted L^T, is the latin square that results from L when the role of rows and columns are exchanged (that is, $L^T(i, j) = L(j, i)$).

1.8 A latin square L of side n is *symmetric* if $L(i,j) = L(j,i)$ for all $1 \le i, j \le n$.

1.9 **Remark** A latin square L is symmetric if and only if $L = L^T = L_{(2,1,3)}$. The square in Example 1.3 is symmetric.

1.10 A latin square L of side n is *idempotent* if $L(i,i) = i$ for $1 \le i \le n$.

1.2 Equivalent Objects

1.11 **Theorem** A latin square of side n is equivalent to

1. the multiplication table (*Cayley table*) of a quasigroup on n elements (§III.2);
2. a transversal design of index one, $TD(3,n)$ (§III.3.2);
3. a $(3,n)$-net (§III.3.2);
4. an orthogonal array of strength two and index one, $OA(3,n)$ (§III.6);
5. a 1-factorization of the complete bipartite graph $K_{n,n}$ (§VII.5);
6. an edge-partition of the complete tripartite graph $K_{n,n,n}$ into triangles;
7. a set of n^2 mutually nonattacking rooks on an $n \times n \times n$ board;
8. a single error detecting code of word length 3, with n^2 words from an $n-$symbol alphabet ([684] p. 354).

1.3 Enumeration

1.12 Two latin squares L and L' of side n are *isotopic or equivalent* if there are three bijections from the rows, columns, and symbols of L to the rows, columns, and symbols, respectively, of L', that map L to L'.

1.13 Two latin squares L and L' of side n are *main class isotopic* or *paratopic* if L is isotopic to any conjugate of L'.

1.14 Two latin squares L and L' of side n are *isomorphic* if there is a bijection $\phi : S \to S$ such that $\phi L(i,j) = L'(\phi(i), \phi(j))$ for every $i, j \in S$, where S is not only the symbol set of each square, but also the indexing set for the rows and columns of each square.

1.15 The set of latin squares paratopic (isotopic or isomorphic) to L is the *main class* (*isotopy class* or *isomorphism class*, respectively) of L.

1.16 **Table** Enumeration of latin squares of side $n \le 10$ (see [1573] and Table 1.24).

$n \to$	1	2	3	4	5	6	7	8
main classes	1	1	1	2	2	12	147	283,657
isotopy classes	1	1	1	2	2	22	564	1,676,267
isomorphism classes	1	1	5	35	1,411	1,130,531	12,198,455,835	2,697,818,331,680,661
reduced squares	1	1	1	4	56	9,408	16,942,080	535,281,401,856
isomorphism classes of reduced squares	1	1	1	2	6	109	23,746	106,228,849

9	10
19,270,853,541	34,817,397,894,749,939
115,618,721,533	208,904,371,354,363,006
15,224,734,061,438,247,321,497	2,750,892,211,809,150,446,995,735,533,513
377,597,570,964,258,816	7,580,721,483,160,132,811,489,280
9,365,022,303,540	20,890,436,195,945,769,617

1.17 **Theorem** The number of reduced squares in an isotopy class of order n latin squares is $(n! \times n)/g$ where g is the order of the autotopy group (g is the number of isotopies that preserve the square). It follows that g divides $n! \times n$.

1.18 **Table** Main classes of latin squares of side n, $4 \leq n \leq 7$. For each, an identifying number is given, followed by five integers giving the number of transversals, the number of 2×2 subsquares, the number of 3×3 subsquares, the order of the autotopy group, and the number of conjugates that are isotopic to the given square, respectively.

$n = 4$

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

4.1: 8,12,0,96,6

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

4.2: 0,4,0,32,6

$n = 5$

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

5.1: 15,0,0,100,6

0	1	2	3	4
1	0	3	4	2
2	3	4	0	1
3	4	1	2	0
4	2	0	1	3

5.2: 3,4,0,12,6

$n = 6$

0	1	2	3	4	5
1	0	3	2	5	4
2	3	4	5	0	1
3	2	5	4	1	0
4	5	0	1	2	3
5	4	1	0	3	2

6.1: 0,9,4,72,6

0	1	2	3	4	5
1	0	3	2	5	4
2	3	4	5	0	1
3	2	5	4	1	0
4	5	0	1	3	2
5	4	1	0	2	3

6.2:32,9,0,24,6

0	1	2	3	4	5
1	0	3	2	5	4
2	3	0	5	1	4
3	4	5	0	2	1
4	5	1	2	0	3
5	2	4	1	3	0

6.3:24,15,0,120,2

0	1	2	3	4	5
1	0	3	4	5	2
2	3	0	5	1	4
3	4	5	0	2	1
4	5	1	2	3	0
5	2	4	1	0	3

6.4: 8,7,0,8,2

0	1	2	3	4	5
1	0	3	4	5	2
2	3	1	5	0	4
3	4	5	1	2	0
4	5	0	2	3	1
5	2	4	0	1	3

6.5: 8,5,0,4,2

0	1	2	3	4	5
1	0	3	4	5	2
2	3	4	5	0	1
3	4	5	2	1	0
4	5	0	1	2	3
5	2	1	0	3	4

6.6: 0,9,4,36,2

0	1	2	3	4	5
1	0	3	2	5	4
2	4	0	5	1	3
3	5	1	4	0	2
4	2	5	0	3	1
5	3	4	1	2	0

6.7: 0,27,4,216,6

0	1	2	3	4	5
1	0	3	2	5	4
2	4	0	5	1	3
3	5	1	4	0	2
4	2	5	1	3	0
5	3	4	0	2	1

6.8: 0,19,0,8,6

0	1	2	3	4	5
1	0	3	2	5	4
2	4	0	5	1	3
3	5	1	4	2	0
4	3	5	1	0	2
5	2	4	0	3	1

6.9: 0,15,0,12,2

0	1	2	3	4	5
1	0	3	2	5	4
2	4	0	5	3	1
3	5	4	0	1	2
4	2	5	1	0	3
5	3	1	4	2	0

6.10: 8,11,0,4,6

0	1	2	3	4	5
1	0	3	4	5	2
2	3	1	5	0	4
3	5	4	1	2	0
4	2	5	0	1	3
5	4	0	2	3	1

6.11: 8,4,0,4,6

0	1	2	3	4	5
1	2	0	4	5	3
2	0	1	5	3	4
3	5	4	1	0	2
4	3	5	2	1	0
5	4	3	0	2	1

6.12: 0,0,4,108,6

$n = 7$

0	1	2	3	4	5	6
1	2	0	4	3	6	5
2	0	1	5	6	3	4
3	4	5	6	0	1	2
4	3	6	0	5	2	1
5	6	3	1	2	4	0
6	5	4	2	1	0	3

7.1: 3,18,1,12,6

0	1	2	3	4	5	6
1	2	0	4	3	6	5
2	0	1	5	6	3	4
3	4	5	6	0	2	1
4	3	6	0	5	1	2
5	6	3	2	1	4	0
6	5	4	1	2	0	3

7.2: 23,26,3,8,2

0	1	2	3	4	5	6
1	2	0	4	3	6	5
2	0	1	5	6	3	4
3	4	5	6	1	2	0
4	3	6	1	5	0	2
5	6	3	2	0	4	1
6	5	4	0	2	1	3

7.3: 63,42,7,168,6

0	1	2	3	4	5	6
1	2	0	4	3	6	5
2	0	1	5	6	3	4
3	4	5	6	0	1	2
4	3	6	0	5	2	1
5	6	3	1	2	4	0
6	5	4	2	1	0	3

7.4: 23,14,1,2,2

0	1	2	3	4	5	6
1	2	0	4	5	6	3
2	0	3	5	6	1	4
3	4	5	6	2	0	1
4	5	6	2	1	3	0
5	6	1	0	3	4	2
6	3	4	1	0	2	5

7.5: 19,6,0,3,2

0	1	2	3	4	5	6
1	2	3	0	5	6	4
2	3	4	5	6	0	1
3	0	5	6	1	4	2
4	5	6	1	3	2	0
5	6	0	4	2	1	3
6	4	1	2	0	3	5

7.6: 25,0,0,6,2

0	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

7.7: 133,0,0,294,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	1	2
4	2	6	5	1	0	3
5	6	1	4	3	2	0
6	5	4	0	2	3	1

7.8: 21,18,1,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	1	2
4	2	6	5	1	3	0
5	6	4	0	3	2	1
6	5	1	4	2	0	3

7.9: 30,16,1,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	2	1
4	2	6	5	1	3	0
5	6	1	4	3	0	2
6	5	4	0	2	1	3

7.10: 43,30,3,4,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	2	1
4	2	6	5	1	3	0
5	6	4	0	2	1	3
6	5	1	4	3	0	2

7.11: 43,18,3,4,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	2	1
4	2	6	5	1	3	0
5	6	4	0	3	1	2
6	5	1	4	2	0	3

7.12: 55,22,3,8,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	2	1
4	5	6	0	1	3	2
5	6	1	4	2	0	3
6	2	4	5	3	1	0

7.13: 13,18,1,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	2	1
4	5	6	0	2	1	3
5	6	1	4	3	0	2
6	2	4	5	1	3	0

7.14: 33,22,1,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	1	6	4	5
3	4	5	6	0	2	1
4	5	6	0	3	1	2
5	6	1	4	2	0	3
6	2	4	5	1	3	0

7.15: 15,22,1,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	5	6	0	1	2	3
5	6	4	1	2	3	0
6	4	1	5	3	0	2

7.16: 30,8,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	5	6	0	1	2	3
5	6	4	1	3	0	2
6	4	1	5	2	3	0

7.17: 14,15,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	5	6	0	1	3	2
5	6	4	1	3	2	0
6	4	1	5	2	0	3

7.18: 20,12,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	5	6	1	2	3	0
5	6	4	0	1	2	3
6	4	1	5	3	0	2

7.19: 22,11,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	5	6	1	3	0	2
5	6	4	0	1	2	3
6	4	1	5	2	3	0

7.20: 15,14,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	5	6	0	1	3	2
5	6	4	1	3	2	0
6	4	1	5	2	0	3

7.21: 24,11,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	6	1	5	2	3	0
5	4	6	0	1	2	3
6	5	4	1	3	0	2

7.22: 18,11,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	6	1	5	3	0	2
5	4	6	1	2	3	0
6	5	4	0	1	2	3

7.23: 22,13,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	0	4	1
4	5	6	1	0	2	3
5	6	4	0	2	3	1
6	4	1	5	3	0	2

7.24: 19,14,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	2	5	6	1	4	0
4	5	6	1	0	2	3
5	6	4	0	2	3	1
6	4	1	5	3	0	2

7.25: 33,18,0,3,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	2	6	5	1	0	3
5	6	1	0	3	4	2
6	5	4	1	2	3	0

7.26: 11,16,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	2	6	5	1	0	3
5	6	4	1	2	3	0
6	5	1	0	3	4	2

7.27: 13,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	5	6	0	1	3	2
5	6	4	1	2	0	3
6	2	1	5	3	4	0

7.28: 16,16,0,1,3

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	5	6	1	2	0	3
5	6	1	0	3	4	2
6	2	4	5	1	3	0

7.29: 21,16,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	5	6	1	2	0	3
5	6	4	0	1	3	2
6	2	1	5	3	4	0

7.30: 32,14,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	5	6	1	2	3	0
5	6	1	0	3	4	2
6	2	4	5	1	0	3

7.31: 15,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	6	1	5	2	0	3
5	2	6	1	3	4	0
6	5	4	0	1	3	2

7.32: 24,14,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	6	1	5	2	3	0
5	2	6	0	1	4	3
6	5	4	1	3	0	2

7.33: 15,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	0	2	1
4	2	6	5	1	0	3
5	6	4	1	3	2	0
6	5	1	0	2	4	3

7.34: 19,16,1,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	0	2
4	5	6	0	2	3	1
5	6	4	1	3	2	0
6	2	1	5	0	4	3

7.35: 24,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	0	2
4	5	6	0	3	2	1
5	6	4	1	2	3	0
6	2	1	5	0	4	3

7.36: 29,14,1,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	0	2
4	5	6	0	3	2	1
5	6	4	1	2	3	0
6	2	1	5	0	4	3

7.37: 14,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	0	2
4	5	6	1	0	2	3
5	6	4	0	2	3	1
6	2	1	5	3	4	0

7.38: 13,16,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	0	2
4	2	6	5	0	3	1
5	6	4	1	3	2	0
6	5	1	0	2	4	3

7.39: 9,8,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	0	2
4	5	6	1	3	2	0
5	6	4	0	2	3	1
6	2	1	5	0	4	3

7.40: 15,14,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	2	0
4	6	1	5	3	0	2
5	2	6	1	0	4	3
6	5	4	0	2	3	1

7.41: 20,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	1	2	0
4	6	1	5	3	0	2
5	2	6	1	0	4	3
6	5	4	0	2	3	1

7.42: 18,20,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	2	0	1
4	5	6	0	1	2	3
5	6	4	1	0	3	2
6	2	1	5	3	4	0

7.43: 16,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	2	0	1
4	5	6	1	0	2	3
5	6	4	0	1	3	2
6	2	1	5	3	4	0

7.44: 19,14,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	2	0	1
4	5	6	1	0	2	3
5	6	1	0	3	4	2
6	2	4	5	1	3	0

7.45: 22,18,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	2	0	1
4	6	1	5	0	3	2
5	2	6	1	3	4	0
6	5	4	0	1	3	2

7.46: 19,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	2	0	1
4	6	1	5	0	3	2
5	2	6	0	1	4	3
6	5	4	1	3	2	0

7.47: 14,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	2	0	1
4	6	1	5	0	3	2
5	2	6	1	3	4	0
6	5	4	0	1	2	3

7.48: 15,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	5	6	2	0	1
4	6	1	5	3	2	0
5	2	6	0	1	4	3
6	5	4	1	0	3	2

7.49: 23,10,0,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	0	2	1
4	2	5	6	1	0	3
5	6	4	1	2	3	0
6	5	1	0	3	4	2

7.50: 19,12,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	0	2	1
4	2	5	6	1	3	0
5	6	1	0	2	4	3
6	5	4	1	3	0	2

7.51: 15,10,1,4,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	0	2	1
4	2	5	6	1	3	0
5	6	4	1	2	0	3
6	5	1	0	3	4	2

7.52: 27,18,1,4,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	0	2	1
4	5	1	6	2	0	3
5	6	4	0	1	3	2
6	2	5	1	3	4	0

7.53: 34,18,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	0	2	1
4	5	1	6	3	0	2
5	6	4	1	2	3	0
6	2	5	0	1	4	3

7.54: 20,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	0	2	1
4	6	5	1	2	3	0
5	2	4	6	1	0	3
6	5	1	0	3	4	2

7.55: 25,12,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	1	0	2
4	5	1	6	2	3	0
5	6	4	0	3	2	1
6	2	5	1	0	4	3

7.56: 28,12,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	1	0	2
4	6	5	1	2	3	0
5	2	1	6	0	4	3
6	5	4	0	3	2	1

7.57: 21,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	2	0	1
4	5	1	6	0	3	2
5	6	4	0	1	2	3
6	2	5	1	3	4	0

7.58: 25,16,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	2	0	1
4	5	1	6	0	3	2
5	6	4	1	3	2	0
6	2	5	0	1	4	3

7.59: 21,10,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	2	0	1
4	5	1	6	3	2	0
5	6	4	0	1	3	2
6	2	5	1	0	4	3

7.60: 28,14,1,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	2	0	1
4	6	5	0	1	2	3
5	2	1	6	3	4	0
6	5	4	1	0	3	2

7.61: 26,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	2	0	1
4	6	5	0	1	3	2
5	2	1	6	0	4	3
6	5	4	1	3	2	0

7.62: 19,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	2	0	1
4	6	5	1	0	2	3
5	2	1	6	3	4	0
6	5	4	0	1	3	2

7.63: 24,14,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	4	6	5	2	0	1
4	6	5	1	0	2	3
5	2	4	6	1	3	0
6	5	1	0	3	4	2

7.64: 19,10,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	5	4	6	2	0	1
4	6	1	5	0	2	3
5	2	6	1	3	4	0
6	4	5	0	1	3	2

7.65: 17,14,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	5	4	6	2	0	1
4	6	1	5	0	3	2
5	4	6	0	1	2	3
6	2	5	1	3	4	0

7.66: 25,18,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	5	4	6	2	0	1
4	6	1	5	0	3	2
5	4	6	1	3	2	0
6	2	5	0	1	4	3

7.67: 16,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	5	4	6	2	0	1
4	6	1	5	3	2	0
5	2	6	0	1	4	3
6	4	5	1	0	3	2

7.68: 41,14,0,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	5	4	6	2	0	1
4	6	5	1	0	3	2
5	2	6	0	1	4	3
6	4	1	5	3	2	0

7.69: 27,14,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	5	4	6	2	0	1
4	6	5	1	0	3	2
5	2	6	0	1	4	3
6	4	1	5	3	2	0

7.70: 24,14,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	0	4	6	1	5
3	6	4	5	2	0	1
4	5	1	6	3	2	0
5	2	6	1	0	4	3
6	4	5	0	1	3	2

7.71: 33,18,0,3,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	0	6	4	5
3	4	5	6	0	1	2
4	2	6	5	3	0	1
5	6	4	1	2	3	0
6	5	0	4	1	2	3

7.72: 47,10,1,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	0	6	4	5
3	4	5	6	0	1	2
4	5	6	1	2	3	0
5	6	0	4	1	2	3
6	2	4	5	3	0	1

7.73: 24,9,1,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	0	6	4	5
3	4	5	6	0	1	2
4	6	0	5	3	2	1
5	2	6	4	1	3	0
6	5	4	1	2	0	3

7.74: 37,18,1,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	0	6	4	5
3	4	5	6	0	1	2
4	6	0	5	3	2	1
5	2	6	4	1	3	0
6	5	4	1	2	0	3

7.75: 24,15,1,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	0	6	4	5
3	4	6	5	0	2	1
4	2	5	6	1	3	0
5	6	0	4	2	1	3
6	5	4	1	3	0	2

7.76: 31,6,3,24,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	0	6	4	5
3	2	5	6	0	4	1
4	5	6	0	1	2	3
5	6	4	1	2	3	0
6	4	0	5	3	1	2

7.77: 21,10,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	0	4	1
4	5	6	0	1	3	2
5	6	4	1	3	2	0
6	4	0	5	2	1	3

7.78: 23,14,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	0	4	1
4	5	6	0	1	3	2
5	6	4	1	3	2	0
6	4	0	5	2	1	3

7.79: 23,10,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	0	4	1
4	5	6	1	2	3	0
5	6	4	0	3	1	2
6	4	0	5	1	2	3

7.80: 20,10,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	0	4	1
4	5	6	1	3	2	0
5	6	4	0	1	3	2
6	4	0	5	2	1	3

7.81: 25,10,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	0	4	1
4	5	6	1	3	2	0
5	6	4	0	2	1	3
6	4	0	5	1	3	2

7.82: 19,8,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	0	4	1
4	6	0	5	1	3	2
5	4	6	0	2	1	3
6	5	4	1	3	2	0

7.83: 19,8,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	0	4	1
4	6	0	5	1	3	2
5	4	6	1	3	2	0
6	5	4	0	2	1	3

7.84: 22,14,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	2	5	6	1	4	0
4	5	6	1	0	2	3
5	6	4	0	3	1	2
6	4	0	5	2	3	1

7.85: 12,11,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	4	1	2	3	0
6	2	0	5	3	4	1

7.86: 19,8,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	5	6	0	2	3	1
5	6	4	1	3	2	0
6	2	0	5	1	4	3

7.87: 19,8,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	5	6	0	3	2	1
5	6	0	1	2	4	3
6	2	4	5	1	3	0

7.88: 18,7,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	5	6	1	2	3	0
5	6	4	0	1	2	3
6	2	0	5	3	4	1

7.89: 17,7,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	5	6	1	3	2	0
5	6	4	0	2	3	1
6	2	0	5	1	4	3

7.90: 23,6,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	6	0	5	1	2	3
5	2	6	0	3	4	1
6	5	4	1	2	3	0

7.91: 22,12,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	6	0	5	1	2	3
5	2	6	1	3	4	0
6	5	4	0	2	3	1

7.92: 22,6,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	1	2
4	6	0	5	2	3	1
5	2	6	1	3	4	0
6	5	4	0	1	2	3

7.93: 14,9,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	2	1
4	6	0	5	2	1	3
5	2	6	1	3	4	0
6	5	4	0	1	3	2

7.94: 22,9,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	5	6	0	2	1
4	5	6	0	1	2	3
5	6	0	1	3	4	2
6	2	4	5	0	3	1

7.95: 12,10,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	2	1	0
4	6	0	5	1	3	2
5	2	6	1	0	4	3
6	5	4	0	3	2	1

7.96: 13,5,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	1	2
4	2	5	6	1	3	0
5	6	0	1	2	4	3
6	5	4	0	3	2	1

7.97: 7,6,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	1	2
4	5	0	6	2	3	1
5	6	4	0	1	2	3
6	2	5	1	3	4	0

7.98: 21,9,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	1	2
4	5	0	6	2	3	1
5	6	4	1	3	2	0
6	2	5	0	1	4	3

7.99: 25,10,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	2	1
4	5	0	6	1	3	2
5	6	4	0	2	1	3
6	2	5	1	3	4	0

7.100: 16,8,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	2	1
4	5	0	6	2	3	1
5	6	4	0	1	3	2
6	2	5	1	3	4	0

7.101: 25,12,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	2	1
4	5	0	6	3	1	2
5	6	4	1	2	3	0
6	2	5	0	1	4	3

7.102: 26,11,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	2	1
4	5	0	6	1	3	2
5	6	4	0	3	2	1
6	2	5	1	0	4	3

7.103: 22,7,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	2	1	0
4	5	0	6	1	3	2
5	6	4	0	3	2	1
6	2	5	1	0	4	3

7.104: 21,10,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	2	1	0
4	6	5	1	0	3	2
5	2	0	6	1	4	3
6	5	4	0	3	2	1

7.105: 30,10,0,2,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	4	6	5	0	2	1
4	5	0	6	2	1	3
5	6	4	0	1	3	2
6	2	5	1	3	4	0

7.106: 26,9,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	5	0	6	1	4	2
4	6	5	1	0	2	3
5	4	6	0	2	3	1
6	2	4	5	3	1	0

7.107: 16,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	5	0	6	1	4	2
4	6	5	1	2	3	0
5	4	6	0	3	2	1
6	2	4	5	0	1	3

7.108: 14,8,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	5	0	6	2	4	1
4	6	5	1	3	2	0
5	4	6	0	1	3	2
6	2	4	5	0	1	3

7.109: 25,16,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	1	4	6	0	5
3	5	4	6	0	1	2
4	6	0	5	1	2	3
5	4	6	0	2	3	1
6	2	5	1	3	4	0

7.110: 25,10,0,1,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	2	5	6	1	4	0
4	6	0	1	2	3	5
5	4	6	0	3	1	2
6	5	1	4	0	2	3

7.111: 14,8,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	2	5	6	1	4	0
4	6	1	0	2	3	5
5	4	6	1	0	2	3
6	5	0	4	3	1	2

7.112: 18,9,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	1	2	5
4	5	6	0	3	1	2
5	6	1	4	2	3	0
6	2	5	1	0	4	3

7.113: 28,9,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	1	2	5
4	5	6	1	2	3	0
5	6	1	0	3	4	2
6	2	5	4	0	1	3

7.114: 19,8,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	1	2	5
4	6	5	0	3	1	2
5	2	6	1	0	4	3
6	5	1	4	2	3	0

7.115: 19,10,0,1,6

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	2	1	5
4	6	5	1	2	3	0
5	2	6	4	0	1	3
6	5	1	0	3	4	2

7.116: 23,6,0,2,2

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	2	1	5
4	5	6	0	1	3	2
5	6	1	4	3	2	0
6	2	5	1	0	4	3

7.117: 21,10,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	2	1	5
4	5	6	1	3	2	0
5	6	1	4	0	3	2
6	2	5	0	1	4	3

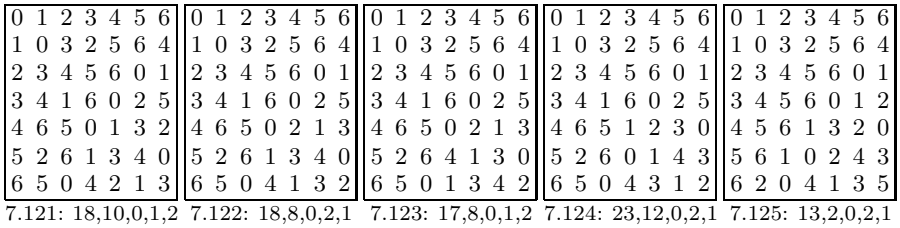
7.118: 17,5,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	2	1	5
4	6	5	0	1	3	2
5	2	6	1	0	4	3
6	5	1	4	3	2	0

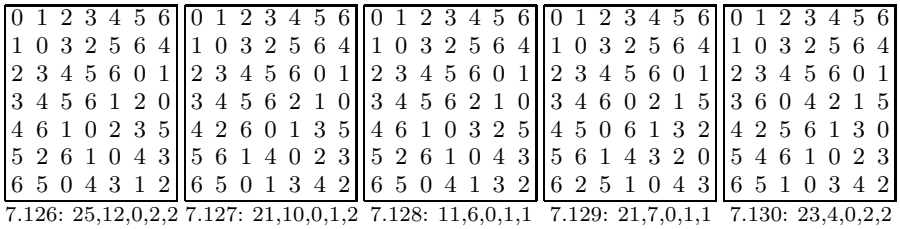
7.119: 17,7,0,1,1

0	1	2	3	4	5	6
1	0	3	2	5	6	4
2	3	4	5	6	0	1
3	4	0	6	2	1	5
4	6	5	0	1	3	2
5	2	6	1	3	4	0
6	5	1	4	0	2	3

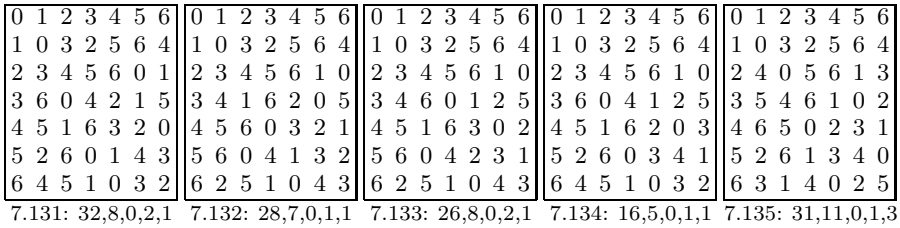
7.120: 21,5,0,1,1



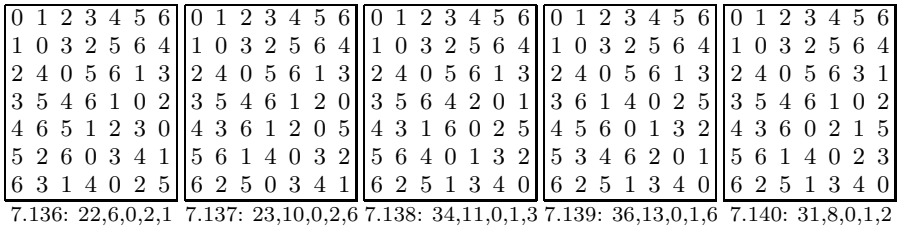
7.121: 18,10,0,1,2 7.122: 18,8,0,2,1 7.123: 17,8,0,1,2 7.124: 23,12,0,2,1 7.125: 13,2,0,2,1



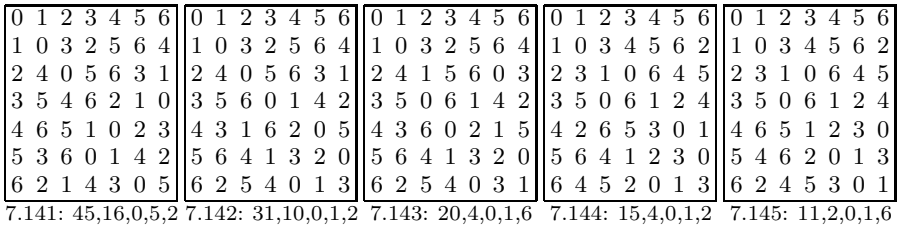
7.126: 25,12,0,2,2 7.127: 21,10,0,1,2 7.128: 11,6,0,1,1 7.129: 21,7,0,1,1 7.130: 23,4,0,2,2



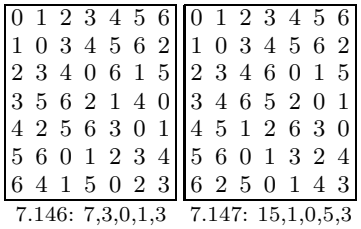
7.131: 32,8,0,2,1 7.132: 28,7,0,1,1 7.133: 26,8,0,2,1 7.134: 16,5,0,1,1 7.135: 31,11,0,1,3



7.136: 22,6,0,2,1 7.137: 23,10,0,2,6 7.138: 34,11,0,1,3 7.139: 36,13,0,1,6 7.140: 31,8,0,1,2



7.141: 45,16,0,5,2 7.142: 31,10,0,1,2 7.143: 20,4,0,1,6 7.144: 15,4,0,1,2 7.145: 11,2,0,1,6



7.146: 7,3,0,1,3 7.147: 15,1,0,5,3

1.19 Theorem ([2091]) Let $L(n)$ denote the number of distinct latin squares of side n. Then $(n!)^{2n}n^{-n^2} \le L(n) \le \prod_{k=1}^{n}(k!)^{n/k}$. Asymptotically $L(n)^{1/n^2} \sim n/e^2$ as $n \to \infty$.

1.20 A $k \times n$ *latin rectangle* is a $k \times n$ array (where $k \le n$) in which each cell contains a single symbol from an n-set S, such that each symbol occurs exactly once in each row and at most once in each column.

1.21 A latin rectangle is *normalized* (or *reduced*) if the first row and first column read $[1, 2, \ldots n]$ and $[1, 2, \ldots, k]$, respectively. $L(k, n)$ denotes the number of normalized $k \times n$ latin rectangles.

1.22 **Remark** The total number of $k \times n$ latin rectangles is $n!\,(n-1)!\,L(k,n)/(n-k)!$.

1.23 **Theorem** ([937], p. 507) The number of $3 \times n$ latin rectangles is $(n!)^2$ times the coefficient of x^n in the power series

$$e^{2x} \sum_{i=0}^{\infty} i! \frac{x^i}{(1+x)^{3i+3}}.$$

1.24 **Table** [1579] $L(k, n)$ for $1 \le k \le n \le 11$.

n	k	$L(k,n)$
1	1	1
2	1	1
	2	1
3	1	1
	2	1
	3	1
4	1	1
	2	3
	3	4
	4	4
5	1	1
	2	11
	3	46
	4	56
	5	56
6	1	1
	2	53
	3	1064
	4	6552
	5	9408
	6	9408
7	1	1
	2	309
	3	35792
	4	1293216
	5	11270400
	6	16942080
	7	16942080
8	1	1
	2	2119
	3	1673792
	4	4209 09504
	5	27206 658048
	6	33 53901 89568
	7	53 52814 01856
	8	53 52814 01856

n	k	$L(k,n)$
9	1	1
	2	16687
	3	1034 43808
	4	20 76245 60256
	5	11268 16430 83776
	6	12 95260 54043 81184
	7	224 38296 79166 91456
	8	377 59757 09642 58816
	9	377 59757 09642 58816
10	1	1
	2	1 48329
	3	81549 99232
	4	14717 45210 59584
	5	746 98838 30762 86464
	6	8 70735 40559 10037 09440
	7	1771 44296 98305 41859 22560
	8	42920 39421 59185 42730 03520
	9	75807 21483 16013 28114 89280
	10	75807 21483 16013 28114 89280
11	1	1
	2	14 68457
	3	79 80304 83328
	4	143 96888 00784 66048
	5	75 33492 32304 79020 93312
	6	9 62995 52373 29250 51587 78880
	7	24012 32164 75173 51550 21735 52640
	8	86 10820 43577 87266 78085 83437 51680
	9	2905 99031 00338 82693 11398 90275 94240
	10	5363 93777 32773 71298 11967 35407 71840
	11	5363 93777 32773 71298 11967 35407 71840

1.25 Table [1575] Estimates of $L(n,n)$ for $12 \le n \le 15$.

n	12	13	14	15
$L(n,n)$	1.62×10^{44}	2.51×10^{56}	2.33×10^{70}	1.5×10^{86}

1.26 Theorem [915] The number of $k \times n$ latin rectangles is asymptotically

$$(n!)^k \left(\frac{n(n-1)\cdots(n-k+1)}{n^k} \right)^n \left(1 - \frac{k}{n}\right)^{-n/2} e^{-k/2}$$

as $n \to \infty$ with $k = o(n^{6/7})$.

1.4 Transversals

1.27 A *transversal* in a latin square of side n is a set of n cells, one from each row and column, containing each of the n symbols exactly once. A *partial transversal of length k* in a latin square of side n is a set of k cells, each from a different row and each from a different column and such that no two contain the same symbol.

1.28 Remark Some latin squares have no transversals at all. One such class of latin squares consists of the addition tables of $\mathbb{Z}_{2n}$ for $n \ge 1$. In fact, any latin square that is the addition table of a group with a unique element of order 2 has no transversals.

1.29 Remark See §VI.6 for some connections between complete mappings of groups (and quasigroups) and transversals in latin squares.

1.30 Remark If a latin square L has a transversal, then any latin square isotopic to L also has a transversal. Indeed, the number of transversals is a main class invariant.

1.31 Theorem [146] Every latin square of even order has an even number of transversals.

1.32 Conjecture (Ryser) Every latin square of odd order has a transversal.

1.33 Theorem (Shor; see [838] and [685, pages 9–10]) Every latin square of side n has a partial transversal of length k where $k \ge max\{n - \sqrt{n}, n - 5.518(\log n)^2\}$.

1.34 Theorem [1572] If $T(n)$ is the maximum number of transversals achieved by a latin square of order n, then $15^{n/5} \le T(n) \le 0.6135^n\, n!\, \sqrt{n}$ for $n \ge 5$.

1.35 Remark In order for a latin square of side n to have an orthogonal mate (see §III.3) it must possess a set of n disjoint transversals.

1.36 Example The square on the right is a latin square of side 10 with 5,504 different transversals [1716]. This square has 12,265,168 distinct orthogonal mates [1506], but it has been proven not to be one of a set of three mutually orthogonal latin squares of side 10.

5	1	7	3	4	0	6	2	8	9
1	2	3	4	5	6	7	8	9	0
7	3	4	5	6	2	8	9	0	1
3	4	5	6	7	8	9	0	1	2
4	5	6	7	8	9	0	1	2	3
0	6	2	8	9	5	1	7	3	4
6	7	8	9	0	1	2	3	4	5
2	8	9	0	1	7	3	4	5	6
8	9	0	1	2	3	4	5	6	7
9	0	1	2	3	4	5	6	7	8

1.37 A *k-transversal* or *k-plex* in a latin square of side n is a set of nk cells, k from each row, k from each column, in which every symbol occurs exactly k times.

1.38 Remark If a latin square possesses k disjoint transversals, then it possesses a k-transversal. The converse is false. For any $k \ge 2$, there exists a k-transversal that contains no c-transversal for $1 \le c < k$. See [2120] for a survey.

1.39 Conjecture (Rodney) Every latin square has a 2-transversal.

1.5 Subsquares and Holes

1.40 If in a latin square L of side n the k^2 cells defined by k rows and k columns form a latin square of side k, it is a latin *subsquare of* L. The subsquare is *proper* if $1 < k < n$.

1.41 **Remark** If two subsquares intersect, their intersection is itself a subsquare.

1.42 **Theorem** A latin square of side n with a proper subsquare of side k exists if and only if $k \leq \lfloor \frac{n}{2} \rfloor$.

1.43 **Theorem** (see [1079]) There exists a latin square of side n that contains latin subsquares of every side k, $k \leq \lfloor \frac{n}{2} \rfloor$, if and only if $1 \leq n \leq 7$ or $n = 9$, 11 or 13.

1.44 **Example** This square of order 11 has subsquares of each possible order. In fact, it has 172 subsquares of order 2, 15 subsquares of order 3, 9 subsquares of order 4, and 3 subsquares of order 5. Two subsquares of order 5 are marked (one in a box, the other with asterisks). Their intersection (in **bold**) is a subsquare of order 2.

1	4	5	3	2	9	a	b	6	7	8
5	2	4	1	3	a	b	9	8	6	7
4	5	3	2	1	b	9	a	7	8	6
2	3	1	**4***	**5***	7	8	6	b^*	9^*	a^*
3	1	2	**5***	**4***	8	6	7	a^*	b^*	9^*
9	a	b	8	7	6	4	5	1	2	3
a	b	9	6	8	5	7	4	3	1	2
b	9	a	7	6	4	5	8	2	3	1
6	8	7	a^*	b^*	1	3	2	9^*	5^*	4^*
7	6	8	b^*	9^*	2	1	3	4^*	a^*	5^*
8	7	6	9^*	a^*	3	2	1	5^*	4^*	b^*

1.45 An *incomplete latin square* $\mathrm{ILS}(n; b_1, b_2, \ldots, b_k)$ is an $n \times n$ array A with entries from an n-set B, together with $B_i \subseteq B$ for $1 \leq i \leq k$ where $|B_i| = b_i$ and $B_i \cap B_j = \emptyset$ for $1 \leq i, j \leq k$. Moreover,

1. each cell of A is empty or contains an element of B;
2. the subarrays indexed by $B_i \times B_i$ are empty (these subarrays are *holes*); and
3. the elements in row or column b are exactly those of $B \setminus B_i$ if $b \in B_i$, and of B otherwise.

A *partitioned incomplete latin square* $\mathrm{PILS}(n; b_1, b_2, \ldots, b_k)$ is an incomplete latin square with $b_1 + b_2 + \cdots + b_k = n$. A $\mathrm{PILS}(n; b_1, b_2, \ldots, b_k)$ is of *type* $(b_1, b_2, \ldots, b_k)$.

1.46 **Example** A $\mathrm{PILS}(7; 1, 1, 1, 2, 2)$.

	4	5	6	7	2	3
3		6	7	1	5	4
2	7		1	6	4	5
7	6	2			3	1
6	3	7			1	2
4	5	1	2	3		
5	1	4	3	2		

1.47 **Remark** Given an $\mathrm{ILS}(n; b_1, b_2, \ldots, b_k)$ it is always possible to "fill in" the hole of size b_i, $1 \leq i \leq k$, with a latin square of side b_i (on the symbols B_i) to obtain a latin square of side n. The existence of a latin square of side n containing a latin subsquare of side k is equivalent to an $\mathrm{ILS}(n; k)$.

1.48 **Theorem** A $\mathrm{PILS}(n; b_1, b_2, b_3)$ exists if and only if $b_1 = b_2 = b_3$. Moreover, a $\mathrm{PILS}(n; b_1, b_2, b_3, b_4)$ exists if and only if the b_i (perhaps after relabeling) satisfy $b_1 = b_2 = b_3$ and $1 \leq b_4 \leq 2b_1$.

1.49 A subsquare of side 2 of a latin square is an *intercalate*. A square with no intercalates is an N_2 *square*. A square with no proper subsquares is an N_∞ *square*.

1.50 **Theorem** Fix $\epsilon > 0$. With probability approaching 1 as $n \to \infty$, a randomly chosen latin square of side n has at least $n^{3/2-\epsilon}$ intercalates.

1.51 **Theorem** There exists an N_2 square of side n if and only if $n \notin \{2, 4\}$.

1.52 **Remark** If n is odd, then the Cayley table of any group of order n has no intercalates. Also, if A and B are N_2 squares, then so is their product.

1.53 **Remark** An algorithm for finding N_2 latin squares is described in Example VII.6.83.

1.54 **Theorem** (see [1079, 1507, 2118]) There exists an N_∞ square of side n if $n \neq 2^a 3^b$, $n < 256$, or n is odd.

1.55 **Example** Latin squares of order 8 and 12 with no proper subsquares.

1	2	3	4	5	6	7	8
2	3	1	5	6	7	8	4
3	1	4	6	7	8	2	5
4	6	8	2	1	3	5	7
5	8	2	7	3	4	6	1
6	5	7	1	8	2	4	3
7	4	5	8	2	1	3	6
8	7	6	3	4	5	1	2

1	2	3	4	5	6	7	8	9	a	b	c
2	3	4	5	6	1	8	9	a	b	c	7
3	1	5	2	7	8	4	a	6	c	9	b
4	5	6	7	1	9	b	c	8	3	2	a
5	6	2	8	a	7	9	b	c	4	1	3
6	c	8	1	3	a	2	7	b	9	4	5
7	8	1	a	c	b	5	4	2	6	3	9
8	9	b	3	4	c	a	6	5	1	7	2
9	b	7	c	2	5	1	3	4	8	a	6
a	7	c	b	9	4	6	1	3	2	5	8
b	4	a	9	8	3	c	2	7	5	6	1
c	a	9	6	b	2	3	5	1	7	8	4

1.56 **Remarks** If p is a prime, then the Cayley table of the cyclic group of order p is an N_∞ square (see Example 1.67). Also, if there exists a perfect 1-factorization of K_{n+1} (§VII.5), then there exists an N_∞ square of side n.

1.6 Hamiltonian and Atomic Latin Squares

1.57 In a latin square L, a *row cycle of length* m is a $2 \times m$ latin rectangle that is a submatrix of L and that contains no $2 \times k$ latin rectangle for $k < m$. A *column cycle* (*symbol cycle*) is a set of entries that become a row cycle in the transpose ((3,1,2)-conjugate, respectively) of L. L is *row-hamiltonian* (*column-hamiltonian* or *symbol-hamiltonian*) if all of its row (column or symbol, respectively) cycles have length equal to the order of L. The term *hamiltonian latin square (HLS)* applies to latin squares that are row-, column-, or symbol-hamiltonian.

1.58 **Example** In this square of order 5, a row cycle of length 3 is marked with *, a column cycle of length 3 is marked with $^\diamond$, and a symbol cycle of length 3 is marked by $^\bullet$. These cycles show that this square is **not** an HLS.

$1^\diamond$	$2^\bullet$	$3^\bullet$	4	$5^\diamond$
2	1^*	4^*	5^*	3
3	4^*	5^*	1^*	2
$4^\diamond$	5	$2^\bullet$	$3^\bullet$	$1^\diamond$
$5^\diamond$	$3^\bullet$	1	$2^\bullet$	$4^\diamond$

1.59 **Example** Square 7.6 in Table 1.18 is symbol-hamiltonian but not row- or column-hamiltonian.

1.60 **Remark** For an HLS of order n to exist, it is necessary that $n = 2$ or n is odd. This is conjectured to be sufficient.

1.61 **Table** [2119] Number of main classes of HLS of order $n \leq 9$.

n	2	3	5	7	9
Main classes of HLS	1	1	1	2	37

1.62 **Theorem** There exists an HLS of order n if $n \leq 50$ and n is odd, or if $n \in \{p, 2p-1, p^2\}$ where p is any odd prime.

1.63 **Remark** If a latin square is row-hamiltonian, then so is its $(1, 3, 2)$-conjugate.

1.64 **Remark** An HLS of order n is equivalent to a perfect 1-factorization of $K_{n,n}$. Perfect 1-factorizations of K_{n+1} can be used to build symmetric symbol-hamiltonian latin squares of order n and *vice versa*, but the relationship is not 1:1. See [2122] for details.

1.65 **Theorem** An HLS has no proper subsquares.

1.66 A latin square is *atomic* if it is row-, column-, and symbol-hamiltonian.

1.67 **Example** Squares 5.1 and 7.7 in Table 1.18 are atomic. Indeed, the Cayley table of any cyclic group of prime order is atomic. A non group-based atomic square of order 11 is given in Example 1.117.

1.68 **Table** [1506, 2121] Number of main classes of atomic latin squares for $n \leq 27$.

n	2	3	5	7	9	11	13	15	17	19	21	23	25	27
Main classes	1	1	1	1	0	7	≥ 8	≥ 0	≥ 2	≥ 10	≥ 0	≥ 5	≥ 1	≥ 2

1.69 **Remark** Atomic squares are known to exist for the composite orders 25, 27, 49, 121, 125, 289, 361, 625, 841, 1369, 1849, 2809, 4489, 24649, and 39601.

1.70 **Remark** For each prime $p \geq 11$ for which 2 is a primitive root, five main classes of atomic square are known. For each prime $p \geq 11$ for which 2 is not a primitive root, two main classes of atomic square are known.

1.7 Completion and Embedding

1.71 An n by n array L with cells that are either empty or contain exactly one symbol is a *partial* latin square if no symbol occurs more than once in any row or column. A partial latin square is *symmetric* (or *commutative*) if when cell (i, j) is occupied by x, then so is cell (j, i), for every $1 \leq i, j \leq n$. A partial latin square is *idempotent* if all of the cells on the main diagonal are occupied and furthermore cell (i, i) is occupied by i. The *size* of a partial latin square is its number of filled cells.

1.72 **Theorem** [1928] A partial latin square of order n and size at most $n - 1$ can always be completed to a latin square of order n.

1.73 **Remark** Evans [803] posed Theorem 1.72 as a question that became widely known as the *Evans Conjecture*. It remained unsolved for 21 years. A symmetric analogue is given in Theorem 1.75.

1.74 **Theorem** [522] Deciding whether a partial latin square can be completed is an NP-complete problem, even if there are no more than 3 unfilled cells in any row or column.

1.75 **Theorem** [85] Every partial symmetric latin square of order n with admissible diagonal and size at most $n - 1$ can be completed to a symmetric latin square of order n.

1.76 **Remark** In Theorem 1.75, the diagonal is *admissible* if and only if the number of symbols occurring on the diagonal a number of times that is different from n modulo 2 is at most the number of empty diagonal cells. This is necessary, because the parity must be changed for every such symbol. Theorem 1.75 addresses the sufficiency.

1.77 **Theorem** A $k \times n$ latin rectangle, $k < n$, can always be completed to a latin square of order n.

1.78 **Theorem** (Ryser) Let L be a partial latin square of order n in which cell (i, j) is filled if and only if $i \le r$ and $j \le s$. Then L can be completed to a latin square of order n if and only if $N(i) \ge r + s - n$ for $i = 1, 2, \ldots, n$, where $N(i)$ denotes the number of elements in L that are equal to i.

1.79 An $n \times n$ partial latin square P is *embedded* in a latin square L if the upper $n \times n$ left corner of L agrees with P.

1.80 **Example** The 4×4 partial latin square P is embedded in the 5×5 latin square L.

$$P = \begin{array}{|cccc|}\hline 1 & 4 & \cdot & \cdot \\ \cdot & \cdot & 3 & 4 \\ \cdot & 1 & 2 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \hline \end{array} \qquad L = \begin{array}{|ccccc|}\hline 1 & 4 & 5 & 2 & 3 \\ 2 & 5 & 3 & 4 & 1 \\ 3 & 1 & 2 & 5 & 4 \\ 5 & 3 & 4 & 1 & 2 \\ 4 & 2 & 1 & 3 & 5 \\ \hline \end{array}$$

1.81 **Theorem** [803] A partial $n \times n$ latin square can be embedded in a $t \times t$ latin square for every $t \ge 2n$.

1.82 **Remark** Theorem 1.81 is the best possible general embedding result, as it is possible to construct for every $n \ge 4$ a partial $n \times n$ latin square that cannot be embedded in a latin square less than twice its size. See §III.2 for related results on embedding partial latin squares.

1.83 **Theorem** [2120] If $1 < k < n$ and $k > \frac{1}{4}n$, then there is a partial latin square P of order n that cannot be completed to a latin square of order n, where P has k filled cells in each row and column and k cells containing each symbol.

1.8 Critical Sets

1.84 A partial latin square P of order n is a *critical set* if it is completable to exactly one latin square of order n, but removal of any of the filled cells from P destroys the uniqueness of completion.

1.85 **Remark** A critical set in a latin square L is a minimal defining set for L in the sense of §VI.13. Every defining set contains a critical set. However, a partial latin square with more than one completion need not be contained in a critical set.

1.86 The smallest and largest sizes of critical sets of order n are denoted $\mathrm{scs}(n)$ and $\mathrm{lcs}(n)$ respectively.

1.87 **Table** Smallest and largest critical sets for order $n \le 10$. (See [174] for scs(8) and references for smaller values.)

n	2	3	4	5	6	7	8	9	10
$\mathrm{scs}(n)$	1	2	4	6	9	12	16	$\le$20	$\le$25
$\mathrm{lcs}(n)$	1	3	7	11	18	$\ge$25	$\ge$37	$\ge$44	$\ge$57

1.88 **Example** Critical sets of order 6 and size $\mathrm{scs}(6) = 9$ and $\mathrm{lcs}(6) = 18$.

$$\begin{array}{|cccccc|}\hline 1 & 2 & 3 & \cdot & \cdot & \cdot \\ 2 & 3 & \cdot & \cdot & \cdot & \cdot \\ 3 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 4 \\ \cdot & \cdot & \cdot & \cdot & 4 & 5 \\ \hline \end{array} \qquad \begin{array}{|cccccc|}\hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & 5 \\ \cdot & 1 & 2 & 5 & \cdot & 4 \\ \cdot & \cdot & \cdot & 1 & 2 & 3 \\ \cdot & \cdot & 4 & 3 & 1 & 2 \\ \cdot & 4 & 5 & 2 & 3 & 1 \\ \hline \end{array}$$

1.89 **Theorem** [441] $\frac{1}{3}n(\log n)^{1/3} \le \mathrm{scs}(n) \le \lfloor n^2/4 \rfloor$.

1.90 **Conjecture** $\mathrm{scs}(n) = \lfloor n^2/4 \rfloor$ for all n.

1.91 **Theorem** [895, 1132] $n^2 - O(n^{5/3}) \le \mathrm{lcs}(n) \le n^2 - \frac{7}{2}n + o(n)$.

1.92 A partial latin square T_1 is a *latin trade* if there exists a partial latin square T_2 with the properties that (1) a cell is filled in T_1 if and only if it is filled in T_2, (2) no symbol occurs in the same cell in T_1 and T_2, and (3) in any given row or column T_1 and T_2 contain exactly the same symbols.

1.93 **Remark** Intercalates are the smallest latin trades. The cycles defined in §1.6 are latin trades.

1.94 **Theorem** Let C be a critical set in a latin square L. Then C intersects every latin trade in L. Moreover, for each entry e in C there exists a trade in L that includes e but no other entry of C.

1.95 **Table** Numbers of main, transpose, and isotopy classes of distinct latin trades of size $n \le 18$ (two trades are in the same transpose class if they are related by isotopy and/or transposition).

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Main	0	0	1	0	1	1	5	4	19	26	163	445	2302	10795	63624	381626	2547990
Transpose	0	0	1	0	2	1	9	7	40	63	401	1202	6503	31505	187643	1137602	7617639
Isotopy	0	0	1	0	3	1	13	10	66	112	723	2283	12616	62163	372147	2268021	15209245

1.96 **Theorem** [440, 752] In the addition table for integers modulo a prime p, the size of the smallest latin trade is at least $e \log p + 2$ but not more than $O(\log^2 p)$.

1.97 **Remark** See [1275] for further results on critical sets including connections with the cycle double cover conjecture and topological embeddings of graphs.

1.9 Sudoku Latin Squares

1.98 Let a, b, and n be positive integers with $a \times b = n$. Partition an $n \times n$ array in the natural way into $a \times b$ *regions*. An (a, b)-*Sudoku latin square* is a latin square on the symbol set $\{1, 2, \ldots n\}$ where each region contains all of the symbols. A *Sudoku latin square* is a $(3, 3)$-*Sudoku latin square*.

1.99 With a, b, and n as above, an (a, b)-*Sudoku critical set* is a partial latin square P that is completable in exactly one way to an (a, b)-Sudoku latin square, but removal of any of the filled cells from P destroys the uniqueness of completion.

1.100 **Example** A Sudoku critical set (of size 17) and its unique completion to a Sudoku latin square.

· · ·	· · ·	· 1 ·
4 · ·	· · ·	· · ·
· 2 ·	· · ·	· · ·
· · ·	· 5 ·	4 · 7
· · 8	· · ·	3 · ·
· · 1	· 9 ·	· · ·
3 · ·	4 · ·	2 · ·
· 5 ·	1 · ·	· · ·
· · ·	8 · 6	· · ·

6 9 3	7 8 4	5 1 2
4 8 7	5 1 2	9 3 6
1 2 5	9 6 3	8 7 4
9 3 2	6 5 1	4 8 7
5 6 8	2 4 7	3 9 1
7 4 1	3 9 8	6 2 5
3 1 9	4 7 5	2 6 8
8 5 6	1 2 9	7 4 3
2 7 4	8 3 6	1 5 9

1.101 A *Sudoku game* consists of completing an (a, b)-Sudoku critical set to an (a, b)-Sudoku latin square. By far the most popular version has $a = b = 3$.

1.102 Remark Sudoku critical sets are known for all sizes from 17 to 35. No Sudoku critical set of size 16 is currently known. Example 1.100 is of size 17.

1.103 Proposition The number of distinct (n, n)-Sudoku latin squares for $n = 1, 2$, and 3 is 1, 288, and 6,670,903,752,021,072,936,960, respectively. The number of inequivalent (n, n)-Sudoku latin squares for $n = 1, 2$, and 3 is 1, 2, and 5,472,730,538, respectively. For $n = 3$ the allowed equivalences are relabeling entries; reflection; rotation; permutation of blocks of rows or columns 1–3, 4–6 and 7–9; permutation of rows or columns 1–3; permutation of rows or columns 4–6; and permutation of rows or columns 7–9.

1.104 Remark The game Sudoku was first popularized in Japan in 1986 and attained international popularity in 2005. Puzzles now appear daily in hundreds of newspapers and on the world wide web. See `http://en.wikipedia.org/wiki/Sudoku` for information on the history, strategy, and variants of Sudoku.

1.10 Diagonal Latin Squares

1.105 Let L be a latin square of side n. Then the *jth right diagonal* of L is the set of n cells of L, $\{(i, j + i) : i = 0, 1, \ldots, n - 1 \pmod n\}$. The *$j$th left diagonal* of L is the set of n cells of L, $\{(i, j - i) : i = 0, 1, \ldots, n - 1 \pmod n\}$.

1.106 A latin square L of side n is a *diagonal latin square* if both its 0th right and $(n-1)$st left diagonals are transversals.

1.107 Theorem [892] A diagonal latin square of side n exists if and only if $n > 3$.

1.108 Example Diagonal latin squares of sides 4, 5, 6, and 8. A diagonal latin square of side 7 can be found in Example VI.6.32.

0	2	3	1
1	3	2	0
2	0	1	3
3	1	0	2

1	3	4	0	2
3	2	0	1	4
0	4	3	2	1
2	0	1	4	3
4	1	2	3	0

1	2	3	4	5	0
0	5	4	3	2	1
2	4	0	1	3	5
3	1	5	2	0	4
5	3	1	0	4	2
4	0	2	5	1	3

0	2	4	6	7	1	3	5
1	7	5	3	2	0	6	4
2	4	6	0	1	3	5	7
3	1	7	5	4	2	0	6
4	6	0	2	3	5	7	1
5	3	1	7	6	4	2	0
6	0	2	4	5	7	1	3
7	5	3	1	0	6	4	2

1.109 Remark A discussion of orthogonal diagonal latin squares can be found in §III.3.8.

1.110 A latin square L of side n is a *Knut Vik design* if every right and left diagonal of L is a transversal.

1.111 Theorem [1070] A Knut Vik design of side n exists if and only if n is not divisible by either 2 or 3.

1.112 Remark The connection between Knut Vik designs and complete mappings is given in Theorem VI.6.31. A Knut Vik design of side 7 is given in Example VI.6.32.

1.113 A latin square L of even order n is a *crisscross latin square* if all the jth right diagonals for even j and all the jth left diagonals for odd j are transversals.

1.114 Theorem [1156] Crisscross latin squares of side n exist if and only if $n \equiv 0 \pmod 4$.

1.115 Example The squares of sides 4 and 8 in Example 1.108 are crisscross latin squares.

1.11 Diagonally Cyclic Latin Squares

1.116 A *standard* DCLS (*diagonally cyclic latin square*) uses $\mathbb{Z}_n$ for its symbol set and on each right diagonal has the symbols occurring in the cyclic order $0, 1, 2, \ldots, n-1$. A DCLS is any square isotopic to a standard DCLS.

1.117 Example On the right is a standard DCLS of order 11 (it is self-orthogonal and atomic, but not isotopic to the addition table of $\mathbb{Z}_{11}$).

1	8	6	0	7	3	5	2	10	9	4
5	2	9	7	1	8	4	6	3	0	10
0	6	3	10	8	2	9	5	7	4	1
2	1	7	4	0	9	3	10	6	8	5
6	3	2	8	5	1	10	4	0	7	9
10	7	4	3	9	6	2	0	5	1	8
9	0	8	5	4	10	7	3	1	6	2
3	10	1	9	6	5	0	8	4	2	7
8	4	0	2	10	7	6	1	9	5	3
4	9	5	1	3	0	8	7	2	10	6
7	5	10	6	2	4	1	9	8	3	0

1.118 Theorem A DCLS of order n exists if and only if n is odd.

1.119 Remark A standard DCLS L is completely determined by any single row (or column). The possible r-th rows are exactly those for which the permutation $i \to L(r, i)$ is an orthomorphism of $\mathbb{Z}_n$. (See §VI.6.)

1.120 Conjecture There exists a subsquare-free DCLS for all odd orders. (This conjecture is proved if the order $n < 10000$ or 3 divides n [1507].)

1.121 Remark For a standard DCLS L of order n, label the rows and columns with indices $0, 1, \ldots, n-1$ in that order. Then L has an automorphism applying the cyclic permutation $(0\ 1\ 2\ \cdots n-1)$ to the rows, columns, and symbols.

1.122 A *standard* f-DCLS uses $\mathbb{Z}_n \cup \{\infty_1, \ldots, \infty_f\}$ for its symbol set and to index its rows and columns. It has an automorphism applying the cyclic permutation $(0\ 1 \cdots n-1)$ to the rows, columns and symbols. An f-DCLS is any latin square isotopic to a standard f-DCLS.

1.123 Theorem For $f \geq 1$ there exists an f-DCLS of order n if and only if $n \geq 2f$.

1.124 Remark A standard f-DCLS has a subsquare of order f at the intersection of the rows and columns with indices in $\{\infty_1, \ldots, \infty_f\}$.

1.125 Remark Squares in the f-DCLS family are versatile and easy to construct. There are many examples of DCLS and 1-DCLS among the SOLS in §III.5.

1.126 Example Standard 1-DCLS and 2-DCLS of order 8, with structure emphasized.

∞_1	3	6	2	5	1	4	0
5	∞_1	4	0	3	6	2	1
3	6	∞_1	5	1	4	0	2
1	4	0	∞_1	6	2	5	3
6	2	5	1	∞_1	0	3	4
4	0	3	6	2	∞_1	1	5
2	5	1	4	0	3	∞_1	6
0	1	2	3	4	5	6	∞_1

∞_2	3	5	4	2	∞_1	1	0
∞_1	∞_2	4	0	5	3	2	1
4	∞_1	∞_2	5	1	0	3	2
1	5	∞_1	∞_2	0	2	4	3
3	2	0	∞_1	∞_2	1	5	4
2	4	3	1	∞_1	∞_2	0	5
5	0	1	2	3	4	∞_2	∞_1
0	1	2	3	4	5	∞_1	∞_2

1.12 Even and Odd Latin Squares

1.127 A *row inversion* in a latin square $L = (a_{i,j})$ is a pair of numbers in a row that are out of order ($a_{i,j} > a_{i,k}$) with $j < k$. A latin square is *row even* (*row odd*) if it contains an even (odd, respectively) number of row inversions. The concepts of *column inversion, column even*, and *column odd* are defined similarly. A latin square is *even* (*odd*) if the sum of the number of row inversions and the number of column inversions is even (odd, respectively).

1.128 RELS(n), ROLS(n), CELS(n), COLS(n), ELS(n), and OLS(n) denote the numbers of row even, row odd, column even, column odd, even, and odd latin squares of side n.

1.129 Remark When n is an odd integer, by permuting a pair of rows or a pair of columns, $\mathrm{RELS}(n) = \mathrm{ROLS}(n)$, $\mathrm{CELS}(n) = \mathrm{COLS}(n)$, and $\mathrm{ELS}(n) = \mathrm{OLS}(n)$.

1.130 Theorem [1144, 1189] Let n be an even integer. Then $\mathrm{RELS}(n) \neq \mathrm{ROLS}(n)$ if and only if $\mathrm{ELS}(n) \neq \mathrm{OLS}(n)$.

1.131 Table [1189] The number of even and odd reduced latin squares of side $2n$ for $1 \leq n \leq 4$.

$2n =$	2	4	6	8
even	1	4	5856	270746124288
odd	0	0	3552	264535277568

1.132 Conjecture (Alon–Tarsi, 1986) If n is even, then $\mathrm{ELS}(n) \neq \mathrm{OLS}(n)$.

1.133 Remark A motivation for the study of even and odd latin squares came from the *Dinitz conjecture*: For each positive integer n and for any collection of n-element sets $S_{i,j}$, an $n \times n$ partial latin square can be found with the (i, j) entry taken from $S_{i,j}$. Alon and Tarsi [80] prove that if $\mathrm{ELS}(n) \neq \mathrm{OLS}(n)$ for all even integers n, then the Dinitz conjecture holds for all even n. Galvin [855] proved the Dinitz conjecture using different methods. Also, the Alon–Tarsi conjecture has been proven for $n = p+1$ with p a prime by Drisko [754].

1.13 Conflict-Free Latin Squares

1.134 Remarks In assigning array elements to memory devices in parallel computation, it is important that array elements that are to be retrieved at the same time be stored in different memory units, permitting parallel access. The attempt to retrieve two array elements from the same device simultaneously is a *memory conflict*. When storing an $n \times n$ array A, one forms an $n \times n$ array S, the *skewing scheme*; the (i, j) entry of S indicates in which memory unit the (i, j) entry of A is to be stored.

1.135 A *template* is a set of ordered pairs of the form $(\rho + i, \gamma + j)$, where ρ and γ are formal parameters and i and j are integers. An *instance* of the template is obtained by choosing integer values for ρ and γ.

1.136 If T is a template with parameters ρ and γ, and S is an $n \times n$ skewing scheme, then S is *conflict-free for* T if for every instance I of T, and any distinct pairs (a, b) and (c, d) in I that index elements of S, the (c, d) entry of S differs from the (a, b) entry of S.

1.137 Remarks Rows and columns form important classes of templates. Conflict-free for rows is precisely row latinicity, and for columns it is column latinicity. Thus, a skewing

scheme that is conflict-free for rows and columns is a partial latin square. In the application, the number of memory units is limited, and hence one prefers skewing schemes with a minimum number of symbols. When the number of symbols is n and the skewing scheme is conflict-free for rows and columns, the scheme is a latin square. Diagonal latin squares arise when one requires diagonals to be conflict-free. The most extensively studied cases are for rectangular templates; see [553, 788].

See Also

§III.3	Mutually orthogonal latin squares.
§III.4	Gives the connection with incomplete transversal designs.
§III.2	The multiplication tables of quasigroups are latin squares.
§III.5	Self-orthogonal latin squares.
§VI.22	Frequency squares are squares with the latin property with more than one symbol in each entry.
§VI.62	Tuscan squares (and their relatives such as row complete latin squares) are squares where each row is a permutation and distance properties are studied.
[684]	An old but comprehensive reference for latin squares.
[685]	A newer reference for latin squares than [684].
[1271]	Contains all main classes of latin squares up to side 8 in electronic form.
[1413]	An excellent introduction to latin squares and applications.

References Cited: [80, 85, 146, 174, 440, 441, 522, 553, 684, 685, 752, 754, 788, 803, 838, 855, 892, 895, 915, 937, 1070, 1079, 1132, 1144, 1156, 1189, 1271, 1275, 1413, 1506, 1507, 1572, 1573, 1575, 1579, 1716, 1928, 2091, 2118, 2119, 2120, 2121, 2122]

2 Quasigroups

Frank E. Bennett
Charles C. Lindner

2.1 Definitions and Examples

2.1 A *quasigroup* is an ordered pair $(Q, \oplus)$, where Q is a set and $\oplus$ is a binary operation on Q such that the equations $a \oplus x = b$ and $y \oplus a = b$ are uniquely solvable for every pair of elements a, b in Q. For Q finite, the *order* of the quasigroup $(Q, \oplus)$ is $| Q |$.

2.2 **Example** A quasigroup and its associated latin square.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	1	0
3	3	2	0	1

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

2.3 **Remark** The multiplication table of a quasigroup defines a *latin square*; that is, a latin square can be viewed as the multiplication table of a quasigroup with the headline and sideline removed.

2.4 A quasigroup $(Q, \cdot)$ is *idempotent* if the identity $x \cdot x = x$ (briefly $x^2 = x$) holds for all x in Q.

2.5 If $(Q, \otimes)$ is a quasigroup, one may define on the set Q six binary operations $\otimes_{(1,2,3)}$, $\otimes_{(1,3,2)}$, $\otimes_{(2,1,3)}$, $\otimes_{(2,3,1)}$, $\otimes_{(3,1,2)}$, and $\otimes_{(3,2,1)}$ as follows: $a \otimes b = c$ if and only if:

$$a \otimes_{(1,2,3)} b = c, \qquad a \otimes_{(1,3,2)} c = b, \qquad b \otimes_{(2,1,3)} a = c,$$
$$b \otimes_{(2,3,1)} c = a, \qquad c \otimes_{(3,1,2)} a = b, \qquad c \otimes_{(3,2,1)} b = a.$$

These six (not necessarily distinct) quasigroups $(Q, \otimes_{(i,j,k)})$, where $\{i, j, k\} = \{1, 2, 3\}$, are the *conjugates* of $(Q, \otimes)$.

2.6 **Example** Examples of six conjugate quasigroups are given in §III.1.

2.7 Two quasigroups $(Q, \cdot)$ and $(Q, *)$ defined on the same set Q are *orthogonal* if the equations $x \cdot y = z \cdot t$ and $x * y = z * t$ together imply $x = z$ and $y = t$.

2.8 **Remark** When two quasigroups $(Q, \cdot)$ and $(Q, *)$ are orthogonal, their corresponding latin squares are also orthogonal in the usual sense.

2.9 A quasigroup (latin square) is *self-orthogonal* if it is orthogonal to its $(2, 1, 3)$-conjugate, its *transpose*. More generally, a quasigroup that is orthogonal to its (i, j, k)-conjugate is *(i, j, k)-conjugate orthogonal*.

2.10 Adopting the functional notation $a(x, y)$ in place of the infix notation $x * y$ for the operation, two binary operations $a(x, y)$ and $b(x, y)$ defined on the same set Q are *orthogonal operations*, written $a \perp b$, if $|\{(x, y)\colon\ a(x, y) = i,\ b(x, y) = j\}| = 1$ for every ordered pair i, j in Q.

2.11 The *spectrum* of the two-variable quasigroup identity $u(x, y) = v(x, y)$ is the set of all integers n such that there exists a quasigroup of order n satisfying the identity $u(x, y) = v(x, y)$.

2.12 **Remark** Two-variable quasigroup identities are often instrumental in the construction or algebraic description of combinatorial designs. For example, an *idempotent totally symmetric quasigroup* $(Q, \cdot)$, or *Steiner quasigroup*, satisfying the identities $\{x^2 = x, x(xy) = y, (xy)y = x\}$, corresponds to a *Steiner triple system* (STS), where $\{x, y, z\}$ is a triple if and only if $x \cdot y = z$ when x, y, z are distinct, and $x^2 = x$ for all $x \in Q$. Similarly, an *idempotent semisymmetric quasigroup* $(Q, \cdot)$, one that satisfies the identities $\{x^2 = x, x(yx) = y\}$, corresponds to a *Mendelsohn triple system* (MTS). Here (x, y, z) is a cyclically ordered triple if and only if $x \cdot y = z$ when x, y, z are distinct, and $x^2 = x$ for all $x \in Q$.

2.13 **Remark** A Hall triple system (see §VI.28) is a Steiner triple system whose related Steiner quasigroup is distributive, in the sense that the following identity holds: $a \circ (x \circ y) = (a \circ x) \circ (a \circ y)$.

2.14 **Remark** The most direct method of constructing finite models of a quasigroup $(Q, \cdot)$ satisfying the two-variable identity $u(x, y) = v(x, y)$ is to look for a model of the identity of the form $x \cdot y = \lambda x + \mu y$, where the elements lie in some finite field. In particular, idempotent models of the identity are of the form $x \cdot y = \lambda x + (1 - \lambda)y$ in $\mathbb{F}_q$, where q is a prime power and $\lambda \neq 0$ or 1. This requires finding a solution to some polynomial equation $f(\lambda) = 0$ in $\mathbb{F}_q$ depending on the identity to be satisfied. More general information on varieties of quasigroups and their related structures can be found in [191, 208, 804, 1455] and in their extensive bibliographies.

2.15 **Example** Let $Q = \mathbb{Z}_7$ and define the operation $x * y = 3x + 5y \pmod 7$ for all x, y in Q. This operation produces an idempotent semisymmetric quasigroup $(Q, *)$ of order 7, which is self-orthogonal. This quasigroup corresponds to a self-orthogonal MTS of

order 7 (SOMTS(7)), generated by developing the two base blocks $(0, 1, 5)$ and $(0, 3, 1)$ (mod 7). This MTS(7) is separable into a pair of orthogonal STS(7). The quasigroup $(Q, *)$ is readily checked to be both $(1, 3, 2)$- and $(3, 2, 1)$-conjugate orthogonal.

2.16 **Example** Let the set Q be based on the elements of $\mathbb{F}_4$ and take λ to be a primitive element in $\mathbb{F}_4$. Then the operation $x \cdot y = \lambda x + (1 - \lambda)y$ in $\mathbb{F}_4$ defines an idempotent semisymmetric quasigroup $(Q, \cdot)$, which is self-orthogonal and corresponds to a SOMTS(4). The quasigroup $(Q, \cdot)$ is $(1, 3, 2)$- and $(3, 2, 1)$-conjugate orthogonal.

2.17 **Example** Consider the quasigroup identity $((yx)y)y = x$. Idempotent models of this identity are of the form $x \cdot y = \lambda x + (1 - \lambda)y$ in $\mathbb{F}_q$, where q is a prime power and $\lambda \neq 0$ or 1 and where the polynomial equation $f(\lambda) = \lambda^3 - \lambda^2 + 1 = 0$ is satisfied in $\mathbb{F}_q$. Idempotent models of $((yx)y)y = x$ for orders $q = 5, 7, 8$ are readily obtained. A quasigroup satisfying the identity $((yx)y)y = x$ is $(2, 3, 1)$-, $(3, 1, 2)$-, and $(3, 2, 1)$-conjugate orthogonal.

2.18 **Example** A quasigroup satisfying the identity $(xy)y = x(xy)$ is necessarily idempotent. Models of this identity of the form $x \cdot y = \lambda x + (1 - \lambda)y$ in $\mathbb{F}_q$ exist for all orders $q = 2^k$ where $k \geq 2$. A quasigroup satisfying the given identity is $(1, 3, 2)$- and $(3, 2, 1)$-conjugate orthogonal.

2.19 A *partial quasigroup of order n* is a pair $(Q, \circ)$, where Q is a finite set of size n and $\circ$ is a binary partial operation on Q such that the equations $a \circ x = b$ and $y \circ a = b$ have at most one solution for all $a, b \in Q$.

2.20 The partial quasigroup $(P, \circ_1)$ is *embedded* in the quasigroup $(Q, \circ_2)$ provided (1) $P \subseteq Q$ and (2) $\circ_2$ agrees with $\circ_1$ on P.

2.21 **Example** The partial quasigroup $(P, \circ_1)$ of order 3 is embedded in the quasigroup $(Q, \circ_2)$ of order 6.

$(P, \circ_1) =$

$\circ_1$	1	2	3
1	3	2	1
2	2	1	
3	1		3

$(Q, \circ_2) =$

$\circ_2$	1	2	3	4	5	6
1	3	2	1	4	5	6
2	2	1	4	5	6	3
3	1	4	3	6	2	5
4	4	5	6	2	3	1
5	5	6	2	3	1	4
6	6	3	5	1	4	2

2.22 Let $w(x, y) = w_1(x, y)w_2(x, y)$ and $v(x, y) = v_1(x, y)v_2(x, y)$ be words in the free groupoid over the alphabet $\{x, y\}$. The partial quasigroup $(P, \circ)$ *satisfies the identity* $w(x, y) = v(x, y)$ if and only if whenever $w(a, b)$ is defined and $v_1(a, b)$ and $v_2(a, b)$ are defined, then $v_1(a, b) \circ v_2(a, b) = v(a, b)$ is defined and $v(a, b) = w(a, b)$. A similar statement holds if $v(a, b)$ is defined.

2.23 **Example** The meanings of the identities $x^2 = x$, $xy = yx$, $x(xy) = y$, $(yx)x = y$, and $x(yx) = y$.

Identity $w(x, y) = v(xy)$	The partial quasigroup $(P, \circ)$ satisfies $w(x, y) = v(x, y)$ if and only if:
$x^2 = x$	$a \circ a$ is defined and $a \circ a = a$ for all $a \in P$.
$xy = yx$	for all $a, b \in P$, either both $a \circ b$ and $b \circ a$ are defined and $a \circ b = b \circ a$, or neither is defined.
$x(xy) = y$	if $a \circ b$ is defined, then $a \circ (a \circ b)$ is defined and $a \circ (a \circ b) = b$.
$x(yx) = y$	if $a \circ b$ is defined, then $b \circ (a \circ b)$ is defined and $b \circ (a \circ b) = a$.

2.24 **Example** In Example 2.21 the partial quasigroup $(P, \circ_1)$ as well as the quasigroup $(Q, \circ_2)$ satisfy the identity $xy = yx$. The partial $xy = yx$ quasigroup $(P, \circ_1)$ is *embedded* in the $xy = yx$ quasigroup $(Q, \circ_2)$.

2.25 **Example** Let $I = \{x^2 = x, xy = yx, (yx)x = y\}$. The partial I quasigroup $(P, \circ_1)$ of order 5 is embedded in the I quasigroup $(Q, \circ_2)$ of order 7.

$(P, \circ_1) =$

$\circ_1$	1	2	3	4	5
1	1	3	2	5	4
2	3	2	1		
3	2	1	3		
4	5			4	1
5	4			1	5

$(Q, \circ_2) =$

$\circ_2$	1	2	3	4	5	6	7
1	1	3	2	5	4	7	6
2	3	2	1	7	6	4	5
3	2	1	3	6	7	5	4
4	5	7	6	4	1	2	3
5	4	6	7	1	5	3	2
6	7	4	5	2	3	6	1
7	6	5	4	3	2	1	7

2.2 Equivalent Objects

2.26 **Theorem** The spectrum of Steiner quasigroups (equivalently, Steiner triple systems) is precisely the set of all positive integers $n \equiv 1$ or $3 \pmod 6$.

2.27 **Theorem** [1455] An idempotent semisymmetric quasigroup of order n (equivalently, a Mendelsohn triple system of order n) exists for precisely all positive integers $n \equiv 0$ or $1 \pmod 3$ except for $n = 6$.

2.28 **Theorem** [206] A self-orthogonal semisymmetric quasigroup of order n (equivalently, a SOMTS(n)) exists for precisely all positive integers $n \equiv 0$ or $1 \pmod 3$ except for $n = 3, 6, 9, 10, 12$ and except possibly for $n = 18$.

2.29 **Remark** Let Q be an n-set and let K_n be based on Q. A quasigroup $(Q, \cdot)$ satisfying the three identities $\{x^2 = x, x(yx) = y(xy), (yx)x = y\}$ is a *Steiner pentagon quasigroup*; it corresponds to a *Steiner pentagon system* (K_n, B), where a pentagon (x, y, z, u, v) belongs to B if and only if $xy = z$ and $yx = v$ for $x \neq y$ and $x^2 = x$ for all x in Q. Steiner pentagon quasigroups are also useful in the construction of other types of combinatorial structures, including perfect Mendelsohn designs with block size five and holey SOLSSOMs.

2.30 **Theorem** [1465] The spectrum of Steiner pentagon quasigroups (equivalently, Steiner pentagon systems) is precisely the set of all positive integers $n \equiv 1$ or $5 \pmod{10}$, except for $n = 15$.

2.3 Short Conjugate-Orthogonal Identities

2.31 **Theorem** [804] Let $a(x, y)$ and $b(x, y)$ be conjugate operations on Q. Then $a \perp b$ if and only if there is a quasigroup word $w(x, y)$ such that $w(a(x, y), b(x, y)) = x$ holds identically.

2.32 An identity of the type described in Theorem 2.31 where $w(x, y)$ is a word of length two is a *short conjugate-orthogonal identity.*

2.33 Two quasigroup identities $u_1(x,y) = v_1(x,y)$ and $u_2(x,y) = v_2(x,y)$ are *conjugate-equivalent* if, when $(Q,\cdot)$ is a quasigroup satisfying one of them, at least one conjugate of $(Q,\cdot)$ satisfies the other.

2.34 Example The identity $yx \cdot xy = x$ is conjugate-equivalent to the identity $(x \cdot yx)y = x$ because it can readily be verified that the $(1,3,2)$-conjugate of a quasigroup satisfying the first identity satisfies the second identity.

2.35 Remark Most of what follows is confined to short conjugate-orthogonal identities and their associated combinatorial structures. Here is provided a set of quasigroup identities that imply that at least two conjugates are orthogonal. See [191, 804] for more details. A name of the identity and/or the associated quasigroup is given when one is in common usage.

2.36 Theorem [182, 191, 804] Any short conjugate-orthogonal identity that is nontrivial is conjugate-equivalent to one of the following:

1.	$xy \cdot yx = x$	*Schröder quasigroup*
2.	$yx \cdot xy = x$	*Stein's third law*
3.	$(xy \cdot y)y = x$	*C_3-quasigroup*
4.	$x \cdot xy = yx$	*Stein's first law*; *Stein quasigroup*
5.	$(yx \cdot y)y = x$	
6.	$yx \cdot y = x \cdot yx$	*Stein's second law*
7.	$xy \cdot y = x \cdot xy$	*Schröder's first law*

The notation xy is shorthand for $(x \cdot y)$. So, for example, the first quasigroup identity is actually $(x \cdot y) \cdot (y \cdot x) = x$.

2.4 Basic Constructions

2.37 Remark The standard construction techniques for finite models of the short conjugate-orthogonal identities combine the direct constructions from finite fields with recursive constructions, including the familiar direct product construction and its numerous generalizations in the form of the singular direct product construction. Pairwise balanced designs (PBDs) are of fundamental importance in the recursive construction of two-variable quasigroup models, and Theorem 2.38 is used extensively.

2.38 Theorem Let V be a variety of algebras that is idempotent and based on two-variable identities. Suppose that there is a PBD$(v, K, 1)$ such that for each block size $k \in K$ there is a model of V of order k. Then there is a model of V of order v.

2.39 Example The idempotent quasigroup of order 4 constructed in Example 2.16 represents a model for each of the identities (1), (3), (4), and (7) in Theorem 2.36. Because there is a PBD$(v, \{4\}, 1)$ for all integers $v \equiv 1$ or $4 \pmod{12}$, Theorem 2.38 guarantees the existence of idempotent quasigroups satisfying each of the identities (1), (3), (4), and (7) in Theorem 2.36 for all orders $v \equiv 1$ or $4 \pmod{12}$.

2.40 Example In Example 2.17, finite fields produced idempotent models of the identity (5) in Theorem 2.36 for orders 5, 7, and 8. Together with the closure $B(5,7,8)$ from Table IV.3.23, Theorem 2.38 guarantees the existence of idempotent quasigroups satisfying the identity $(yx \cdot y)y = x$ for all but a relatively small number of orders.

2.41 Example For each of the identities (2) and (6) in Theorem 2.36, there are idempotent models in $\mathbb{F}_q$ for all prime powers $q \equiv 1 \pmod 4$. In particular, there are idempotent quasigroups satisfying each of the two identities for order $k \in \{5, 9, 13, 17, 29\}$. Together with $B(5,9,13)$ from Table IV.3.23, Theorem 2.38 therefore guarantees the

existence of idempotent quasigroups satisfying each of the identities (2) and (6) in Theorem 2.36 for all orders $v \equiv 1 \pmod 4$, except for $v = 33$.

2.5 Existence and Equivalences

2.42 Table Existence results for quasigroups in all cases of Theorem 2.36.

Case	Spectrum	Reference
1. Schröder quasigroup	$n \equiv 0, 1 \pmod 4$, $n \neq 5$	[201, 580, 1455]
2. Stein's third law	$n \equiv 0, 1 \pmod 4$	[191, 208, 844, 1455, 1926]
3. C_3-quasigroup	$n \equiv 0, 1 \pmod 3$, $n \neq 6$	[191]
4. Stein quasigroup	$n \geq 1$, $n \notin \{2, 3, 6, 7, 8, 10, 12, 14, 15, 18\}$, except possibly for $n \in \{22, 23, 26, 27, 30, 34, 38, 42, 43, 46, 50, 54, 62, 66, 74, 78, 90, 98, 102, 114, 126\}$	[191, 2199]
5. $(yx \cdot y)y = x$	$n \geq 1$, $n \notin \{2, 6, 10\}$, except possibly for $n \in \{14, 18, 26, 30, 38, 42, 158\}$	[190, 844, 1926, 2199]
6. $yx \cdot y = x \cdot yx$	does not contain 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15; contains all positive integers $n \equiv 1 \pmod 4$, except possibly $n = 33$; other cases open.	[191, 208, 844, 1926, 2199]
7. Schröder's first law	does not contain 2, 3, 5, 6, 7, 10, 11, 12, 14, 15; contains all other positive integers $n \equiv 0, 1 \pmod 4$ except possibly for $n \in \{20, 21, 24, 41, 44, 48, 53, 60, 69, 77\}$; other cases open.	[191, 208, 844, 1926, 2199]

2.43 Table Existence results for *idempotent* quasigroups in cases of Theorem 2.36. In cases (4), (6), and (7), the identity forces the quasigroup to be idempotent, so the result of Table 2.42 is not repeated here.

Case	Spectrum	Reference
1. Schröder quasigroup	$n \equiv 0, 1 \pmod 4$, $n \neq 5, 9$	[201, 580]
2. Stein's third law	$n \equiv 0, 1 \pmod 4$, $n \neq 4, 8$	[191, 208, 844, 1455, 1926]
3. C_3-quasigroup	$n \equiv 1 \pmod 3$	[191]
5. $(yx \cdot y)y = x$	$n \geq 1, n \notin \{2, 3, 4, 6, 9, 10, 12, 13, 14, 15, 16\}$, except possibly for $n \in \{18, 20, 22, 24, 26, 28, 30, 34, 38, 39, 42, 44, 46, 51, 52, 58, 60, 62, 66, 68, 70, 72, 74, 75, 76, 86, 87, 90, 94, 96, 98, 99, 100, 102, 106, 108, 110, 114, 116, 118, 122, 132, 142, 146, 154, 158, 164, 170, 174\}$	[190, 844, 1926, 2199]

2.44 Remark With regards to Table 2.42, combining the current results on $B(4, 8)$ from Table IV.3.23 with Example 2.18 and Theorem 2.38, one obtains the existence of quasigroups satisfying the identity (7) in Theorem 2.36 for orders $v = 101, 164$.

2.45 Table Conjugate orthogonality implied in each case of Theorem 2.36.

Case	(1,3,2)	(2,1,3)	(2,3,1)	(3,1,2)	(3,2,1)
1. Schröder quasigroup		X			
2. Stein's third law		X			
3. C_3-quasigroup					X
4. Stein quasigroup	X	X			
5. $(yx \cdot y)y = x$			X	X	X
6. $yx \cdot y = x \cdot yx$			X	X	
7. Schröder's first law	X				X

2.46 Remark The Schröder identity is conjugate invariant in the sense that every conjugate of a Schröder quasigroup is also a Schröder quasigroup. Consequently, Schröder quasigroups provide examples of latin squares with self-orthogonal conjugates. More importantly, Schröder quasigroups have been used in the construction and description of a variety of other combinatorial designs, including a class of edge-colored graph designs that correspond to triple tournaments (see, for example, [143, 191, 201, 580, 1455]).

2.47 Proposition A Schröder quasigroup of order n is equivalent to a SOLS(n) with the Weisner property (§III.5.5) and to an OA$(4, n)$ that has the Klein 4-group as a conjugate invariant subgroup.

2.48 Theorem [201] There exists an idempotent Schröder quasigroup of order n missing a sub-quasigroup of order 2 if and only if $n \equiv 2, 3 \pmod 4$, $n \geq 7$, and $n \neq 10$.

2.49 Remark Stein's third law has been useful in the construction of combinatorial designs (see, for example, [143, 191, 208, 1455]).

2.50 Proposition A quasigroup of order n satisfying Stein's third law is equivalent to an OA$(4, n)$ having the cyclic group of order 4 as a conjugate invariant subgroup.

2.51 Proposition An idempotent quasigroup of order n satisfying Stein's third law is equivalent to an $(n, 4, 1)$-perfect Mendelsohn design, and to a directed triple tournament with n players.

2.52 Proposition A C_3-quasigroup of order n is equivalent to an OA$(4, n)$ that has the cyclic group of order 3 as a conjugate invariant subgroup. When idempotent, it is equivalent to an almost resolvable MTS(n).

2.53 Remark Stein quasigroups are perhaps the most extensively studied of the short conjugate-orthogonal identities. Stein [1955] investigated these quasigroups with the hope of finding a counterexample to the Euler conjecture concerning orthogonal latin squares. However, investigations continued long after the disproof of the Euler conjecture because their broad spectrum provides a source for SOLS among other things.

2.54 Remark Idempotent models of quasigroups satisfying the identity $(yx \cdot y)y = x$ produce a class of 2-fold perfect resolvable Mendelsohn designs [190].

2.55 Remark Schröder's first law is conjugate invariant. Quasigroups satisfying Schröder's first law produce a class of 2-fold perfect resolvable Mendelsohn designs.

2.6 Embedding Results

2.56 Remark In Table 2.57 the identities (2), (3), and (4) are conjugate as are the identities (5), (6), and (7). So the embedding in [621] for (2) treats (3) and (4), and the embedding in [621] for (5) treats (6) and (7). The column headed "Best Possible Embedding" means that with possibly one or two small exceptions, it is possible to

construct a partial I quasigroup of order n that cannot be embedded in an I quasigroup of order less than the given bound.

2.57 Table Let I be a subset of the identities $\{x^2 = x, xy = yx, (yx)x = y, x(xy) = y, x(yx) = y\}$. The best results to date (with respect to the size of the containing quasigroup) of the problem of embedding a partial I quasigroup of order n in an I quasigroup of order t:

	Partial I-Quasigroup of Order n with $I =$	Best Possible Embedding	Best Embedding to Date
1	ϕ	all $t \geq 2n$	all $t \geq 2n$ [803]
2	$xy = yx$ (commutative)	all even $t \geq 2n$	all even $t \geq 2n$ [621]
3	$x(xy) = y$		
4	$(yx)x = y$		
5	$x^2 = x, xy = yx$	all odd $t \geq 2n+1$	all odd $t \geq 2n+1$ [621]
6	$x^2 = x, x(xy) = y$		
7	$x^2 = x, (yx)x = y$		
8	$x^2 = x$ (idempotent)	all $t \geq 2n+1$	all $t \geq 2n+1$ [86]
9	$x(yx) = y$ (semisymmetric)	all $t \geq 2n$	all $t \geq 6n$ such that $t \equiv 0$ or $3 \pmod 6$ [622]
10	$x(xy) = y$, $(yx)x = y$ (totally symmetric)	all even $t \geq 2n+4$	all even $t \geq 2n+4$ [359]
11	$x^2 = x$, $x(yx) = y$ (Mendelsohn quasigroup)	all $t \geq 2n+1$ such that $t \equiv 0$ or $1 \pmod 3$	all $t \geq 4n$ such that $t \equiv 0$ or $1 \pmod 3$ [1810]
12	$x^2 = x$, $x(xy) = y$ and $(yx)x = y$ (Steiner quasigroup)	all $t \geq 2n+1$ such that $t \equiv 1$ or $3 \pmod 6$	all $t \geq 2n+1$ such that $t \equiv 1$ or $3 \pmod 6$ [361]

2.58 Remarks There is a vast literature on embedding partial quasigroups and designs. As a rule of thumb, almost any partial quasigroup one can think of can be finitely embedded. But in almost all of these embeddings the containing quasigroup is "extremely large". Those listed in Table 2.57 appear to be the most fundamental ones for which a "small" embedding exists. Doyen–Wilson type embeddings (complete systems in complete systems) have been omitted as well because they are not partial.

See Also

§I.2	Steiner triple systems are equivalent to Steiner quasigroups.
§III.1	Latin squares correspond to multiplication tables of quasigroups.
§III.3	Quasigroup identities lead to orthogonal arrays with various conjugate orthogonal subgroups.
§III.5	Self-orthogonal latin squares arise from (2,1,3)-conjugate orthogonal quasigroups.
§VI.12	Steiner pentagon systems are equivalent to Steiner pentagon quasigroups.
§VI.35	Mendelsohn triple systems are equivalent to idempotent semisymmetric quasigroups.
[208]	An extensive survey on quasigroup identities and their use in the construction of combinatorial designs.
[684]	A textbook on latin squares and quasigroups.
[1454, 1456, 1460]	An extensive introduction to the general problem of embedding (partial) quasigroups and designs into quasigroups and designs of the same type.

References Cited: [86,143,182,190,191,201,206,208,359,361,580,621,622,684,803,804,844,1454, 1455,1456,1460,1465,1810,1926,1955,2199]

3 Mutually Orthogonal Latin Squares (MOLS)

R. Julian R. Abel
Charles J. Colbourn
Jeffrey H. Dinitz

3.1 Definition and Example

3.1 Two latin squares L and L' of the same order are *orthogonal* if $L(a,b) = L(c,d)$ and $L'(a,b) = L'(c,d)$, implies $a = c$ and $b = d$.

3.2 **Remark** An equivalent definition for orthogonality: Two latin squares of side n $L = (a_{i,j})$ (on symbol set S) and $L' = (b_{i,j})$ (on symbol set S') are *orthogonal* if every element in $S \times S'$ occurs exactly once among the n^2 pairs $(a_{i,j}, b_{i,j})$, $1 \le i, j \le n$.

3.3 A set of latin squares $L_1, \ldots, L_m$ is *mutually orthogonal*, or a set of *MOLS*, if for every $1 \le i < j \le m$, L_i and L_j are orthogonal. These are also referred to as *POLS*, *pairwise orthogonal* latin squares.

3.4 **Example** Three mutually orthogonal latin squares of side 4.

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

3.2 Equivalent Objects

3.5 An *orthogonal array* $\mathrm{OA}(k,s)$ is a $k \times s^2$ array with entries from an s-set S having the property that in any two rows, each (ordered) pair of symbols from S occurs exactly once.

3.6 **Remark** A far more general definition of orthogonal arrays can be found in §III.6.1.

3.7 **Remark** Let $\{L_i : 1 \le i \le k\}$ be a set of k MOLS on symbols $\{1, \ldots, n\}$. Form a $(k+2) \times n^2$ array $A = (a_{ij})$ whose columns are $(i, j, L_1(i,j), L_2(i,j), \ldots, L_k(i,j))^T$ for $1 \le i, j \le k$. Then A is an orthogonal array, $\mathrm{OA}(k+2, n)$. This process can be reversed to recover k MOLS of side n from an $\mathrm{OA}(k+2, n)$, by choosing any two rows of the OA to index the rows and columns of the k squares.

3.8 **Example** An $\mathrm{OA}(5, 4)$ derived from the 3 MOLS in Example 3.4.

$$\begin{pmatrix} 1111222233334444 \\ 1234123412341234 \\ 1234432121433412 \\ 1234341243212143 \\ 1234214334124321 \end{pmatrix}$$

3.9 A *transversal design* of *order* or *groupsize* n, *blocksize* k, and *index* λ, denoted $\mathrm{TD}_\lambda(k,n)$, is a triple $(V,\mathcal{G},\mathcal{B})$, where

1. V is a set of kn elements;
2. $\mathcal{G}$ is a partition of V into k classes (the *groups*), each of size n;
3. $\mathcal{B}$ is a collection of k-subsets of V (the *blocks*);
4. every unordered pair of elements from V is contained either in exactly one group or in exactly λ blocks, but not both.

When $\lambda = 1$, one writes simply $\mathrm{TD}(k,n)$.

3.10 **Remark** Let A be an $\mathrm{OA}(k,n)$ on the n symbols in X. On $V = X \times \{1,\ldots,k\}$ (a set of size kn), form a set $\mathcal{B}$ of k-sets as follows. For $1 \le j \le n^2$, include $\{(a_{i,j},i) : 1 \le i \le k\}$ in $\mathcal{B}$. Then let $\mathcal{G}$ be the partition of V whose classes are $\{X \times \{i\} : 1 \le i \le k\}$. Then $(V,\mathcal{G},\mathcal{B})$ is a $\mathrm{TD}(k,n)$. This process can be reversed to recover an $\mathrm{OA}(k,n)$ from a $\mathrm{TD}(k,n)$.

3.11 **Example** A $\mathrm{TD}(5,4)$ derived from the $\mathrm{OA}(5,4)$ in Example 3.8. On the element set $\{1,2,3,4\} \times \{1,2,3,4,5\}$, the blocks are

{ 11,12,13,14,15 }	{ 11,22,23,24,25 }	{ 11,32,33,34,35 }	{ 11,42,43,44,45 }
{ 21,12,43,34,25 }	{ 21,22,33,44,15 }	{ 21,32,23,14,45 }	{ 21,42,13,24,35 }
{ 31,12,23,44,35 }	{ 31,22,13,34,45 }	{ 31,32,43,24,15 }	{ 31,42,33,14,25 }
{ 41,12,33,24,45 }	{ 41,22,43,14,35 }	{ 41,32,13,44,25 }	{ 41,42,23,34,15 }

3.12 A $\mathrm{TD}_\lambda(k,n)$ $(V,\mathcal{G},\mathcal{B})$ is *α-resolvable* if its blocks can be partitioned into sets $\mathcal{B}_1,\ldots,\mathcal{B}_s$, where every element of V occurs exactly α times in each $\mathcal{B}_i$. The classes $\mathcal{B}_1,\ldots,\mathcal{B}_s$ are *α-parallel classes*. When $\alpha = 1$ the design is *(completely) resolvable* and the classes are *parallel classes*. An $\mathrm{RTD}_\lambda(k,n)$ is a 1-resolvable $\mathrm{TD}_\lambda(k,n)$.

3.13 **Remark** Let $(V,\mathcal{G},\mathcal{B})$ be a $\mathrm{TD}_\lambda(k+1,n)$. Let $G \in \mathcal{G}$ and $G = \{g_1,\ldots,g_n\}$. Form $\mathcal{B}_i = \{B \backslash \{g_i\} : g_i \in B \in \mathcal{B}\}$, and let $\widehat{\mathcal{B}} = \bigcup_{i=1}^n \mathcal{B}_i$. Then $(V \setminus G, \mathcal{G} \setminus \{G\}, \widehat{\mathcal{B}})$ is an $\mathrm{RTD}_\lambda(k,n)$. Its λ-parallel classes are $\mathcal{B}_1,\ldots,\mathcal{B}_n$. This process can be reversed to form a $\mathrm{TD}_\lambda(k+1,n)$ from an $\mathrm{RTD}_\lambda(k,n)$.

3.14 **Example** A resolvable $\mathrm{TD}(4,4)$ derived from the $\mathrm{TD}(5,4)$ in Example 3.11. On the element set $\{1,2,3,4\} \times \{2,3,4,5\}$, the blocks are:

{ 12,13,14,15 }	{ 22,23,24,25 }	{ 32,33,34,35 }	{ 42,43,44,45 }
{ 12,43,34,25 }	{ 22,33,44,15 }	{ 32,23,14,45 }	{ 42,13,24,35 }
{ 12,23,44,35 }	{ 22,13,34,45 }	{ 32,43,24,15 }	{ 42,33,14,25 }
{ 12,33,24,45 }	{ 22,43,14,35 }	{ 32,13,44,25 }	{ 42,23,34,15 }

Each row is a parallel class.

3.15 A (k,n)-*net* is a pair $(X,\mathcal{C})$ where X is a set of n^2 elements, and $\mathcal{C}$ is a set of kn subsets (*blocks*) of X each of size n with the property that two distinct blocks intersect in at most one element. Moreover, the blocks of $\mathcal{C}$ can be partitioned into k parallel classes each containing n blocks.

3.16 **Remark** Let $(V,\mathcal{G},\mathcal{B})$ be a $\mathrm{TD}(k,n)$. Interchanging the roles of elements and blocks gives a (k,n)-net.

3.17 **Example** The (5,4)-net obtained from the $\mathrm{TD}(5,4)$ in Example 3.11 is an affine plane of order four.

3.18 **Theorem** The existence of k MOLS of side n is equivalent to the existence of

1. a transversal design of index one, blocksize $k+2$, and groupsize n, namely, a $\mathrm{TD}(k+2,n)$,

2. a resolvable transversal design of index one, blocksize $k+1$, and groupsize n, namely, an RTD$(k+1, n)$,
3. a $(k+2, n)$-net,
4. an orthogonal array of strength two, index one, degree $k+2$, and order n, namely an OA$(k+2, n)$, and
5. an edge-partition of the complete $(k+2)$-partite graph $K_{n,\ldots,n}$ into complete subgraphs of order $k+2$.

3.19 A set of $n-1$ MOLS of side n is a *complete set* of MOLS.

3.20 **Theorem** The existence of a complete set of MOLS of side n is equivalent to the existence of a projective plane of order n (§VII.2.1) and an affine plane of order n (§VII.2.2).

3.21 **Remark** It is not known whether there exists a complete set of MOLS of side n for any n that is not a power of a prime. There is no complete set of MOLS of side 6 or 10. The smallest unknown case is $n = 12$.

3.3 Basic Facts about N(n)

3.22 $N(n)$ is the maximum number of latin squares in a set of MOLS of side n. $N(1^n)$ is the maximum number of latin squares in a set of idempotent MOLS of side n.

3.23 **Remark**

Euler's 36 Officers Problem:

A very curious question, which has exercised for some time the ingenuity of many people, has involved me in the following studies, which seem to open a new field of analysis, in particular the study of combinations. The question revolves around arranging 36 officers to be drawn from 6 different ranks and also from 6 different regiments so that they are ranged in a square so that in each line (both horizontal and vertical) there are 6 officers of different ranks and different regiments.

Euler went on to conjecture that such an $n \times n$ array does not exist for $n = 6$, nor does one exist whenever $n \equiv 2 \pmod 4$. This was known as the *Euler conjecture* until its disproof (see Theorem 3.43).

3.24 **Remark** By convention, $N(0) = N(1) = \infty$.

3.25 **Theorem** For every $n > 1$, $1 \leq N(n) \leq n-1$.

3.26 **Theorem** (MacNeish [1499]) $N(n \times m) \geq \min\{N(n), N(m)\}$.

3.27 **Theorem** (Rees [1790]) If $n < m$, $N(1^{n \times m}) \geq \min\{N(n), N(m)-1\}$.

3.28 **Theorem** If $q = p^e$ is a prime power, then $N(q) = q-1$.

3.29 **Construction** Construct the complete set of MOLS of order q for Theorem 3.28 as follows: For each $\alpha \in \mathbb{F}_q \setminus \{0\}$, define the latin square $L_\alpha(i,j) = i + \alpha j$, where $i, j \in \mathbb{F}_q$ and the algebra is performed in $\mathbb{F}_q$. The set of latin squares $\{L_\alpha | \alpha \in \mathbb{F}_q \setminus \{0\}\}$ is a set of $q-1$ MOLS of side q.

3.30 **Corollary** If $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where each p_i is a prime, then $N(n) \geq min\{p_i^{e_i} - 1 | i = 1, 2, \ldots k\}$.

3.31 **Theorem** A latin square of side n has an orthogonal mate ($N(n) \geq 2$) if and only if it contains n disjoint transversals (equivalently, the corresponding TD$(3, n)$ is resolvable).

3.32 Theorem Let $s \equiv 1$ or $2 \pmod 4$ and assume that s is not the sum of two squares.

1. Let t be the largest positive integer for which $\frac{1}{2}t^4 - t^3 + t^2 + \frac{1}{2}t - 1 < s$. Then $N(s) \leq s - t - 2$.
2. [1596] Let t be the largest positive integer for which $8t^3 + 18t^2 + 8t + 4 - 2\rho(t^2 - t - 1) + \frac{9}{2}\rho(\rho - 1)(t - 1) < 3s$, where $\rho \equiv t + 1 \pmod 3$ and $\rho \in \{0, 1, 2\}$. Then $N(s) \leq s - t - 2$.

3.33 Example $N(n) \leq n - 4$ for $n = 14, 21, 22$
$N(n) \leq n - 5$ for $n = 30, 33, 38, 42, 46, 54, 57, 62, 66, 69, 70, 77, 78$
$N(n) \leq n - 6$ for $n = 86, 93, 94$

3.34 Theorem [502] $\lim_{n\to\infty} N(n) = \infty$. In fact, for n sufficiently large, $N(n) \geq n^{\frac{1}{14.8}}$ [224].

3.4 MOLS of Small Side

3.35 Remark Sets of k orthogonal latin squares of side n for $n \leq 10$ where k is the largest number such that $N(n) \geq k$ are displayed in this section. Also displayed are the constructions that yield the squares of sides $n \leq 56$ and $n = 62$, 75, and 80 that attain the lower bound for $N(n)$ in the cases where n is not a prime power.

3.36 Theorem $N(3) = 2$.

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

3.37 Theorem $N(4) = 3$. (The set of 3 MOLS of order 4 is given in Example 3.4).

3.38 Theorem $N(5) = 4$.

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

3.39 Theorem $N(6) = 1$.

3.40 Theorem $N(7) = 6$.

0	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

0	1	2	3	4	5	6
2	3	4	5	6	0	1
4	5	6	0	1	2	3
6	0	1	2	3	4	5
1	2	3	4	5	6	0
3	4	5	6	0	1	2
5	6	0	1	2	3	4

0	1	2	3	4	5	6
3	4	5	6	0	1	2
6	0	1	2	3	4	5
2	3	4	5	6	0	1
5	6	0	1	2	3	4
1	2	3	4	5	6	0
4	5	6	0	1	2	3

0	1	2	3	4	5	6
4	5	6	0	1	2	3
1	2	3	4	5	6	0
5	6	0	1	2	3	4
2	3	4	5	6	0	1
6	0	1	2	3	4	5
3	4	5	6	0	1	2

0	1	2	3	4	5	6
5	6	0	1	2	3	4
3	4	5	6	0	1	2
1	2	3	4	5	6	0
6	0	1	2	3	4	5
4	5	6	0	1	2	3
2	3	4	5	6	0	1

0	1	2	3	4	5	6
6	0	1	2	3	4	5
5	6	0	1	2	3	4
4	5	6	0	1	2	3
3	4	5	6	0	1	2
2	3	4	5	6	0	1
1	2	3	4	5	6	0

3.41 Theorem $N(8) = 7$.

0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6
2	3	0	1	6	7	4	5
3	2	1	0	7	6	5	4
4	5	6	7	0	1	2	3
5	4	7	6	1	0	3	2
6	7	4	5	2	3	0	1
7	6	5	4	3	2	1	0

0	1	2	3	4	5	6	7
2	3	0	1	6	7	4	5
4	5	6	7	0	1	2	3
6	7	4	5	2	3	0	1
5	4	7	6	1	0	3	2
7	6	5	4	3	2	1	0
1	0	3	2	5	4	7	6
3	2	1	0	7	6	5	4

0	1	2	3	4	5	6	7
3	2	1	0	7	6	5	4
6	7	4	5	2	3	0	1
5	4	7	6	1	0	3	2
1	0	3	2	5	4	7	6
2	3	0	1	6	7	4	5
7	6	5	4	3	2	1	0
4	5	6	7	0	1	2	3

0	1	2	3	4	5	6	7
4	5	6	7	0	1	2	3
5	4	7	6	1	0	3	2
1	0	3	2	5	4	7	6
7	6	5	4	3	2	1	0
3	2	1	0	7	6	5	4
2	3	0	1	6	7	4	5
6	7	4	5	2	3	0	1

0	1	2	3	4	5	6	7
5	4	7	6	1	0	3	2
7	6	5	4	3	2	1	0
2	3	0	1	6	7	4	5
3	2	1	0	7	6	5	4
6	7	4	5	2	3	0	1
4	5	6	7	0	1	2	3
1	0	3	2	5	4	7	6

0	1	2	3	4	5	6	7
6	7	4	5	2	3	0	1
1	0	3	2	5	4	7	6
7	6	5	4	3	2	1	0
2	3	0	1	6	7	4	5
4	5	6	7	0	1	2	3
3	2	1	0	7	6	5	4
5	4	7	6	1	0	3	2

0	1	2	3	4	5	6	7
7	6	5	4	3	2	1	0
3	2	1	0	7	6	5	4
4	5	6	7	0	1	2	3
6	7	4	5	2	3	0	1
1	0	3	2	5	4	7	6
5	4	7	6	1	0	3	2
2	3	0	1	6	7	4	5

3.42 Theorem $N(9) = 8$.

0	1	2	3	4	5	6	7	8
1	2	0	4	5	3	7	8	6
2	0	1	5	3	4	8	6	7
3	4	5	6	7	8	0	1	2
4	5	3	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1
6	7	8	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3
8	6	7	2	0	1	5	3	4

0	1	2	3	4	5	6	7	8
2	0	1	5	3	4	8	6	7
1	2	0	4	5	3	7	8	6
6	7	8	0	1	2	3	4	5
8	6	7	2	0	1	5	3	4
7	8	6	1	2	0	4	5	3
3	4	5	6	7	8	0	1	2
5	3	4	8	6	7	2	0	1
4	5	3	7	8	6	1	2	0

0	1	2	3	4	5	6	7	8
3	4	5	6	7	8	0	1	2
6	7	8	0	1	2	3	4	5
4	5	3	7	8	6	1	2	0
7	8	6	1	2	0	4	5	3
1	2	0	4	5	3	7	8	6
8	6	7	2	0	1	5	3	4
2	0	1	5	3	4	8	6	7
5	3	4	8	6	7	2	0	1

0	1	2	3	4	5	6	7	8
4	5	3	7	8	6	1	2	0
8	6	7	2	0	1	5	3	4
7	8	6	1	2	0	4	5	3
2	0	1	5	3	4	8	6	7
3	4	5	6	7	8	0	1	2
5	3	4	8	6	7	2	0	1
6	7	8	0	1	2	3	4	5
1	2	0	4	5	3	7	8	6

0	1	2	3	4	5	6	7	8
5	3	4	8	6	7	2	0	1
7	8	6	1	2	0	4	5	3
1	2	0	4	5	3	7	8	6
3	4	5	6	7	8	0	1	2
8	6	7	2	0	1	5	3	4
2	0	1	5	3	4	8	6	7
4	5	3	7	8	6	1	2	0
6	7	8	0	1	2	3	4	5

0	1	2	3	4	5	6	7	8
6	7	8	0	1	2	3	4	5
3	4	5	6	7	8	0	1	2
8	6	7	2	0	1	5	3	4
5	3	4	8	6	7	2	0	1
2	0	1	5	3	4	8	6	7
4	5	3	7	8	6	1	2	0
1	2	0	4	5	3	7	8	6
7	8	6	1	2	0	4	5	3

0	1	2	3	4	5	6	7	8
7	8	6	1	2	0	4	5	3
5	3	4	8	6	7	2	0	1
2	0	1	5	3	4	8	6	7
6	7	8	0	1	2	3	4	5
4	5	3	7	8	6	1	2	0
1	2	0	4	5	3	7	8	6
8	6	7	2	0	1	5	3	4
3	4	5	6	7	8	0	1	2

0	1	2	3	4	5	6	7	8
8	6	7	2	0	1	5	3	4
4	5	3	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1
1	2	0	4	5	3	7	8	6
6	7	8	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3
3	4	5	6	7	8	0	1	2
2	0	1	5	3	4	8	6	7

3.43 Theorem (Parker; see [92]) $N(10) \geq 2$. See Remark VI.35.19 for a pair with four disjoint common transversals, and Example 5.6 for a self-orthogonal example.

3.44 Theorem [1206] $N(12) \geq 5$. The first row of each of the five squares L_1, L_2, L_3, L_4, L_5 is given. Each square is obtained by developing the first row over $\mathbb{Z}_2 \times \mathbb{Z}_6$. The group element (x, y) is written as xy.

L_1: 00 01 02 03 04 05 10 11 12 13 14 15
L_2: 00 03 10 01 13 15 02 12 05 04 11 14
L_3: 00 12 01 15 05 13 03 14 02 11 10 04
L_4: 00 04 15 14 02 11 12 10 13 01 03 05
L_5: 00 10 12 02 11 01 13 15 04 14 05 03

3.45 Remark Many of the constructions for MOLS in the remainder of this section use difference matrices, quasi-difference matrices, or $V(m,t)$ vectors. To go from these objects to a set of MOLS, see the constructions in §VI.17.

3.46 Theorem [2037] $N(14) \geq 3$. This follows from the existence of a $(13,5;1,1;1)$ quasi-difference matrix:

$$\begin{pmatrix} 0 & 12 & 10 & 0 & 6 & 12 & 0 & 10 & 8 & - & 7 & 0 & 1 & 6 & 9 \\ 4 & 0 & 10 & 10 & 0 & 5 & 11 & 0 & 4 & 0 & - & 8 & 3 & 5 & 1 \\ 4 & 12 & 0 & 2 & 4 & 0 & 12 & 7 & 0 & 11 & 0 & - & 9 & 2 & 3 \\ 10 & 4 & 12 & 11 & 7 & 8 & 3 & 9 & 1 & 11 & 7 & 8 & - & 0 & 0 \\ 5 & 2 & 6 & 10 & 4 & 12 & 6 & 5 & 2 & 3 & 9 & 1 & 0 & - & 0 \end{pmatrix}.$$

3.47 Theorem [6, 1847] $N(15) \geq 4$. This follows from the existence of a $(14,6;1,0;1)$ quasi-difference matrix:

$$\begin{pmatrix} - & 0 & 0 & 11 & 0 & 2 & 0 & 1 & 0 & 4 & 0 & 5 & 0 & 6 & 0 \\ 1 & 5 & - & 13 & 8 & 5 & 10 & 12 & 6 & 11 & 12 & 4 & 9 & 10 & 1 \\ 8 & 3 & 8 & 12 & - & 1 & 4 & 7 & 10 & 2 & 9 & 10 & 11 & 13 & 2 \\ 0 & - & 11 & 0 & 2 & 0 & 1 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 \\ 5 & 1 & 13 & - & 5 & 8 & 12 & 10 & 11 & 6 & 4 & 12 & 10 & 9 & 8 \\ 3 & 8 & 12 & 8 & 1 & - & 7 & 4 & 2 & 10 & 10 & 9 & 13 & 11 & 9 \end{pmatrix}.$$

3.48 Theorem [2117] $N(18) \geq 3$. Consider the matrix:

$$\left(\begin{array}{cc|ccccccccc} 0 & 0 & 10 & 1 & 8 & 5 & 7 & 0 & 4 & 6 & 13 \\ 7 & 1 & 2 & 3 & 11 & 9 & 12 & - & - & - & - \\ \hline 1 & 7 & 12 & 0 & 6 & 2 & 3 & 8 & 9 & 10 & 5 \\ 8 & 4 & 11 & - & - & - & - & 13 & 7 & 4 & 1 \end{array}\right).$$

Form a new array by replacing every column $(a,b,c,d)^T$, except the first column, by the pair of columns $(a,b,c,d)^T$ and $(b,a,d,c)^T$. This is a quasi-difference matrix with $n = 14$, $u = 4$, $\lambda = 1$, and $\mu = 0$; form the corresponding OA$(4,18)$. It is resolvable, as follows: Four parallel classes are given by extending the orbits of $(0,0,0,0)^T$, $(0,7,1,8)^T$, $(0,1,7,4)^T$, and $(1,0,4,7)^T$ modulo 14 with the four parallel classes of the resolvable OA$(4,4)$ on the fixed points. Fourteen parallel classes are formed by developing the parallel class consisting of the remaining 18 columns modulo 14. Thus, there is an OA$(5,18)$.

3.49 Theorem [2038, 47] $N(20) \geq 4$. Consider the matrix:

$$\begin{pmatrix} - & 7 & 13 & 1 & 16 & 9 & 2 \\ 0 & 1 & 15 & 7 & 17 & 6 & 14 \\ 0 & 11 & 10 & 11 & 5 & 4 & 3 \\ 7 & - & 13 & 16 & 1 & 2 & 9 \\ 1 & 0 & 15 & 17 & 7 & 14 & 6 \\ 11 & 0 & 10 & 5 & 11 & 3 & 4 \end{pmatrix}.$$

Each column $(a,b,c,d,e,f)^T$ is replaced by columns $(a,b,c,d,e,f)^T$, $(b,c,a,f,d,e)^T$, and $(c,a,b,e,f,d)^T$ to obtain a $(19,6;1,1;1)$ quasi-difference matrix.

3.50 Theorem [1669] $N(21) \geq 5$. Consider the following array over $\mathbb{Z}_{21}$:

$$\begin{pmatrix} 8 & 17 & 20 & 2 \\ 9 & 16 & 4 & 15 \\ 11 & 5 & 10 & 6 \\ 14 & 1 & 3 & 13 \\ 18 & 19 & 12 & 7 \end{pmatrix}.$$

Replace each column by its five cyclic shifts, then append a row and column of zeros. The result is a $(21,6,1)$ difference matrix.

3.51 **Theorem** [2, 49] $N(22) \geq 3$. Consider the following arrays over $\mathbb{Z}_{21}$:

$$A_1 = \begin{pmatrix} 1 & 13 & 18 & 3 & 16 & 19 & - \\ 16 & 19 & 1 & 13 & 18 & 3 & 0 \\ 18 & 3 & 16 & 19 & 1 & 13 & 0 \\ 6 & 15 & 6 & 15 & 6 & 15 & 0 \\ 12 & 9 & 19 & 16 & 5 & 2 & 0 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 0 \\ 7 & 14 \\ 14 & 7 \\ - & 0 \\ 0 & - \end{pmatrix}.$$

Replace each column (a, b, c, d, e) of A_1 by 3 columns (a, b, c, d, e), $(16c, 16a, 16b, 16d + 7, 16e + 14)$, and $(4b, 4c, 4a, 4d + 14, 4e + 7)$; then append the columns of A_2. This gives a (21,5;1,1;1) quasi-difference matrix.

3.52 **Theorem** [27] $N(24) \geq 7$. Consider the following matrix over $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$:

$$\begin{pmatrix} 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\ 0000 & 0010 & 0100 & 0110 & 1000 & 1010 & 1100 & 1110 & 2000 & 2010 & 2100 & 2110 \\ 0000 & 0011 & 1001 & 2110 & 0111 & 2011 & 2111 & 1000 & 0100 & 1100 & 1101 & 2010 \\ 0000 & 1010 & 1011 & 2000 & 1101 & 2110 & 0001 & 0101 & 2100 & 2001 & 0111 & 1100 \\ 0000 & 0001 & 2010 & 1111 & 2111 & 2100 & 1101 & 0011 & 1010 & 2101 & 1000 & 0110 \\ 0000 & 1000 & 2001 & 1011 & 0100 & 1100 & 0110 & 2101 & 2111 & 0010 & 1111 & 2011 \\ 0000 & 1001 & 0111 & 2100 & 2000 & 0010 & 1110 & 2011 & 1100 & 1011 & 0101 & 2111 \\ 0000 & 1011 & 2101 & 0100 & 2110 & 1001 & 2000 & 0110 & 0101 & 1111 & 2011 & 1010 \end{pmatrix}.$$

Replace each column $(a, b, c, d, e, f, g, h)^T$ by $(a, b, c, d, e, f, g, h)^T$ and $(a+(0, 0, 0, 0), b+(0, 0, 0, 1), c+(0, 0, 1, 0), d+(0, 0, 1, 1), e+(0, 1, 0, 0), f+(0, 1, 0, 1), g+(0, 1, 1, 0), h+(0, 1, 1, 1)\ )^T$. The result is a difference matrix with eight rows over $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

3.53 **Theorem** [526] $N(26) \geq 4$.

Consider the matrix shown on the right. Replace each column by six columns that are the six cyclic shifts of the column. The result is a quasi-difference matrix with $n = 21$, $u = 5$, $\lambda = 1$ and $\mu = 0$.

$$\begin{pmatrix} - & - & - & - & - \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 6 & 7 & 8 & 14 \\ 3 & 11 & 20 & 18 & 10 \\ 6 & 10 & 14 & 1 & 5 \\ 4 & 19 & 5 & 12 & 2 \end{pmatrix}$$

3.54 **Theorem** [6] $N(28) \geq 5$. Let z be a primitive element in $\mathbb{F}_4$. Consider the array A over $\mathbb{F}_4 \times \mathbb{Z}_7$:

$$\begin{pmatrix} (0,0) & (z{+}1,6) & (1,1) & (1,1) & (1,3) & (1,4) & (0,0) & (1,4) & (z,5) \\ (z,2) & (0,0) & (1,5) & (z,1) & (z,2) & (z,6) & (z{+}1,3) & (0,0) & (z,1) \\ (z,3) & (z{+}1,4) & (0,0) & (z{+}1,5) & (z{+}1,2) & (z{+}1,4) & (z{+}1,2) & (1,6) & (0,0) \\ (0,5) & (z,6) & (0,5) & (0,6) & (z,3) & (0,0) & (0,4) & (1,5) & (z{+}1,4) \\ (0,3) & (0,3) & (z{+}1,5) & (0,0) & (0,5) & (z{+}1,6) & (1,1) & (0,1) & (z,3) \\ (1,3) & (0,6) & (0,6) & (1,5) & (0,0) & (0,3) & (z{+}1,6) & (z,2) & (0,2) \end{pmatrix}.$$

Replace each column $(a, b, c, d, e, f)^T$ by three columns $(a, b, c, d, e, f)^T$, $(b, c, a, f, d, e)^T$, and $(c, a, b, e, f, d)^T$. Then append a column whose entries all equal (0,0). This gives a (28,6,1) difference matrix.

3.55 **Theorem** [47] $N(30) \geq 4$.

Consider the matrix over $\mathbb{Z}_5 \times \mathbb{Z}_5$ shown on the right. Replace each column $(a, b, c, d, e, f)^T$ by the five columns $(a + (i, i), b + (2i, i), c + (i, 0), d + (4i, 0), e + (3i, 4i), f + (4i, 4i))^T$ for $0 \leq i \leq 4$. The result is a quasi-difference matrix over $\mathbb{Z}_5 \times \mathbb{Z}_5$ with $n = 25$, $u = 5$, $\lambda = 1$, and $\mu = 1$.

$$\begin{pmatrix} 00 & - & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & - & 04 & 02 & 03 & 01 \\ 00 & 31 & 30 & - & 40 & 10 & 20 \\ 00 & 30 & 02 & 12 & - & 01 & 03 \\ 00 & 33 & 12 & 42 & 20 & - & 04 \\ 00 & 42 & 24 & 03 & 23 & 32 & - \end{pmatrix}$$

3.56 Theorem [38] $N(33) \geq 5$. Consider the matrices:

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 15 & 11 & 22 & 4 & 17 & 8 \\ 19 & 7 & 14 & 32 & 22 & 18 \\ 22 & 19 & 8 & 24 & 21 & 6 \\ 9 & 12 & 15 & 7 & 26 & 14 \\ 14 & 28 & 23 & 2 & 19 & 3 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 1 & 7 \\ 0 & 4 & 28 \\ 0 & 16 & 13 \\ 0 & 31 & 19 \\ 0 & 25 & 10 \\ 0 & 22 & 0 \end{pmatrix}.$$

Replace each column $C = (a, b, c, d, e, f)^T$ of A_1 by the five columns $t^i(C)$, $0 \leq i \leq 4$, where $t(C) = (4e, 4a, 4b, 4c, 4d, 4f)^T$. Then append the columns of A_2. The result is a difference matrix over $\mathbb{Z}_{33}$.

3.57 Theorem [6] $N(34) \geq 4$. Consider the matrices:

$$A_1 = \begin{pmatrix} - & 0 & 0 & 0 & 0 & 0 \\ 30 & 17 & 10 & 25 & 23 & 8 \\ 22 & 4 & 32 & 29 & 28 & 22 \\ 25 & 10 & 20 & 15 & 21 & 16 \\ 0 & 12 & 15 & 16 & 32 & 23 \\ 6 & 11 & 18 & 14 & 9 & 20 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 3 & 10 & 5 \\ 4 & 12 & 7 & 20 \\ 16 & 15 & 28 & 14 \\ 31 & 27 & 13 & 23 \\ 25 & 9 & 19 & 26 \\ 11 & 11 & 0 & - \end{pmatrix}.$$

Replace each column $C = (a, b, c, d, e, f)^T$ of A_1 by the five columns $t^i(C)$, $0 \leq i \leq 4$, where $t(C) = (4e, 4a, 4b, 4c, 4d, 4f)^T$. Then append the columns of A_2. The result is a (33,6;1,0;1) quasi-difference matrix.

3.58 Theorem (Wojtas, alternate construction to [2160]) $N(35) \geq 5$. Append a row of all zeroes to the following array to obtain a (35,6,1) difference matrix over $\mathbb{Z}_{35}$:

$$\begin{pmatrix} 0\,15\,30\,10\,25 & 1 & 16\,31\,11\,26 & 2 & 17\,32\,12 & 6 & 3 & 18\,33\,27\,21 & 4 & 19\,13 & 7 & 22 & 5 & 34\,28 & 8 & 23\,20\,14\,29 & 9 & 24 \\ 0\,22\,16 & 3 & 4 & 9 & 10\,32\,26\,13\,18 & 5 & 27\,14\,15\,20 & 7 & 1 & 23\,31\,29 & 2 & 24\,11\,19\,17\,25 & 12 & 6 & 28\,33\,34\,21 & 8 & 30 \\ 0\,29 & 2 & 31\,18\,10\,32\,26\,34\,28\,27\,21\,15 & 9 & 17\,30 & 3 & 4 & 5 & 20\,12 & 6 & 14\,22\,16 & 8 & 23\,24\,25\,33\,11\,19\,13 & 7 & 1 \\ 0 & 8 & 9 & 17\,11\,25\,19\,27\,28 & 1 & 15\,23\,31 & 4 & 26\,12 & 6 & 14\,29\,16 & 2 & 3 & 18\,33\,34\,20 & 7 & 22\,30\,24\,10\,32 & 5 & 13\,21 \\ 0 & 1 & 23\,24\,32\,33 & 6 & 7 & 29\,30\,10\,11\,12\,13\,28 & 8 & 9 & 31 & 4 & 5 & 27\,14\,15\,16 & 3 & 25\,26\,34\,21\,22 & 2 & 17\,18\,19\,20 \end{pmatrix}$$

3.59 Theorem [27] $N(36) \geq 8$. Consider the matrix A over $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$:

$$A = \begin{pmatrix} 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\ 0000 & 0100 & 1000 & 1100 & 0001 & 0101 & 1001 & 1101 & 0002 & 0102 & 1002 & 1102 \\ 0000 & 1112 & 0021 & 0012 & 0120 & 0102 & 1111 & 0111 & 1110 & 1022 & 1001 & 1010 \\ 0000 & 0010 & 1010 & 0100 & 1100 & 1020 & 1000 & 0120 & 1120 & 0020 & 1110 & 0110 \\ 0000 & 0120 & 0010 & 1110 & 1020 & 1010 & 0100 & 0020 & 0110 & 1100 & 1120 & 1000 \\ 0000 & 0110 & 0120 & 1120 & 1102 & 0012 & 1122 & 1002 & 1001 & 1011 & 0021 & 0111 \\ 0000 & 1010 & 1101 & 1012 & 1022 & 0021 & 0101 & 0100 & 1122 & 0110 & 0012 & 1121 \\ 0000 & 1100 & 0110 & 1021 & 0102 & 1022 & 0022 & 1110 & 1011 & 0121 & 1111 & 0002 \\ 0000 & 1000 & 1110 & 0112 & 1121 & 0111 & 0011 & 1020 & 0122 & 1102 & 1022 & 0001 \end{pmatrix}.$$

A $(36, 9, 1)$ difference matrix is obtained by adding the following 3 vectors to each of the 12 columns of A: $(\ (0,0,0,0), (0,0,y,0), (0,0,2y,0), (0,0,0,y), (0,0,0,2y), (0,0,y,y), (0,0,2y,2y), (0,0,y,2y), (0,0,2y,y)\ )^T$ for $0 \leq y \leq 2$.

3.60 Theorem [47] $N(38) \geq 4$. Consider the matrix:

$$\begin{pmatrix} - & 10 & 1 & 2 & 6 & 3 & 22 & 5 & 7 & 9 & 14 & 18 & 28 \\ 0 & 1 & 10 & 20 & 23 & 30 & 35 & 13 & 33 & 16 & 29 & 32 & 21 \\ 0 & 26 & 26 & 15 & 8 & 4 & 17 & 19 & 34 & 12 & 31 & 24 & 25 \\ 10 & - & 10 & 6 & 2 & 22 & 3 & 7 & 5 & 14 & 9 & 28 & 18 \\ 1 & 0 & 26 & 23 & 20 & 35 & 30 & 33 & 13 & 29 & 16 & 21 & 32 \\ 26 & 0 & 1 & 8 & 15 & 17 & 4 & 34 & 19 & 31 & 12 & 25 & 24 \end{pmatrix}.$$

Each column $(a,b,c,d,e,f)^T$ is replaced by columns $(a,b,c,d,e,f)^T$, $(b,c,a,f,d,e)^T$, and $(c,a,b,e,f,d)^T$ to obtain a $(37,6;1,1;1)$ quasi-difference matrix (QDM).

3.61 **Theorem** [38] $N(39) \geq 5$. Consider the matrices

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 23 & 13 & 5 & 12 & 11 \\ 25 & 11 & 22 & 34 & 23 & 6 \\ 13 & 4 & 20 & 17 & 15 & 29 \\ 27 & 21 & 8 & 16 & 19 & 26 \\ 16 & 19 & 34 & 38 & 26 & 21 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 \\ 16 \\ 22 \\ 17 \\ 38 \\ 23 \end{pmatrix}.$$

Replace each column $C = (a,b,c,d,e,f)^T$ of A_1 by the three columns C, $t(C)$, and $t(t(C))$, where $t(C) = (16c, 16a, 16b, 16f, 16d, 16e)^T$. Then multiply the resulting 18 columns and the column of A_2 by 1 and -1. Finally, append a column of zeros. The result is a difference matrix over $\mathbb{Z}_{39}$.

3.62 **Theorem** [26] $N(40) \geq 7$. Let ω be a primitive root in $\mathbb{F}_{2^3}$ satisfying $\omega^3 = \omega + 1$. Let

$$A = \begin{pmatrix} (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) \\ (0,\emptyset) & (1,\emptyset) & (2,2) & (3,2) & (4,2) & (2,\emptyset) & (3,\emptyset) & (4,\emptyset) & (0,2) & (1,2) \\ (0,\emptyset) & (2,5) & (4,5) & (1,2) & (3,6) & (3,4) & (0,0) & (2,1) & (4,1) & (1,6) \\ (0,\emptyset) & (3,4) & (1,4) & (4,0) & (2,5) & (3,\emptyset) & (1,0) & (4,1) & (2,2) & (0,3) \\ (0,\emptyset) & (4,6) & (3,\emptyset) & (2,3) & (1,4) & (2,1) & (1,\emptyset) & (0,4) & (4,0) & (3,2) \\ (0,\emptyset) & (1,2) & (4,6) & (4,4) & (1,0) & (0,6) & (2,3) & (3,6) & (3,5) & (2,5) \\ (1,\emptyset) & (0,3) & (1,2) & (4,5) & (4,\emptyset) & (2,3) & (0,0) & (2,2) & (3,0) & (3,\emptyset) \\ (4,\emptyset) & (1,3) & (0,0) & (1,1) & (4,0) & (3,1) & (2,5) & (0,\emptyset) & (2,1) & (3,\emptyset) \end{pmatrix} \text{ and}$$

$$Y = \begin{pmatrix} \emptyset & 0 & 1 & 6 & 5 & 4 & 3 & 2 \\ \emptyset & 1 & 2 & 0 & 6 & 5 & 4 & 3 \end{pmatrix},$$

where the second coordinates of entries in A, and the entries in Y are interpreted as follows. Entry i denotes ω^i, and entry $\emptyset$ denotes the zero element of $\mathbb{F}_{2^3}$. Now if $A(x,y) = (a,b)$, let $\tau_i(A(x,y)) = (a, b + Y(i,x))$ for $i = 1,2$. The group generated by τ_1 and τ_2 has order 4. Developing columns of A under the action of this group yields 40 columns, which form a difference matrix over $\mathbb{F}_5 \times \mathbb{F}_{2^3}$.

3.63 **Theorem** [6] $N(42) \geq 5$. Consider the matrices:

$$A_1 = \begin{pmatrix} - & - & - \\ 0 & 0 & 0 \\ 18 & 11 & 5 \\ 26 & 10 & 30 \\ 20 & 3 & 33 \\ 5 & 25 & 24 \\ 17 & 4 & 22 \end{pmatrix} \quad A_2 = \begin{pmatrix} - \\ 0 \\ 4 \\ 23 \\ 23 \\ 4 \\ 0 \end{pmatrix}.$$

The seven cyclic shifts of the columns of $(A_1 | -A_1 | A_2)$ give a $(35,7;1,1;7)$ QDM.

3.64 **Theorem** [6] $N(44) \geq 5$. Consider the array over $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{11}$:

$$\begin{pmatrix} 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 \\ 114 & 014 & 117 & 106 & 119 & 012 & 015 & 011 \\ 106 & 013 & 100 & 019 & 111 & 014 & 119 & 109 \\ 116 & 119 & 012 & 110 & 010 & 115 & 004 & 009 \\ 109 & 002 & 001 & 102 & 007 & 116 & 110 & 107 \\ 101 & 106 & 113 & 015 & 005 & 013 & 010 & 110 \end{pmatrix}.$$

Replace each column $C = [(x_1,y_1,z_1),(x_2,y_2,z_2),...,(x_5,y_5,z_5),(x_6,y_6,z_6)]^T$ by the five columns $t^i(C)$, where $t(C) = [(x_5,y_5,5z_5),\ (x_1,y_1,5z_1),\ (x_2,y_2,5z_2),\ (x_3,y_3,5z_3),$

$(x_4, y_4, 5z_4)$, $(x_6, y_6, 5z_6)]^T$. Append the four columns $[(x, y, z)$, $(x, y, 5z)$, $(x, y, 3z)$, $(x, y, 4z)$, $(x, y, 9z)$, $(0, 0, 0)]^T$ for $(x, y, z) =$ (0,0,0), (1,0,1), (1,1,2) and (0,0,8), giving a (44,6,1) difference matrix.

3.65 Theorem [10] $N(45) \geq 6$. Consider the matrices:

$$A_1 = \begin{pmatrix} 000 \\ 000 \\ 000 \\ 000 \\ 000 \\ 000 \\ 000 \end{pmatrix} \quad A_2 = \begin{pmatrix} 221 & 311 & 412 & 401 & 011 & 021 & 322 \\ 121 & 422 & 120 & 410 & 311 & 300 & 212 \\ 411 & 221 & 320 & 120 & 210 & 100 & 321 \\ 010 & 211 & 400 & 002 & 422 & 322 & 122 \\ 312 & 210 & 022 & 421 & 021 & 201 & 112 \\ 211 & 122 & 301 & 210 & 100 & 421 & 110 \\ 000 & 000 & 000 & 000 & 000 & 000 & 000 \end{pmatrix}.$$

Let A_3 be the array over $\mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ obtained by interchanging the following pairs of rows in A_2, 1 and 6, 2 and 5, 3 and 4, while leaving row 7 unaltered. Replace each column $[(x_1, y_1, z_1), (x_2, y_2, z_2), \ldots (x_7, y_7, z_7)]^T$ of $[A_1|A_2|A_3]$ by the following three columns for $i = 0, 1, 2$: $[(x_1, y_1, z_1 + i), (x_2, y_2 + 2i, z_2), (x_3, y_3 + i, z_3 + 2i), (x_4, y_4 + 2i, z_4 + i), (x_5, y_5 + i, z_5), (x_6, y_6, z_6 + 2i), (x_7, y_7, z_7)]^T$. This gives a (45,7,1) difference matrix.

3.66 Theorem $N(46) \geq 4$, from the existence of a $V(4, 9)$ vector (Table VI.17.54).

3.67 Theorem [25] $N(48) \geq 8$. This follows from existence of a $(48, 9, 1)$ difference matrix over $\mathbb{Z}_3 \times \mathbb{F}_{2^4}$. In what follows, ω is a primitive element of $\mathbb{F}_{2^4}$ satisfying $\omega^4 = \omega + 1$, and for the second coordinates of all entries, ω^i is written as i. The first 12 columns of this matrix are as follows:

$$\begin{pmatrix} (0,4) & (2,2) & (2,2) & (0,13) & (0,4) & (2,13) & (0,1) & (0,7) & (1,7) & (2,2) & (0,6) & (2,9) \\ (2,7) & (0,9) & (2,7) & (2,3) & (0,3) & (0,9) & (1,12) & (0,6) & (0,12) & (2,14) & (2,7) & (0,11) \\ (2,12) & (2,12) & (0,14) & (0,14) & (2,8) & (0,8) & (0,2) & (1,2) & (0,11) & (0,1) & (2,4) & (2,12) \\ (1,3) & (0,2) & (0,10) & (0,14) & (0,9) & (1,3) & (0,12) & (2,13) & (2,1) & (2,9) & (2,0) & (1,7) \\ (0,0) & (1,8) & (0,7) & (1,8) & (0,4) & (0,14) & (2,6) & (0,2) & (2,3) & (1,12) & (2,14) & (2,5) \\ (0,12) & (0,5) & (1,13) & (0,4) & (1,13) & (0,9) & (2,8) & (2,11) & (0,7) & (2,10) & (1,2) & (2,4) \\ (1,12) & (2,0) & (1,14) & (0,6) & (1,9) & (0,14) & (1,4) & (0,5) & (1,8) & (1,3) & (2,1) & (1,1) \\ (1,4) & (1,2) & (2,5) & (0,4) & (0,11) & (1,14) & (1,13) & (1,9) & (0,10) & (1,6) & (1,8) & (2,6) \\ (2,10) & (1,9) & (1,7) & (1,4) & (0,9) & (0,1) & (0,0) & (1,3) & (1,14) & (2,11) & (1,11) & (1,13) \end{pmatrix}$$

and the others are obtained by adding the following 3 vectors to these columns: $((0, 12 + u)$, $(0, 2 + u)$, $(0, 7 + u)$, $(0, u)$, $(0, 5 + u)$, $(0, 10 + u)$, $(0, 3 + u)$, $(0, 8 + u)$, $(0, 13 + u))^T$ for $u = 0$, 1, and 4.

3.68 Theorem $N(50) \geq 6$. This follows from the existence of a $V(6, 7)$ vector (Table VI.17.54).

3.69 Theorem [38] $N(51) \geq 5$.

Let A be the array on the right with entries from $\mathbb{Z}_{51}$. Replace each column of $[A| - A]$ by its five cyclic shifts. Then append a row and column of zeros. The result is a (51,6,1) difference matrix.

$$\begin{pmatrix} 5 & 33 & 29 & 30 & 1 \\ 8 & 3 & 47 & 10 & 13 \\ 14 & 27 & 6 & 12 & 28 \\ 9 & 16 & 44 & 49 & 11 \\ 34 & 32 & 36 & 26 & 20 \end{pmatrix}$$

3.70 Theorem [6] $N(52) \geq 5$. Consider arrays over $\mathbb{F}_4 \times \mathbb{Z}_{13}$:

$$A_1 = \begin{pmatrix} (0,0) & (0,0) & (0,0) & (0,0) & (0,0) \\ (z^2,10) & (0,7) & (1,10) & (z,10) & (z^2,3) \\ (z,10) & (z^2,2) & (1,11) & (z,2) & (z^2,7) \\ (z,8) & (z^2,12) & (0,10) & (z^2,11) & (z^2,6) \\ (1,2) & (0,2) & (z^2,8) & (z,3) & (z,7) \\ (1,6) & (z,12) & (0,7) & (z^2,6) & (z,2) \end{pmatrix} \quad A_2 = \begin{pmatrix} (1,1) & (z^2,11) \\ (z,3) & (1,7) \\ (z^2,9) & (z,8) \\ (1,4) & (z^2,3) \\ (z,12) & (1,9) \\ (z^2,10) & (z,1) \end{pmatrix}.$$

For a column $C = ((x_1, y_1), (x_2, y_2) \ldots (x_6, y_6))^T$, let $t_1(C) = ((z \cdot x_3, 3 \cdot y_3), (z \cdot x_1, 3 \cdot y_1), (z \cdot x_2, 3 \cdot y_2), (z \cdot x_6, 3 \cdot y_6), (z \cdot x_4, 3 \cdot y_4), (z \cdot x_5, 3 \cdot y_5))^T$, and $t_2(C) = ((x_3, y_3), (x_1, y_1), (x_2, y_2), (x_5, y_5), (x_6, y_6), (x_4, y_4))^T$. (Here $z^2 = z + 1$). Apply the group of order 9 generated by t_1, t_2 to the columns of A_1 to give 45 columns; then apply the group of order 3 generated by t_2 to the columns of A_2 to give another 6 columns. Finally append a column whose entries all equal (0,0). This gives a (52,6,1) difference matrix.

3.71 **Theorem** [6] $N(54) \geq 5$. Consider the matrices:

$$A_1 = \begin{pmatrix} - & - & - & - \\ 0 & 0 & 0 & 0 \\ 1 & 27 & 16 & 7 \\ 24 & 40 & 1 & 35 \\ 10 & 30 & 22 & 44 \\ 5 & 18 & 14 & 33 \\ 30 & 16 & 33 & 27 \end{pmatrix} \quad A_2 = \begin{pmatrix} - \\ 0 \\ 3 \\ 7 \\ 7 \\ 3 \\ 0 \end{pmatrix}.$$

The seven cyclic shifts of the columns of $(A_1| - A_1|A_2)$ give a $(45, 9; 1, 1; 7)$ QDM.

3.72 **Theorem** [2161] $N(55) \geq 6$. Consider the array over $\mathbb{Z}_{55}$:

$$\begin{pmatrix} 1 & 7 & 14 & 19 & 28 & 33 & 40 & 46 & 50 \\ 2 & 13 & 25 & 38 & 52 & 12 & 20 & 32 & 45 \\ 39 & 6 & 8 & 26 & 24 & 51 & 11 & 34 & 37 \\ 54 & 48 & 41 & 36 & 27 & 22 & 15 & 9 & 5 \\ 53 & 42 & 30 & 17 & 3 & 43 & 35 & 23 & 10 \\ 16 & 49 & 47 & 29 & 31 & 4 & 44 & 21 & 18 \end{pmatrix}.$$

Replace each column by its six cyclic shifts, then append a row and column of zeros. The result is a $(55, 7, 1)$ difference matrix.

3.73 **Theorem** [2, 1608] $N(56) \geq 7$. Let ω be a primitive element of $\mathbb{F}_8$ satisfying $\omega^3 = \omega + 1$. Consider the 8×8 array over $\mathbb{F}_8 \times \mathbb{Z}_7$:

$$\begin{pmatrix} (0,0) & (\omega^0,0) & (\omega^1,0) & (\omega^2,0) & (\omega^3,0) & (\omega^4,0) & (\omega^5,0) & (\omega^6,0) \\ (0,1) & (\omega^1,6) & (\omega^2,1) & (\omega^3,1) & (\omega^4,6) & (\omega^5,1) & (\omega^6,6) & (\omega^0,6) \\ (0,4) & (\omega^2,3) & (\omega^3,4) & (\omega^4,4) & (\omega^5,3) & (\omega^6,4) & (\omega^0,3) & (\omega^1,3) \\ (0,2) & (\omega^3,5) & (\omega^4,2) & (\omega^5,2) & (\omega^6,5) & (\omega^0,2) & (\omega^1,5) & (\omega^2,5) \\ (0,2) & (\omega^4,5) & (\omega^5,2) & (\omega^6,2) & (\omega^0,5) & (\omega^1,2) & (\omega^2,5) & (\omega^3,5) \\ (0,4) & (\omega^5,3) & (\omega^6,4) & (\omega^0,4) & (\omega^1,3) & (\omega^2,4) & (\omega^3,3) & (\omega^4,3) \\ (0,1) & (\omega^6,6) & (\omega^0,1) & (\omega^1,1) & (\omega^2,6) & (\omega^3,1) & (\omega^4,6) & (\omega^5,6) \\ (1,0) & (1,0) & (1,0) & (1,0) & (1,0) & (1,0) & (1,0) & (1,0) \end{pmatrix}.$$

Each column $C = [(x_1, y_1)(x_2, y_2)(x_3, y_3)(x_4, y_4)(x_5, y_5)(x_6, y_6)(x_7, y_7)(x_8, y_8)]^T$ is replaced by the 7 columns $t^i(C)$ $(0 \leq i \leq 6)$ where $t(C) = [(\omega x_7, y_7)\ (\omega x_1, y_1)\ (\omega x_2, y_2)\ (\omega x_3, y_3)\ (\omega x_4, y_4)\ (\omega x_5, y_5)\ (\omega x_6, y_6)\ (\omega x_8, y_8)]^T$. The result is a (56,8,1) difference matrix over $\mathbb{F}_8 \times \mathbb{Z}_7$.

3.74 **Theorem** [6] $N(62) \geq 5$. Consider the matrices:

$$A_1 = \begin{pmatrix} 0 & - & - & - \\ 17 & 0 & 0 & 0 \\ 29 & 28 & 35 & 23 \\ 36 & 50 & 5 & 33 \\ 31 & 2 & 43 & 30 \\ 16 & 47 & 44 & 51 \\ 41 & 11 & 1 & 17 \end{pmatrix} \quad A_2 = \begin{pmatrix} - & - \\ 1 & 11 \\ 3 & 19 \\ 7 & 33 \\ 34 & 33 \\ 30 & 19 \\ 28 & 11 \end{pmatrix}.$$

The seven cyclic shifts of the columns of $(A_1| - A_1|A_2)$ give a $(54, 8; 1, 1; 7)$ QDM.

3.75 Theorem [27] $N(75) \geq 7$. Consider the matrices over $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$:

$$A_1 = \begin{pmatrix} 000 \\ 000 \\ 000 \\ 000 \\ 000 \\ 000 \\ 000 \\ 000 \end{pmatrix} \quad A_2 = \begin{pmatrix} 200 & 000 & 000 & 100 & 000 & 100 & 100 \\ 023 & 144 & 113 & 104 & 243 & 003 & 144 \\ 132 & 211 & 140 & 030 & 104 & 241 & 012 \\ 024 & 131 & 202 & 001 & 240 & 122 & 000 \\ 112 & 223 & 031 & 142 & 210 & 143 & 244 \\ 014 & 044 & 241 & 130 & 131 & 200 & 240 \\ 044 & 201 & 233 & 232 & 002 & 212 & 142 \\ 242 & 241 & 231 & 122 & 130 & 002 & 242 \end{pmatrix}.$$

Let A_3 be the matrix obtained by interchanging rows i and $9-i$ (for $1 \leq i \leq 4$) in A_2. The required $(75, 8, 1)$ difference matrix is then obtained by adding the following vectors to the 15 columns of $[A_1|A_2|A_3]$: $[(0,0,x),\ (0,x,0),\ (0,x,2x),\ (0,2x,2x),\ (0,3x,3x),\ (0,4x,3x),\ (0,4x,0),\ (0,0,4x)]^T$ for $0 \leq x \leq 4$.

3.76 Theorem [2, 26] $N(80) \geq 9$. Let ω be a primitive root in $\mathbb{F}_{2^4}$ satisfying $\omega^4 = \omega + 1$. Let

$$A = \begin{pmatrix} (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) & (0,\emptyset) \\ (0,\emptyset) & (1,\emptyset) & (2,3) & (3,\emptyset) & (4,3) & (2,\emptyset) & (3,3) & (4,\emptyset) & (0,3) & (1,3) \\ (0,\emptyset) & (2,8) & (4,6) & (1,3) & (3,3) & (3,13) & (0,13) & (2,6) & (4,14) & (1,12) \\ (0,\emptyset) & (3,11) & (1,0) & (4,9) & (2,0) & (3,7) & (1,8) & (4,10) & (2,10) & (0,11) \\ (0,\emptyset) & (4,8) & (3,14) & (2,14) & (1,12) & (2,10) & (1,10) & (0,3) & (4,5) & (3,8) \\ (0,\emptyset) & (1,8) & (4,14) & (4,12) & (1,1) & (0,1) & (2,8) & (3,12) & (3,6) & (2,1) \\ (1,\emptyset) & (0,6) & (1,1) & (4,4) & (4,13) & (2,6) & (0,14) & (2,9) & (3,0) & (3,3) \\ (4,\emptyset) & (1,9) & (0,7) & (1,1) & (4,8) & (3,5) & (2,14) & (0,0) & (2,\emptyset) & (3,0) \\ (4,\emptyset) & (4,6) & (1,2) & (0,\emptyset) & (1,13) & (3,8) & (3,2) & (2,0) & (0,14) & (2,\emptyset) \\ (1,\emptyset) & (4,9) & (4,1) & (1,0) & (0,4) & (2,5) & (3,\emptyset) & (3,5) & (2,\emptyset) & (0,\emptyset) \end{pmatrix}$$

$$\text{and let } Y = \begin{pmatrix} \emptyset & 0 & 1 & 14 & 12 & 7 & 2 & 11 & 3 & 6 \\ \emptyset & 1 & 2 & 0 & 13 & 8 & 3 & 12 & 4 & 7 \\ \emptyset & 2 & 3 & 1 & 14 & 9 & 4 & 13 & 5 & 8 \end{pmatrix},$$

where the second coordinates of entries in A and the entries in Y are interpreted as follows. Entry i denotes ω^i, and entry $\emptyset$ denotes the zero element of $\mathbb{F}_{2^4}$. Now if $A(x,y) = (a,b)$, let $\tau_i(A(x,y)) = (a, b + Y(i,x))$ for $i = 1,2,3$. The group generated by τ_1 and τ_2 has order 8. Developing columns of A under the action of this group yields 80 columns, which form a difference matrix over $\mathbb{F}_5 \times \mathbb{F}_{2^4}$.

3.5 Complete Sets of Order 9

3.77 Remarks Owens and Preece [1710] determined the 19 equivalence classes of complete sets of MOLS of order 9, using a definition of equivalence that permits reordering the rows and columns of all squares together, and the symbols of each square individually. There are four nonisomorphic projective planes: the desarguesian plane Φ, the translation plane Ω, the dual translation plane Ω^D, and the Hughes plane Ψ. See §VII.2.

3.78 Table The 19 inequivalent complete sets of order 9. For each, the eight orthogonal latin squares are given, and under each is provided a name for the isotopy class to which the square belongs (see [1710]), and the number of intercalates in the square.

For each set, the plane from which it arises is given along with some information about the manner in which the complete set is formed. Here, ℓ_∞ is the line at infinity, t is the translation line of Ω, and T is the translation point of Ω^D. In the Hughes plane, lines are classified as real or complex [1819]. Details are given in [1710].

Set 1 (Plane Φ)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231564897	456789123	645978312	897231564	312645978	564897231	789123456	978312645
312645978	789123456	897231564	645978312	231564897	978312645	456789123	564897231
456789123	312645978	978312645	564897231	789123456	645978312	231564897	897231564
564897231	645978312	231564897	312645978	978312645	789123456	897231564	456789123
645978312	978312645	456789123	789123456	897231564	231564897	564897231	312645978
789123456	231564897	564897231	978312645	456789123	897231564	312645978	645978312
897231564	564897231	789123456	456789123	645978312	312645978	978312645	231564897
978312645	897231564	312645978	231564897	564897231	456789123	645978312	789123456
a,0	a,0	a,0	a,0	a,0	a,0	a,0	a,0
Set 2 (Plane Ω, $t = \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231564897	456789123	645978312	564897231	312645978	789123456	897231564	978312645
312645978	789123456	897231564	978312645	231564897	456789123	645978312	564897231
456789123	312645978	564897231	897231564	789123456	231564897	978312645	645978312
564897231	645978312	789123456	312645978	978312645	897231564	456789123	231564897
645978312	978312645	312645978	456789123	897231564	564897231	231564897	789123456
789123456	231564897	978312645	645978312	456789123	312645978	564897231	897231564
897231564	564897231	231564897	789123456	645978312	978312645	312645978	456789123
978312645	897231564	456789123	231564897	564897231	645978312	789123456	312645978
a,0	a,0	a,0	a,0	a,0	a,0	a,0	a,0
Set 3 (Plane Ω, $t = \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
312645978	645978312	564897231	456789123	231564897	978312645	789123456	897231564
231564897	897231564	978312645	789123456	312645978	564897231	456789123	645978312
789123456	978312645	231564897	564897231	456789123	897231564	645978312	312645978
978312645	231564897	645978312	897231564	564897231	456789123	312645978	789123456
897231564	456789123	789123456	231564897	645978312	312645978	978312645	564897231
456789123	564897231	312645978	978312645	789123456	645978312	897231564	231564897
645978312	789123456	456789123	312645978	897231564	231564897	564897231	978312645
564897231	312645978	897231564	645978312	978312645	789123456	231564897	456789123
a,0	a,0	a,0	a,0	a,0	a,0	a,0	a,0
Set 4 (Plane Ω, $t \neq \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231564897	456789123	645978312	564897231	312645978	789123456	897231564	978312645
312645978	789123456	897231564	978312645	231564897	456789123	645978312	564897231
498732156	312867594	576394821	849521367	765189432	231975648	984613275	657248913
587293641	694538217	758162493	312974856	946817325	875341962	469725138	231689574
679328514	967214835	312589647	485763192	854971263	548692371	231847956	796135428
765189432	231975648	984613275	657248913	498732156	312867594	576394821	849521367
854971263	548692371	231847956	796135428	679328514	967214835	312589647	485763192
946817325	875341962	469725138	231689574	587293641	694538217	758162493	312974856
b_R,48	b_R,48	b_R,48	b_R,48	b_R,48	b_R,48	b_R,48	b_R,48
Set 5 (Plane Ω, $t \neq \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231987654	789165423	897541362	978614235	312879546	456723198	645238917	564392871
312879546	456723198	645238917	564392871	231987654	789165423	897541362	978614235
456723198	231987654	978614235	645238917	789165423	312879546	564392871	897541362
564392871	897541362	456723198	231987654	978614235	645238917	789165423	312879546
645238917	564392871	231987654	789165423	897541362	978614235	312879546	456723198
789165423	312879546	564392871	897541362	456723198	231987654	978614235	645238917
897541362	978614235	312879546	456723198	645238917	564392871	231987654	789165423
978614235	645238917	789165423	312879546	564392871	897541362	456723198	231987654
b_C,48	b_C,48	b_C,48	b_C,48	b_C,48	b_C,48	b_C,48	b_C,48
Set 6 (Plane Ω, $t \neq \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
312987654	978324561	789263145	897532416	231645978	645891327	564719832	456178293
231879546	564918273	456197328	645781932	312564897	897243615	978632451	789325164
756123498	687231945	214978653	938645271	465789132	579312864	892564317	341897526
964312875	215789634	837645912	479123568	546897321	782564193	351978246	698231457
845231967	739645128	598312476	216897354	654978213	361789542	487123695	972564831
489765123	846597312	371829564	562314897	798132456	954678231	635241978	217983645
697548312	452163897	965784231	381279645	879321564	218937456	746895123	534612978
578694231	391872456	642531897	754968123	987213645	436125978	219387564	865749312
b_S,48	c,32	c,32	c,32	a,0	c,32	c,32	c,32

Set 7 (Plane Ω^D, $T \in \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231564897	456789123	645978312	564897231	312645978	789123456	897231564	978312645
312645978	789123456	897231564	978312645	231564897	456789123	645978312	564897231
456789123	312645978	978312645	645978312	789123456	231564897	564897231	897231564
564897231	897231564	456789123	312645978	978312645	645978312	789123456	231564897
645978312	564897231	312645978	789123456	897231564	978312645	231564897	456789123
789123456	231564897	564897231	897231564	456789123	312645978	978312645	645978312
897231564	978312645	231564897	456789123	645978312	564897231	312645978	789123456
978312645	645978312	789123456	231564897	564897231	897231564	456789123	312645978
a,0	a,0	a,0	a,0	a,0	a,0	a,0	a,0
Set 8 (Plane Ω^D, $T \in \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231564897	765189432	854971263	946817325	312645978	498732156	679328514	587293641
312645978	498732156	679328514	587293641	231564897	765189432	854971263	946817325
456789123	231975648	548692371	875341962	789123456	312867594	967214835	694538217
564897231	657248913	796135428	231689574	978312645	849521367	485763192	312974856
645978312	984613275	231847956	469725138	897231564	576394821	312589647	758162493
789123456	312867594	967214835	694538217	456789123	231975648	548692371	875341962
897231564	576394821	312589647	758162493	645978312	984613275	231847956	469725138
978312645	849521367	485763192	312974856	564897231	657248913	796135428	231689574
a,0	a,0	a,0	a,0	a,0	a,0	a,0	a,0
Set 9 (Plane Ω^D, $T \in \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
312645978	576918243	485197326	694781532	231564897	849273615	967832451	758329164
231564897	984327561	796283145	875932416	312645978	657891324	548719632	469178253
789123456	648231975	371548692	962875341	456789123	594312867	835967214	217694538
978312645	391765824	842679513	457123968	564897231	736984152	219548376	685231497
897231564	752849136	569312478	381694257	645978312	218765943	476123895	934587621
456789123	867594312	214835967	538217694	789123456	975648231	692371548	341962875
645978312	439182657	958764231	216349875	897231564	361527498	784695123	572813946
564897231	215673498	637921854	749568123	978312645	482139576	351284967	896745312
a,0	d,72	d,72	d,72	a,0	d,72	d,72	d,72
Set 10 (Plane Ω^D, $T \notin \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231879546	756123498	845231967	964312875	312987654	489765123	697548312	578694231
312987654	489765123	697548312	578694231	231879546	756123498	845231967	964312875
489765123	231879546	578694231	845231967	756123498	312987654	964312875	697548312
578694231	697548312	756123498	231879546	964312875	845231967	489765123	312987654
697548312	964312875	231879546	489765123	845231967	578694231	312987654	756123498
756123498	312987654	964312875	697548312	489765123	231879546	578694231	845231967
845231967	578694231	312987654	756123498	697548312	964312875	231879546	489765123
964312875	845231967	489765123	312987654	578694231	697548312	756123498	231879546
b_S,48	b_S,48	b_S,48	b_S,48	b_S,48	b_S,48	b_S,48	b_S,48
Set 11 (Plane Ω^D, $T \notin \ell_\infty$)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
312879546	675948213	584697321	496785132	231564897	948213675	769132458	857321964
231987654	894321567	976213845	785132496	312645978	567894321	458769132	649578213
789165423	546297831	231549678	967813245	498732156	654378912	875921364	312684597
978614235	231865974	849371562	654928317	587293641	796182453	312547896	465739128
897541362	758139426	465782193	231674958	679328514	312965847	546893271	984217635
456723198	987612345	312864957	548397621	765189432	879531264	694278513	231945876
645238917	469783152	798125436	312569874	854971263	231647598	987314625	576892341
564392871	312574698	657938214	879241563	946817325	485729136	231685948	798163452
b_C,48	e,24	e,24	e,24	b_R,48	e,24	e,24	e,24
Set 12 (Plane Ψ, real ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231564897	456789123	564897231	645978312	312645978	789123456	978312645	897231564
312645978	789123456	978312645	897231564	231564897	456789123	564897231	645978312
456789123	312897564	897564312	564312897	789123456	231978645	645231978	978645231
564897231	645231897	312978456	789564123	978312645	897645312	231789564	456123978
645978312	978564231	456123897	312789645	897231564	564312978	789645123	231897456
789123456	231978645	645231978	978645231	456789123	312897564	897564312	564312897
897231564	564312978	789645123	231897456	645978312	978564231	456123897	312789645
978312645	897645312	231789564	456123978	564897231	645231897	312978456	789564123
a,0	f_S,36	f_S,36	f_S,36	a,0	f_S,36	f_S,36	f_S,36

Set 13 (Plane Ψ, real ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
789123456	897231564	978312645	231564897	456789123	645978312	564897231	312645978
456789123	645978312	564897231	312645978	789123456	897231564	978312645	231564897
231978645	564312978	897645312	978231456	312564897	456897123	789123564	645789231
645231978	789645123	231789564	897123645	564978231	978312456	312564897	456897312
978645231	231897456	456123978	789312564	897231645	312564897	645789312	564978123
312897564	978564231	645231897	564789312	231645978	789123645	456978123	897312456
564312897	312789645	789564123	456978231	645897312	231645978	897231456	978123564
897564312	456123897	312978456	645897123	978312564	564789231	231645978	789231645
f_C,36	f_C,36	f_C,36	g_R,0	h_R,0	h_R,0	h_R,0	g_R,0
Set 14 (Plane Ψ, real ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
498732156	679328514	587293641	231645978	756189423	845971362	964817235	312564897
765189432	854971263	946817325	312564897	489723156	697238514	578392641	231645978
312645978	967832451	694781532	879213645	231597864	458369127	785124396	546978213
849273615	485197326	312645978	798321564	567834291	976512843	231968457	654789132
576918243	312645978	758329164	987132456	894261537	231784695	649573812	465897321
231564897	548719632	875932416	654897321	312678945	769143258	496285173	987321564
984327561	231564897	469178253	546789132	675942318	312895476	857631924	798213645
657891324	796283145	231564897	465978213	948315672	584627931	312749568	879132456
f_R,36	f_R,36	f_R,36	g_C,0	h_C,0	h_C,0	h_C,0	g_C,0
Set 15 (Plane Ψ, real ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
312564897	849327561	967283145	758932416	231645978	675891234	584719623	496178352
231645978	657918243	548197326	469781532	312564897	894372615	976823451	785239164
546897213	465789132	382514697	871325964	798132456	957648321	639271548	214963875
654978132	372561894	791632458	546897321	987213645	438129576	215384967	869745213
465789321	981243675	654978213	392164857	879321564	216537498	748695132	537812946
987321645	798132456	236845971	614578293	465789132	549213867	852967314	371694528
798213456	516894327	879321564	235649178	654978213	381765942	467132895	942587631
879132564	234675918	415769832	987213645	546897321	762984153	391548276	658321497
g_S,0	g_S,0	g_S,0	g_S,0	a,0	d,72	d,72	d,72
Set 16 (Plane Ψ, real ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
489723156	314579628	678931245	962345871	756198432	241687593	597812364	835264917
756189423	271863954	864397512	538614297	489732165	317925846	945278631	692541378
312948675	796185243	987524361	845732916	231867594	469273158	654391827	578619432
975612348	639748512	452179836	381297654	567384921	894531267	218965473	746823195
648375912	567294831	215743698	479168523	894621357	936812475	782539146	351987264
231894567	485327196	546218973	697581432	312975648	758169324	879643215	964732851
867531294	948612375	391865427	754923168	675249813	582794631	436187952	219378546
594267831	852931467	739682154	216879345	948513276	675348912	361724598	487195623
h_S,0	h_S,0	d,72	d,72	h_S,0	h_S,0	d,72	d,72
Set 17 (Plane Ψ, complex ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231645978	879213564	798321456	987132645	312564897	654978321	465789213	546897132
312564897	546897213	654978132	465789321	231645978	987321645	879132564	798213456
489723156	312948675	975612348	648375912	756189423	231894567	594267831	867531294
578392641	457639128	312785964	896241573	964817235	749163852	231578496	685924317
697238514	784125936	569843271	312697458	845971362	476582193	958314627	231769845
765189432	231564897	846297513	579813264	498732156	312645978	687921345	954378621
854971263	965782341	487139625	231564897	679328514	598217436	746893152	312645978
946817325	698371452	231564897	754928136	587293641	865739214	312645978	479182563
i_R,24	i_R,24	i_R,24	i_R,24	i_R,24	i_R,24	i_R,24	i_R,24
Set 18 (Plane Ψ, complex ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
231879654	765132498	946213875	854321967	312987546	489765132	578694321	697548213
312987546	489765132	578694321	697548213	231879654	765132498	946213875	854321967
465732198	572891364	854327916	319684572	798165423	637918245	281549637	946273851
546293871	318547926	692178453	765932148	987614235	854329617	439781562	271865394
654328917	946283571	317965248	482719635	879541362	291674853	765832194	538197426
798165423	637918245	281549637	946273851	465732198	572891364	854327916	319684572
879541362	291674853	765832194	538197426	654328917	946283571	317965248	482719635
987614235	854329617	439781562	271865394	546293871	318547926	692178453	765932148
i_C,24	i_C,24	i_C,24	i_C,24	i_C,24	i_C,24	i_C,24	i_C,24

Set 19 (Plane Ψ, complex ℓ_∞)							
123456789	123456789	123456789	123456789	123456789	123456789	123456789	123456789
312987546	576894312	694578123	485769231	231645897	948231675	857123964	769312458
231879654	894312567	785231496	976123845	312564978	657948231	469785312	548697123
765132498	319527846	972845361	548391627	456789132	281673954	694218573	837964215
946213875	657138294	318962547	892675413	564897321	739584162	271349658	485721936
854321967	782649135	469713852	317284596	645978213	576192348	938567421	291835674
489765132	945281673	537694218	251837964	798123456	864319527	316972845	672548391
697548213	438765921	241389675	764912358	879231564	315827496	582694137	956173842
578694321	261973458	856127934	639548172	987312645	492765813	745831296	314289567
i_S,24	j,24	j,24	j,24	k,0	j,24	j,24	j,24

3.6 MOLS of Side n ≤ 10,000

3.79 **Remark** Table 3.87 updates a similar table by Brouwer [334] from 1979 as well as Table II.2.72 in the first edition of the *Handbook* from 1996. This table has been produced using a program that attempts to incorporate all existing constructions for sets of MOLS. The constructions used and the program developed are described in [543]. Tables 3.81, 3.83, 3.86, and 3.88 are derived from information in Table 3.87.

3.80 n_k is the largest order for which the existence of k MOLS is unknown.

3.81 **Table** n_k for $k \leq 15$ and $k = 30$.

k	n_k	k	n_k	k	n_k	k	n_k	k	n_k
2	6	3	10	4	22	5	60	6	74
7	570	8	2766	9	3678	10	5804	11	7222
12	7286	13	7288	14	7874	15	8360	30	52502

3.82 i_k is the largest order for which the existence of k idempotent MOLS is unknown.

3.83 **Table** i_k for $k \leq 15$.

k	i_k	k	i_k	k	i_k	k	i_k	k	i_k
2	6	3	10	4	26	5	60	6	98
7	702	8	2766	9	3678	10	5804	11	7222
12	7286	13	7618	14	7874	15	10618		

3.84 **Remark** In [2] it is shown that the only possible exceptions for 15 idempotent MOLS of orders exceeding 9718 are 10606 and 10618. Indeed writing $10606 = 421 \cdot 25 + (81 = 3 \cdot 27)$, one can establish that 10606 is not an exception.

3.85 o_k is the largest *odd* order for which the existence of k MOLS is unknown.

3.86 **Table** o_k for $k \leq 15$.

k	o_k	k	o_k	k	o_k	k	o_k	k	o_k
2	–	3	–	4	–	5	15	6	51
7	335	8	1263	9	1935	10	2607	11	3471
12	3505	13	3565	14	3603	15	3603		

3.87 **Table** Lower bounds on $N(n)$, the number of MOLS of side n. Italicized entries are lower bounds on $N(1^n)$ (all the MOLS are idempotent), when the best current bound matches the lower bound on $N(n)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	∞	∞	1	2	3	4	1	6	7	8	2	10	5	12	3	4	15	16	3	18
20	4	5	3	22	7	24	4	26	5	28	4	30	31	5	4	5	8	36	4	5
40	7	40	5	42	5	6	4	46	8	48	6	5	5	52	5	6	7	7	5	58
60	4	60	5	6	63	7	5	66	5	6	6	70	7	72	5	7	6	6	6	78
80	9	80	8	82	6	6	6	6	7	88	6	7	6	6	6	6	7	96	6	8
100	8	100	6	102	7	7	6	106	6	108	6	6	13	112	6	7	6	8	6	6
120	7	120	6	6	6	124	6	126	127	7	6	130	6	7	6	7	7	136	6	138
140	6	7	6	10	10	7	6	7	6	148	6	150	7	8	8	7	6	156	7	6
160	9	7	6	162	6	7	6	166	7	168	6	8	6	172	6	6	14	9	6	178
180	6	180	6	6	7	9	6	10	6	8	6	190	7	192	6	7	6	196	6	198
200	7	8	6	7	6	8	6	8	14	11	10	210	6	7	6	7	7	8	6	10
220	6	12	6	222	13	8	6	226	6	228	6	7	7	232	6	7	6	7	6	238
240	7	240	6	242	6	7	6	12	7	7	6	250	6	12	9	7	255	256	6	12
260	6	8	8	262	7	8	7	10	7	268	7	270	15	16	6	13	10	276	6	9
280	7	280	6	282	6	12	6	7	15	288	6	6	6	292	6	6	7	10	10	12
300	7	7	7	7	15	15	6	306	7	7	7	310	7	312	7	10	7	316	7	10
320	15	15	6	16	8	12	6	7	7	9	6	330	7	8	7	6	8	336	6	7
340	6	10	10	342	7	7	6	346	6	348	8	12	18	352	6	9	7	9	6	358
360	8	360	6	7	7	10	6	366	15	15	7	15	7	372	7	15	7	13	7	378
380	7	12	7	382	15	15	7	15	7	388	7	16	7	8	7	7	8	396	7	7
400	15	400	7	15	11	8	7	15	8	408	7	13	8	12	10	9	18	15	7	418
420	7	420	7	15	7	16	6	7	7	10	6	430	15	432	6	15	6	18	7	438
440	7	15	7	442	7	13	7	11	15	448	7	15	7	7	7	15	7	456	7	16
460	7	460	7	462	15	15	7	466	8	8	7	15	7	15	10	18	7	15	6	478
480	15	15	6	15	8	7	6	486	7	15	6	490	6	16	6	7	15	15	6	498
500	7	12	9	502	7	15	6	15	7	508	6	15	511	18	7	15	8	12	8	15
520	8	520	10	522	12	15	8	16	15	528	7	15	8	12	7	15	8	15	10	15
540	12	540	7	15	18	7	7	546	7	8	7	18	7	7	7	7	7	556	7	12
560	15	7	7	562	7	7	6	7	7	568	6	570	7	7	15	22	8	576	7	7
580	7	8	7	10	7	8	7	586	7	18	17	7	15	592	8	15	7	7	8	598
600	14	600	12	15	7	15	16	606	18	15	7	15	8	612	8	15	7	616	7	618
620	8	22	8	15	15	624	7	8	8	16	7	630	7	8	7	8	7	12	7	8
640	9	640	7	642	7	7	7	646	8	10	7	7	7	652	7	7	15	15	7	658
660	7	660	7	15	7	15	7	22	7	15	7	15	15	672	7	24	8	676	7	15
680	7	15	7	682	8	15	7	15	15	15	7	690	8	15	7	15	7	16	7	15
700	8	700	7	18	15	15	7	15	8	708	7	15	7	22	21	15	7	15	8	718
720	15	9	8	12	10	24	12	726	7	728	16	16	18	732	7	7	22	10	8	738
740	7	7	7	742	7	15	7	8	7	10	7	750	15	15	8	15	8	756	8	15
760	7	760	8	15	8	15	8	15	15	768	8	15	8	772	8	24	23	15	8	18
780	8	18	7	26	15	15	10	786	12	15	7	15	20	15	18	15	8	796	22	16
800	24	15	8	15	8	15	8	15	8	808	8	810	8	15	8	15	15	18	8	8
820	8	820	8	822	8	15	8	826	8	828	8	15	12	16	7	8	7	26	25	838
840	8	840	8	20	8	10	8	16	15	15	12	22	7	852	16	15	22	856	7	858
860	22	15	24	862	26	15	7	15	8	15	9	15	7	15	7	15	7	876	8	15
880	15	880	8	882	8	15	7	886	7	15	8	15	10	18	8	15	13	15	8	28
900	27	16	8	8	8	22	8	906	8	18	10	910	15	14	8	15	16	10	18	918
920	24	8	22	12	24	24	26	8	28	928	7	18	7	7	7	14	7	936	7	15
940	7	940	7	22	15	15	7	946	7	12	12	15	7	952	7	15	7	15	8	15
960	15	960	29	15	8	15	8	966	8	15	8	970	10	18	12	15	15	976	16	18
980	18	15	7	982	27	15	24	15	26	22	28	990	31	31	7	15	8	996	25	26

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1000	7	15	21	16	19	15	7	18	15	1008	13	18	8	1012	9	22	7	28	7	1018
1020	7	1020	7	30	1023	24	7	15	9	15	9	1030	7	1032	7	15	8	16	9	1038
1040	15	15	8	15	8	15	8	15	8	1048	8	1050	8	15	8	15	15	16	8	8
1060	8	1060	8	1062	8	15	8	15	10	1068	7	15	15	28	7	24	7	15	8	15
1080	12	22	8	15	8	15	8	1086	16	15	8	1090	8	1092	8	15	8	1096	8	15
1100	8	15	8	1102	15	15	8	26	8	1108	8	18	8	15	8	15	8	1116	7	15
1120	16	18	7	1122	7	15	7	22	8	1128	7	15	8	15	10	9	15	15	7	16
1140	7	8	7	15	7	15	7	30	30	15	7	1150	15	1152	7	15	8	26	12	24
1160	12	26	7	1162	16	18	18	15	15	15	22	1170	24	15	26	24	28	15	30	30
1180	8	1180	8	15	31	15	8	1186	8	28	8	15	8	1192	8	15	8	15	8	15
1200	15	1200	8	15	8	15	8	16	8	15	8	15	8	1212	8	15	18	1216	7	22
1220	7	15	8	1222	7	24	7	15	7	1228	7	1230	15	9	8	15	7	1236	7	15
1240	7	16	8	10	8	7	8	28	8	1248	8	8	7	7	7	8	8	8	7	1258
1260	7	12	23	7	15	15	9	15	9	26	9	30	30	23	8	15	9	1276	9	1278
1280	15	30	10	1282	12	15	9	24	16	1288	18	1290	8	18	22	15	24	1296	26	15
1300	28	1300	30	1302	8	15	8	1306	30	15	8	15	31	15	12	15	8	15	8	1318
1320	8	1320	8	26	8	24	7	1326	15	15	8	1330	8	30	30	15	8	15	9	30
1340	12	15	8	30	15	30	12	15	9	26	16	24	18	15	9	20	22	22	24	15
1360	26	1360	28	28	30	30	9	1366	28	1368	30	15	9	1372	30	15	31	16	8	15
1380	8	1380	8	15	8	15	8	18	8	15	8	15	15	15	8	15	8	10	9	1398
1400	10	15	8	22	8	8	8	15	10	1408	8	16	7	9	9	22	9	12	7	8
1420	9	28	7	1422	15	24	9	1426	9	1428	7	26	7	1432	9	15	7	15	7	1438
1440	15	15	7	15	9	15	9	1446	7	15	7	1450	7	1452	9	15	15	30	30	1458
1460	8	15	8	30	8	15	8	30	10	30	12	1470	22	30	16	28	18	15	8	24
1480	22	1480	24	1482	26	18	28	1486	30	1488	13	15	8	1492	30	15	8	15	30	1498
1500	30	18	9	15	31	15	9	15	9	14	9	1510	9	24	9	9	9	36	9	30
1520	30	9	9	1522	9	30	9	9	9	30	10	1530	12	9	9	30	16	30	18	18
1540	8	26	22	1542	24	8	26	20	28	1548	30	30	15	1552	8	15	30	8	8	1558
1560	30	15	30	15	8	15	30	1566	31	15	8	1570	8	15	12	15	8	18	8	1578
1580	8	15	8	1582	15	24	8	8	8	15	8	36	7	26	8	15	8	1596	8	15
1600	24	1600	8	15	8	15	8	1606	8	1608	8	15	8	1612	7	15	15	15	8	1618
1620	8	1620	7	15	7	15	7	1626	7	15	7	15	24	22	8	15	8	1636	7	15
1640	7	15	7	30	30	15	7	26	15	30	7	15	11	30	10	30	12	1656	7	30
1660	16	30	18	1662	15	30	22	1666	24	1668	26	24	28	22	30	30	19	15	7	22
1680	30	1680	9	15	30	15	30	15	9	15	30	18	30	1692	9	15	31	1696	9	1698
1700	9	15	8	15	8	15	8	15	8	1708	21	28	15	15	8	15	10	16	7	15
1720	8	1720	9	1722	9	15	7	15	26	21	8	15	8	1732	7	15	7	15	7	36
1740	9	1740	8	15	15	15	8	1746	8	15	8	16	9	1752	9	15	9	15	8	1758
1760	26	15	8	40	9	15	8	15	8	28	8	27	8	15	8	24	15	1776	9	15
1780	8	15	8	1782	8	15	8	1786	8	1788	8	15	15	15	9	15	8	15	8	15
1800	8	1800	8	15	9	15	8	30	15	26	8	1810	8	36	7	15	9	22	9	16
1820	9	15	9	1822	26	24	9	15	9	30	30	1830	9	15	9	30	9	15	9	30
1840	15	30	12	18	9	30	16	1846	18	1848	9	30	22	16	24	15	28	30	28	28
1860	30	1860	25	22	8	22	30	1866	8	18	30	1870	30	1872	8	15	30	1876	30	1878
1880	8	15	30	8	8	8	8	15	31	1888	8	30	30	15	8	15	8	30	8	15
1900	8	1900	10	30	15	15	8	1906	16	30	18	15	8	1912	22	15	24	26	26	30
1920	28	30	30	30	27	9	7	40	30	9	8	1930	30	1932	30	8	15	15	30	15
1940	30	10	8	28	30	15	8	15	8	1948	30	1950	31	15	8	15	8	18	8	15
1960	8	36	8	15	8	15	8	15	15	15	8	26	8	1972	8	24	9	15	9	1978
1980	9	15	9	15	30	30	9	1986	9	15	30	15	10	1992	30	15	30	1996	9	1998

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2000	30	16	30	2002	9	9	30	22	9	40	9	2010	30	28	30	30	31	2016	8	15
2020	27	42	8	15	23	30	21	2026	8	2028	8	30	15	30	13	15	11	30	8	2038
2040	8	15	8	30	8	30	8	22	2047	15	8	15	8	2052	8	15	8	16	10	28
2060	8	15	9	2062	15	15	8	15	8	2068	8	18	8	15	9	24	8	30	30	15
2080	30	2080	8	2082	8	15	8	2086	10	2088	12	15	8	30	16	30	18	15	8	2098
2100	22	36	24	15	26	30	28	42	30	30	30	2110	15	2112	30	15	9	28	30	24
2120	30	15	10	15	30	18	30	16	15	2128	30	2130	8	26	9	15	30	2136	30	15
2140	9	2140	9	2142	31	15	9	18	9	15	9	15	9	2152	10	15	12	15	9	16
2160	15	2160	9	15	9	14	9	15	9	15	10	14	12	40	9	15	16	15	9	2178
2180	8	15	9	36	9	15	9	2186	9	15	9	23	15	15	8	15	9	2196	12	15
2200	9	30	30	2202	8	15	9	2206	15	2208	8	30	10	2212	12	15	8	30	16	30
2220	18	2220	8	30	22	24	24	16	26	30	28	30	30	30	30	15	10	2236	30	2238
2240	16	30	30	2242	30	15	8	15	30	22	30	2250	8	18	30	15	15	36	8	15
2260	30	15	30	30	30	30	9	2266	30	2268	8	15	31	2272	10	30	12	15	8	42
2280	16	2280	18	15	8	30	22	2286	24	15	26	30	28	2292	30	30	30	2296	9	30
2300	30	15	9	46	30	30	30	15	9	2308	30	2310	30	22	9	20	30	15	9	15
2320	15	15	30	22	30	15	9	30	28	16	30	15	9	2332	30	15	31	15	9	2338
2340	8	2340	8	10	9	15	8	2346	8	28	8	2350	15	12	8	15	9	2356	9	10
2360	8	15	8	16	8	9	8	10	36	22	10	2370	8	10	8	18	26	2376	8	10
2380	8	2380	8	2382	15	15	8	15	8	2388	8	15	8	2392	8	42	10	15	13	2398
2400	15	2400	8	26	8	15	9	28	7	15	7	2410	8	18	17	15	15	2416	7	40
2420	8	15	8	2422	14	24	12	15	8	15	16	15	18	15	8	15	9	2436	9	15
2440	9	2440	10	15	10	15	10	2446	15	30	30	15	9	27	9	30	9	15	9	2458
2460	10	30	12	15	15	30	16	2466	18	15	9	30	22	2472	24	15	26	2476	28	36
2480	30	30	30	15	12	30	30	15	9	30	30	46	30	15	9	15	30	30	30	28
2500	8	40	30	2502	8	15	9	22	30	15	30	30	30	30	9	15	30	30	8	15
2520	30	2520	30	30	12	24	9	30	31	30	18	2530	9	30	22	15	24	42	26	2538
2540	28	30	30	2542	30	15	9	30	30	2548	9	2550	30	30	30	15	9	2556	30	30
2560	30	30	9	28	30	15	10	16	9	23	30	15	30	30	30	30	15	15	30	2578
2580	9	28	30	30	30	30	12	12	12	30	30	2590	31	2592	8	30	22	48	24	22
2600	26	30	28	30	30	30	30	9	15	2608	30	15	9	30	30	30	30	2616	8	26
2620	30	2620	30	42	40	30	30	36	8	15	8	24	30	2632	30	15	8	30	8	16
2640	30	18	8	15	30	15	30	2646	28	15	8	15	30	15	30	15	31	2656	10	2658
2660	8	15	9	2662	9	15	9	15	7	16	9	2670	15	15	8	24	8	2676	8	15
2680	9	15	8	2682	9	15	8	2686	15	2688	8	15	10	2692	8	15	8	15	9	2698
2700	9	36	8	15	15	15	10	2706	8	15	10	2710	9	2712	8	15	10	15	10	2718
2720	31	15	9	15	9	24	10	26	10	2728	10	2730	9	15	10	15	15	15	8	15
2740	8	2740	8	15	9	15	8	40	9	2748	8	15	42	2752	9	15	8	15	9	30
2760	30	15	8	15	9	30	7	2766	15	30	10	30	12	46	8	30	16	2776	18	15
2780	9	30	22	22	24	15	26	30	28	2788	30	2790	30	15	9	30	30	2796	9	30
2800	30	2800	30	2802	9	15	30	30	30	2808	8	30	30	28	9	15	15	30	30	2818
2820	30	15	8	30	9	24	30	15	8	18	30	18	30	2832	9	15	9	2836	30	23
2840	30	15	30	2842	8	15	8	15	31	15	10	2850	8	15	9	15	8	2856	8	15
2860	8	2860	29	13	29	15	9	46	29	18	29	15	8	16	29	22	8	15	8	2878
2880	29	42	29	15	9	29	9	2886	29	26	8	48	29	15	29	15	15	2896	9	15
2900	29	15	30	2902	8	15	8	15	8	2908	10	40	31	15	9	15	8	2916	9	15
2920	8	22	21	36	9	18	9	2926	15	28	9	15	10	15	12	15	9	15	16	2938
2940	18	16	9	26	22	15	9	15	9	15	9	15	9	2952	9	15	9	2956	9	15
2960	15	15	9	2962	9	15	9	15	9	2968	9	2970	9	15	10	15	15	15	12	15
2980	9	15	10	18	9	15	9	28	9	48	8	15	15	40	9	15	9	36	9	2998

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3000	9 3000		9	15	10	15	9	30	46	15	9 3010		9	30	8	15	10	30	10 3018	
3020	12	15	9 3022		16	30	18	15	9	30	22	15	24	15	26	30	28 3036		30	30
3040	31 3040		9	30	30	15	9	30	30 3048		30	26	9	42	30	30	30	30	9	30
3060	30 3060		9	15	9	30	30 3066		30	15	9	36	15	30	30	15	8	26	30 3078	
3080	30	15	9 3082		9	18	30	15	30 3088		30	15	9	15	10	15	30	18	9	15
3100	9	15	9	28	31	15	9	25	9 3108		8	15	9	15	8	15	8	15	9 3118	
3120	15 3120		8	15	9 3124		8	52	8	15	9	30	30	15	8	15	48 3136		9	42
3140	8	30	10	30	12	15	9	30	16	46	18	22	15	30	22	15	24	15	26	30
3160	28	30	30 3162		30	15	9 3166		30 3168		9	30	30	30	30	24	23	15	30	30
3180	30 3180		10	30	30	15	10 3186		12	30	30 3190		30	30	30	30	8	30	30	30
3200	24	30	30 3202		30	30	12	24	9 3208		30	30	30	18	30	30	22 3216		24	15
3220	30 3220		28	30	30	30	30	15	30 3228		30	15	31	52	30	30	30	15	9	40
3240	30	30	30	30	9	30	30	16	15	15	10 3250		30 3252		30	15	9 3256		9 3258	
3260	30	15	10	30	30	30	30	26	10	26	9 3270		30	15	30	24	30	28	10	15
3280	15	16	30	48	9	15	10	18	28	15	30	15	9	36	30	15	31	15	9 3298	
3300	10 3300		10	15	10	15	10 3306		10	15	9	15	15 3312		9	15	9	30	30 3318	
3320	9	40	9 3322		9	23	9	30	14 3328		12 3330		10	30	16	30	18	46	9	30
3340	22	15	24 3342		26	30	28 3346		30	30	30	15	10	30	30	13	10	30	30 3358	
3360	30 3360		10	15	30	30	30	30	12	30	30 3370		10 3372		10	30	30	15	30	30
3380	30	30	9	30	30	30	9	30	30 3388		30 3390		52	30	10	30	30	42	30	24
3400	30	39	22	40	24	23	30 3406		28	30	30	30	30 3412		30	30	30	15	30	30
3420	30	30	30	15	31	24	30	30	30	30	25	46	30 3432		9	15	10	30	30	18
3440	30	15	13	30	10	30	30	15	22 3448		30	30	30	13	24	30	26 3456		30	15
3460	30 3460		30 3462		9	15	9 3466		30 3468		9	10	15	22	10	24	30	18	9	48
3480	30 3480		30	42	10	15	30	39	31	15	9 3490		9	11	10	13	10	15	12 3498	
3500	9	15	10	30	30	11	10	15	9	30	10 3510		9	30	10	30	12 3516		9	30
3520	26	30	18	15	12	30	22 3526		24 3528		26	30	28 3532		30	30	30	26	10 3538	
3540	30 3540		11	30	30	30	30 3546		11	15	30	52	30	30	10	30	30 3556		10 3558	
3560	11	30	30	12	30	12	11	30	15	42	30 3570		11	30	30	30	30	48	10	30
3580	10 3580		30 3582		30	30	30	16	10	36	10	15	30 3592		11	15	11	18	10	58
3600	30	15	10	13	30	15	30 3606		9	15	30	22	30 3612		9	15	31 3616		9	15
3620	10	15	9 3622		10	28	11	15	9	25	11 3630		15	15	10	15	10 3636		9	15
3640	9	15	8 3642		11	15	9	15	26	40	10	15	9	15	12	15	9	25	9 3658	
3660	11	15	11	15	15	15	10	18	9	15	9 3670		10 3672		10	15	9 3676		8	21
3680	15	15	10	28	27	15	10	24	9	15	10 3690		10	18	10	16	15 3696		10	26
3700	16 3700		18	15	24	15	22	15	24 3708		26	15	28	46	10	15	10	15	9 3718	
3720	10 3720		10	15	11	24	9 3726		15	15	9	15	10 3732		10	15	9	36	9 3738	
3740	9	15	10	18	15	39	10	15	9	22	10	30	30	26	9	15	10	30	12	15
3760	15 3760		10	52	12	15	10 3766		16 3768		18	15	9	30	22	24	58	15	26 3778	
3780	28	30	30	30	30	15	10	30	30	15	10	30	30 3792		30	15	10 3796		30	30
3800	30	30	10 3802		30	15	9	46	31	30	30	36	30	15	9	30	9	30	30	15
3820	10 3820		30 3822		30	15	10	42	10	30	30	15	30 3832		30	15	10	15	10	15
3840	30	30	10	15	10	26	10 3846		30	15	9 3850		30 3852		30	15	15	15	30	16
3860	30	15	10 3862		30	15	9	15	9	52	9	48	31	15	10	30	30 3876		10	15
3880	10 3880		9	15	10	30	10	30	15 3888		10	30	16	30	18	15	9	30	22	15
3900	24	48	26	30	60	30	30 3906		30	15	9 3910		30	15	11	30	30 3916		30 3918	
3920	15	15	30 3922		30	30	9	30	30 3928		9 3930		9	30	30	15	30	30	30	30
3940	9	30	30 3942		9	30	30 3946		30	30	12	30	15	58	30	30	30	30	30	36
3960	26	40	24	15	30	30	28 3966		30	48	30	28	30	36	30	24	30	40	30	30
3980	30	18	30	16	30	30	30	30	30 3988		30	22	10	24	10	30	30	28	30	30

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
4000	31	4000	10	4002	30	30	10	4006	30	30	30	30	9	4012	9	30	30	30	30	4018
4020	30	4020	9	26	9	24	30	4026	9	30	9	30	30	36	30	30	9	26	30	30
4040	30	30	10	20	30	18	30	30	15	4048	30	4050	18	15	9	15	28	4056	30	15
4060	26	30	30	16	31	30	10	48	27	30	9	30	10	4072	21	30	19	30	16	4078
4080	18	30	10	30	22	15	24	60	26	30	28	4090	30	4092	30	30	4095	30	30	4098
4100	9	30	30	30	30	15	9	15	30	30	30	4110	15	30	30	15	10	22	10	30
4120	30	15	30	15	11	30	9	4126	30	4128	10	30	30	4132	30	15	11	30	10	4138
4140	30	40	30	30	30	15	10	15	10	15	30	30	9	4152	11	30	9	4156	30	4158
4160	15	30	30	22	30	15	29	24	30	22	30	42	29	15	30	24	29	4176	10	15
4180	10	36	30	46	29	15	30	52	30	58	29	15	31	15	29	15	29	15	10	15
4200	12	4200	29	15	29	15	29	15	15	15	10	4210	29	15	9	15	9	4216	10	4218
4220	29	15	9	40	29	24	29	15	10	4228	29	4230	29	15	10	15	29	18	13	26
4240	15	4240	10	4242	30	15	9	30	30	15	12	15	9	4252	13	15	31	30	10	4258
4260	12	4260	10	30	16	30	18	42	9	30	22	4270	24	4272	26	30	28	30	30	30
4280	30	15	10	4282	30	15	9	30	63	4288	30	15	10	52	30	30	30	4296	9	30
4300	30	15	10	15	15	30	30	58	30	30	30	30	9	30	30	30	9	30	30	30
4320	30	30	12	30	10	30	30	4326	30	30	30	60	22	15	24	15	30	4336	28	4338
4340	30	30	30	42	30	30	30	30	30	4348	30	30	30	30	30	28	30	4356	30	30
4360	30	48	30	4362	13	18	13	30	30	16	30	15	30	4372	30	30	30	15	30	30
4380	30	30	30	15	31	30	12	40	30	15	30	4390	30	22	13	15	13	4396	30	52
4400	15	26	12	30	13	30	30	15	13	4408	30	15	30	15	10	30	30	30	30	15
4420	12	4420	30	4422	13	15	13	20	12	42	30	15	15	15	30	15	30	30	12	22
4440	30	4440	11	15	13	15	30	4446	31	15	10	4450	12	60	13	15	12	4456	13	15
4460	13	15	13	4462	15	15	11	15	10	40	12	16	13	15	13	24	13	36	13	15
4480	16	4480	10	4482	10	15	12	15	13	4488	13	15	10	4492	13	15	15	15	10	25
4500	10	15	10	15	10	15	12	4506	13	26	13	15	15	4512	10	15	10	4516	10	4518
4520	10	15	12	4522	13	24	10	15	15	15	11	22	10	15	10	15	10	15	10	15
4540	12	18	13	15	63	15	10	4546	10	4548	10	15	10	28	10	15	12	15	12	46
4560	15	4560	11	26	11	15	10	4566	10	15	12	15	12	16	13	15	31	22	11	18
4580	10	15	10	4582	10	15	10	15	12	15	13	4590	15	15	10	15	10	4596	12	15
4600	10	42	10	4602	12	15	9	16	15	15	13	15	11	15	9	15	9	18	10	30
4620	30	4620	12	15	16	36	15	15	13	30	15	30	15	40	15	30	16	4636	18	4638
4640	31	30	22	4642	24	15	26	30	28	4648	30	4650	30	15	15	30	30	4656	12	30
4660	30	58	30	4662	14	15	30	30	30	30	14	30	63	4672	12	15	14	30	30	4678
4680	30	30	30	30	14	30	30	42	15	30	30	4690	30	30	14	30	15	30	30	36
4700	35	30	30	4702	22	15	24	15	30	30	28	30	30	30	30	30	30	52	30	30
4720	30	4720	30	4722	30	30	30	30	30	4728	30	31	30	4732	30	15	36	30	12	30
4740	30	15	30	15	30	30	30	46	30	15	30	4750	30	48	30	15	30	66	30	4758
4760	30	15	30	30	30	15	13	15	31	18	30	30	11	15	10	30	10	39	30	58
4780	15	30	30	4782	30	15	12	4786	30	4788	30	15	10	4792	30	15	14	15	15	4798
4800	15	4800	30	15	10	15	30	24	30	30	10	16	30	4812	14	15	15	4816	30	60
4820	30	15	10	22	28	24	12	15	12	15	30	4830	31	26	12	15	10	23	10	15
4840	10	46	11	28	12	15	15	36	15	15	11	15	10	22	10	15	11	15	10	42
4860	11	4860	14	15	18	17	12	30	30	15	10	4870	11	30	11	15	12	4876	11	30
4880	15	16	10	30	16	30	18	26	10	4888	22	66	24	15	26	30	28	58	30	30
4900	30	28	12	4902	30	15	10	30	30	4908	30	15	15	4912	30	30	30	30	10	4918
4920	30	15	11	15	10	30	30	15	30	15	12	4930	11	4932	30	15	11	4936	30	30
4940	30	60	10	4942	15	30	30	15	30	48	30	4950	10	15	10	15	30	4956	10	15
4960	15	40	11	30	30	15	12	4966	30	4968	30	15	10	4972	30	30	30	15	12	15
4980	30	16	10	15	11	30	10	4986	30	15	10	15	30	4992	30	30	10	18	30	4998

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5000	11	15	10	5002	30	18	30	15	15	5008	10	5010	11	15	10	15	30	28	30	15
5020	10	5020	10	5022	31	15	10	15	10	46	10	15	9	15	10	15	10	15	10	5038
5040	15	5040	10	15	11	15	10	48	9	15	10	5050	10	30	30	15	63	15	10	5058
5060	11	15	10	60	10	30	12	15	10	36	16	30	18	15	10	30	22	5076	24	15
5080	26	5080	28	30	30	30	30	5086	31	30	30	15	12	30	30	30	30	15	10	5098
5100	30	5100	30	30	15	30	30	5106	11	15	10	30	30	5112	30	15	10	30	10	5118
5120	30	39	10	46	30	40	30	15	10	30	13	30	30	15	30	30	30	15	10	15
5140	11	52	30	36	11	15	13	5146	13	45	30	15	31	5152	30	15	30	26	10	30
5160	30	30	30	15	12	15	30	5166	15	15	15	5170	15	30	30	15	15	30	30	5178
5180	30	30	15	70	63	30	15	30	15	5188	30	28	30	30	16	30	18	5196	15	30
5200	22	15	30	42	30	30	28	40	39	5208	30	36	15	30	30	15	31	30	30	30
5220	30	22	15	15	30	30	30	5226	15	30	30	5230	24	5232	26	30	30	5236	30	31
5240	30	30	13	48	36	30	15	30	40	30	30	58	15	30	15	30	30	30	30	30
5260	30	5260	22	18	24	15	30	30	28	30	30	30	30	5272	30	30	30	30	30	5278
5280	31	5280	30	30	30	30	30	30	30	30	30	30	30	66	15	30	15	5296	30	16
5300	30	15	30	5302	30	30	30	15	30	5308	30	46	63	30	30	30	30	30	30	26
5320	30	30	30	5322	15	18	30	16	30	5328	12	16	10	5332	30	30	30	15	15	30
5340	30	48	30	15	31	30	30	5346	30	15	10	5350	30	52	11	15	15	30	15	30
5360	30	15	12	30	30	30	30	30	10	30	30	40	15	30	15	42	30	30	30	30
5380	16	5380	18	15	14	30	22	5386	30	18	30	30	28	5392	30	30	30	15	12	5398
5400	30	15	30	30	30	30	30	5406	31	15	30	30	30	5412	9	30	30	5416	12	5418
5420	11	30	30	15	30	15	13	66	12	60	30	5430	11	30	30	30	30	5436	15	30
5440	40	5440	30	5442	30	30	30	15	11	5448	11	15	30	30	15	15	15	30	10	52
5460	30	42	41	30	30	38	30	15	11	30	30	5470	30	30	12	16	30	5476	16	5478
5480	18	30	10	5482	30	18	24	15	30	30	30	30	30	31	30	30	38	22	36	30
5500	30	5500	40	5502	42	30	10	5506	14	15	12	24	30	36	30	15	10	15	10	5518
5520	30	5520	10	15	10	15	30	5526	10	15	30	5530	30	15	10	15	31	48	10	28
5540	10	15	9	25	9	15	10	15	12	30	30	15	15	15	11	30	10	5556	10	30
5560	10	66	12	5562	9	30	16	30	18	5568	10	30	22	5572	24	24	26	30	28	30
5580	30	5580	30	15	15	30	30	36	12	30	30	5590	30	15	13	15	30	30	30	30
5600	15	30	30	15	11	15	10	30	30	70	30	30	30	30	10	30	30	40	12	30
5620	30	30	30	5622	12	30	11	30	30	30	30	30	30	42	22	15	24	15	30	5638
5640	28	5640	30	30	30	30	30	5646	30	30	30	5650	30	5652	30	30	30	5656	30	5658
5660	30	30	30	30	30	15	10	30	10	5668	30	52	30	15	30	30	30	30	30	15
5680	30	30	30	5682	30	30	30	46	30	5688	30	30	30	5692	30	15	63	30	30	40
5700	30	5700	10	15	11	30	30	30	30	18	11	5710	30	28	30	15	30	5716	30	30
5720	30	15	30	58	30	24	10	15	31	30	10	30	30	15	11	15	30	5736	30	30
5740	11	5740	30	5742	15	15	10	30	30	5748	30	70	11	30	11	15	14	15	11	30
5760	30	30	30	15	11	15	11	72	30	15	11	28	11	22	30	15	16	52	30	5778
5780	30	15	11	5782	30	15	10	15	10	15	30	5790	31	15	10	15	11	15	10	15
5800	11	5800	11	15	9	15	11	5806	15	39	10	15	11	5812	12	15	10	15	10	15
5820	10	5820	13	15	63	24	10	5826	11	15	10	16	10	18	10	15	10	15	13	5838
5840	15	15	10	5842	10	15	10	15	11	5848	10	5850	10	15	12	15	15	5856	10	15
5860	10	5860	10	27	11	15	10	5866	10	5868	11	15	15	15	13	46	11	15	10	5878
5880	10	5880	10	15	10	15	12	15	22	21	13	42	13	70	11	15	13	5896	13	16
5900	13	15	13	5902	15	16	13	18	12	18	13	22	13	72	13	15	13	60	13	15
5920	15	30	30	5922	13	15	13	5926	13	48	13	30	13	30	13	15	15	30	16	5938
5940	18	15	10	30	22	16	24	18	26	30	28	30	30	5952	30	15	12	30	30	58
5960	13	30	30	66	30	15	13	15	30	46	45	30	11	42	30	24	13	42	11	36
5980	30	5980	30	30	30	30	16	5986	30	52	13	30	30	30	30	30	26	30	28	30

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
6000	30	31	30	30	30	30	36	6006	24	15	40	6010	42	30	30	30	46	30	30	30
6020	30	30	30	30	30	30	30	30	30	6028	30	45	30	30	30	30	30	6036	13	30
6040	13	30	30	6042	30	15	30	6046	30	30	30	15	30	6052	30	30	30	30	30	72
6060	30	30	30	30	30	30	30	6066	12	30	30	30	30	6072	12	24	12	58	30	6078
6080	46	30	10	30	30	15	30	24	30	6088	30	6090	30	15	30	15	30	15	13	15
6100	30	6100	30	30	30	15	12	30	30	40	30	30	31	6112	30	30	11	30	10	30
6120	30	6120	30	30	16	48	18	15	15	45	22	6130	30	6132	30	30	28	30	30	30
6140	30	15	12	6142	30	30	30	30	30	30	30	6150	30	15	30	30	30	46	11	30
6160	30	60	30	6162	30	30	30	15	30	30	30	30	11	6172	30	30	31	45	30	36
6180	30	30	12	30	11	30	30	30	30	30	30	40	22	15	24	15	30	6196	28	6198
6200	30	30	30	6202	30	30	30	30	63	30	30	6210	30	30	30	30	30	6216	30	30
6220	30	6220	30	48	47	30	11	44	30	6228	30	15	30	38	30	36	30	15	30	30
6240	30	6240	30	30	30	30	30	6246	30	30	30	30	30	36	30	31	30	6256	30	30
6260	36	15	15	6262	44	30	42	30	15	6268	46	6270	48	30	30	30	30	6276	30	16
6280	30	15	30	60	15	15	30	6286	30	30	30	26	15	15	30	30	30	30	30	6298
6300	30	6300	15	15	31	30	30	30	30	15	15	6310	15	58	15	15	15	6316	30	70
6320	30	15	15	6322	15	39	30	16	15	6328	15	30	30	15	15	30	30	6336	30	15
6340	15	16	30	6342	15	15	15	15	30	18	30	15	15	6352	15	18	15	15	15	6358
6360	30	6360	30	15	15	15	30	6366	31	15	15	22	15	6372	15	15	15	15	15	6378
6380	15	15	15	15	15	15	15	15	15	6388	15	70	15	15	15	15	15	6396	15	78
6400	24	36	15	18	11	15	15	42	15	48	15	15	15	52	15	15	15	16	15	48
6420	15	6420	15	22	15	24	15	6426	15	15	15	58	15	15	13	15	15	40	10	46
6440	15	15	15	16	15	15	15	15	15	6448	15	6450	11	26	13	16	15	15	15	15
6460	15	15	15	22	63	15	15	28	15	6468	12	15	15	6472	15	15	15	15	15	15
6480	15	6480	15	15	13	15	13	15	15	15	15	6490	15	42	15	15	31	72	13	66
6500	15	15	12	15	11	15	15	26	15	22	15	16	15	15	13	15	15	18	12	16
6520	11	6520	15	15	15	15	15	60	24	6528	13	15	15	46	11	17	12	15	15	15
6540	15	30	30	15	15	15	15	6546	11	15	14	6550	11	6552	12	15	15	78	16	30
6560	31	6560	15	6562	22	15	24	16	26	6568	28	6570	30	30	30	24	15	6576	30	15
6580	11	6580	30	30	30	15	11	15	30	30	30	30	63	30	30	15	11	15	11	6598
6600	30	15	30	15	11	30	10	6606	30	15	10	30	30	30	30	16	11	30	11	6618
6620	30	15	30	36	30	52	11	15	11	15	30	30	11	15	11	30	11	6636	30	15
6640	15	30	30	15	30	15	11	30	30	60	30	15	11	6652	30	15	15	15	11	6658
6660	11	6660	30	15	11	15	30	58	30	30	12	15	30	6672	12	15	11	30	30	6678
6680	30	15	12	40	12	15	14	15	18	6688	30	6690	30	15	11	15	12	36	30	15
6700	14	6700	12	6702	30	16	11	30	30	6708	30	15	11	48	30	15	11	15	14	6718
6720	30	30	30	80	11	24	12	23	11	15	11	52	51	6732	30	48	15	6736	30	22
6740	30	42	11	40	12	15	11	15	16	16	18	42	31	30	22	28	24	28	26	15
6760	28	6760	30	6762	12	15	10	66	36	17	11	15	40	15	42	24	15	26	46	6778
6780	48	6780	15	15	52	15	15	17	12	15	13	6790	15	6792	15	15	15	15	15	15
6800	15	15	15	6802	15	17	15	15	15	23	15	48	15	15	15	15	15	16	15	15
6820	15	18	15	6822	15	24	15	6826	15	6828	15	15	15	6832	15	15	15	15	15	15
6840	15	6840	15	15	15	15	15	40	63	21	15	15	15	15	15	15	15	6856	15	6858
6860	15	15	15	6862	15	15	15	15	15	6868	15	6870	15	16	15	15	15	15	15	15
6880	31	15	15	6882	15	15	15	70	15	6888	15	15	15	60	15	15	15	15	15	6898
6900	15	66	15	15	15	15	15	6906	15	15	15	6910	26	30	30	15	15	6916	15	30
6920	15	16	15	30	15	30	15	15	15	40	16	30	18	15	15	30	22	24	24	26
6940	26	30	28	52	31	30	30	6946	15	6948	30	15	15	30	30	30	30	15	15	6958
6960	30	6960	30	30	15	30	30	6966	15	16	15	6970	30	18	30	15	63	6976	15	30
6980	30	15	15	6982	30	30	30	15	15	30	15	6990	30	15	30	30	30	6996	15	15

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
7000	*15*	7000	*30*	*46*	*15*	*15*	*15*	30	*15*	*42*	*30*	*15*	15	7012	*30*	*15*	*30*	*15*	*15*	7018
7020	*30*	30	*30*	*15*	*15*	*24*	*30*	7026	15	*15*	15	*78*	*15*	30	*30*	*15*	*15*	*30*	*30*	7038
7040	*30*	*30*	15	7042	*30*	30	*15*	30	*15*	52	*30*	30	*30*	30	*16*	30	*18*	7056	*15*	30
7060	*22*	30	*30*	30	*30*	30	*28*	*36*	30	7068	*30*	*15*	*16*	30	*30*	30	*30*	30	*30*	7078
7080	*30*	*72*	*30*	*15*	*30*	30	*30*	30	*15*	30	*30*	*15*	*30*	*40*	*30*	30	*30*	*46*	*30*	*39*
7100	*30*	*30*	15	7102	*30*	30	*30*	30	*30*	7108	*30*	30	*30*	30	15	30	*30*	30	*30*	30
7120	*30*	7120	*22*	*16*	*30*	*15*	*30*	7126	*28*	7128	30	*30*	30	30	*30*	30	*31*	30	*30*	*58*
7140	*30*	*36*	*30*	30	*30*	30	*30*	30	*30*	30	*30*	7150	*30*	*22*	*13*	30	*15*	30	*30*	7158
7160	*30*	16	*30*	*30*	*30*	*30*	*30*	*15*	*30*	*66*	*30*	*70*	*30*	30	*30*	30	*30*	7176	*30*	30
7180	*30*	*42*	*30*	*15*	*15*	30	*30*	7186	*30*	30	*13*	*15*	13	7192	*30*	30	*30*	30	15	30
7200	*30*	*18*	*30*	30	*30*	30	*30*	7206	*30*	*80*	*30*	7210	*30*	7212	*15*	*15*	*30*	30	*30*	7218
7220	*30*	*15*	*10*	*30*	*30*	30	*30*	*30*	*30*	7228	*30*	*30*	*63*	30	*30*	30	*30*	7236	*30*	30
7240	*16*	30	*18*	7242	14	30	*22*	7246	*30*	30	*30*	30	*28*	7252	30	*30*	*30*	*15*	13	30
7260	*30*	*52*	*30*	30	*31*	30	*30*	*42*	*30*	*15*	*30*	30	*30*	30	13	30	*30*	*18*	*30*	30
7280	*30*	30	*30*	7282	*30*	*15*	*11*	*30*	*12*	*36*	*30*	30	*30*	30	*30*	30	*30*	7296	*30*	30
7300	15	*48*	*30*	*66*	*30*	30	*30*	7306	15	7308	*30*	16	*30*	*70*	13	*15*	13	30	*15*	30
7320	*30*	7320	*30*	30	*30*	*24*	*30*	*16*	*31*	30	*30*	7330	*30*	7332	*15*	*15*	*30*	*15*	*15*	*40*
7340	*15*	30	*15*	30	*30*	*15*	*15*	*15*	*30*	7348	*30*	7350	*15*	*15*	*30*	30	*15*	*15*	*15*	30
7360	*30*	30	*30*	*36*	*15*	30	*15*	*52*	*15*	7368	*15*	30	*30*	*72*	*30*	*58*	*15*	*15*	*15*	*46*
7380	*30*	*60*	15	30	*15*	30	*30*	*82*	*15*	30	*30*	30	*30*	7392	15	*15*	*30*	*16*	*15*	*48*
7400	*24*	*15*	*30*	30	*30*	*15*	*15*	*15*	*15*	*30*	*30*	7410	15	*15*	*30*	30	*30*	7416	*15*	30
7420	*30*	*40*	*30*	*15*	*28*	30	*16*	30	*18*	*16*	*15*	30	*22*	7432	*30*	20	*26*	30	*28*	*42*
7440	30	*30*	30	*18*	*15*	30	*30*	*22*	*15*	30	*30*	7450	*30*	*28*	*15*	*15*	*31*	7456	*30*	7458
7460	15	30	*30*	*16*	*15*	*15*	*15*	30	*30*	*15*	*30*	*30*	*30*	*30*	*15*	30	*30*	7476	15	30
7480	*30*	7480	*30*	30	*15*	30	*15*	7486	*30*	7488	*30*	30	*30*	*58*	*57*	*15*	*24*	54	*30*	7498
7500	*28*	30	30	48	30	46	*30*	7506	*30*	30	*30*	30	*30*	30	*30*	36	*30*	7516	*30*	*72*
7520	*30*	30	*30*	7522	*30*	*31*	15	30	*15*	7528	*36*	*16*	*30*	*30*	*40*	*30*	*42*	7536	*30*	30
7540	*46*	7540	*48*	30	*30*	30	*52*	7546	*30*	7548	*30*	30	*58*	30	*30*	30	*22*	30	*30*	7558
7560	*30*	7560	*28*	30	30	*30*	*30*	30	*30*	30	*30*	*66*	*30*	7572	*30*	30	*30*	7576	*30*	30
7580	*30*	30	*30*	7582	*30*	30	*30*	*26*	*30*	7588	*30*	7590	*30*	*15*	*30*	16	*30*	*70*	*30*	*30*
7600	*30*	30	*30*	7602	*30*	30	*30*	7606	*30*	30	*30*	30	*30*	30	*30*	*39*	58	30	13	30
7620	*30*	7620	*30*	30	*15*	*60*	15	30	*30*	30	*30*	30	*30*	30	*30*	*15*	*30*	30	*30*	7638
7640	*30*	30	*30*	7642	*30*	*15*	*30*	*15*	*31*	7648	*30*	30	*30*	30	*30*	*15*	15	*15*	*30*	30
7660	*30*	*46*	*30*	*78*	*30*	30	15	30	*30*	7668	*30*	30	*30*	7672	14	30	*15*	*15*	*15*	30
7680	*15*	7680	*30*	30	*30*	*15*	*15*	7686	*15*	*15*	*30*	7690	*15*	*48*	*30*	30	*30*	*42*	*30*	7698
7700	*30*	30	*30*	7702	*30*	*15*	*30*	*15*	*15*	*15*	*30*	17	*31*	30	*30*	*15*	*15*	7716	*15*	*15*
7720	14	*15*	14	7722	*30*	30	*30*	7726	*15*	*58*	*30*	30	*30*	*15*	*15*	30	*15*	*15*	14	*70*
7740	*13*	7740	*15*	30	*63*	30	*15*	*60*	*59*	*15*	*15*	56	*15*	7752	14	*15*	*30*	7756	17	7758
7760	*30*	*15*	*30*	*16*	*16*	17	*30*	*15*	28	38	*22*	36	*30*	*15*	*30*	*24*	*31*	30	*30*	*31*
7780	14	*30*	*30*	*42*	*36*	*15*	14	30	*40*	7788	*42*	30	*15*	7792	*46*	*15*	*48*	30	*16*	30
7800	56	*28*	*15*	30	*22*	*15*	*58*	*36*	*60*	30	*28*	*72*	30	*30*	30	*15*	*15*	7816	*30*	*16*
7820	*15*	30	*30*	7822	*30*	*24*	14	*15*	*30*	7828	*30*	*40*	15	30	*30*	*16*	*15*	*16*	*13*	30
7840	*30*	7840	*30*	*15*	14	*30*	*15*	30	*30*	*46*	15	30	*30*	7852	*30*	*15*	*15*	*80*	*13*	30
7860	*30*	*23*	*30*	30	*30*	*15*	*15*	7866	*15*	*15*	*30*	30	*15*	7872	*13*	30	*15*	7876	*30*	7878
7880	*15*	30	*30*	7882	*30*	*15*	*15*	30	*30*	30	*30*	*15*	*15*	*15*	*30*	*15*	*15*	*52*	*15*	30
7900	*15*	7900	*30*	*15*	18	*15*	*30*	7906	*30*	*30*	*15*	*26*	*30*	*40*	*15*	*16*	*15*	30	*30*	7918
7920	*30*	7920	*15*	30	*15*	*24*	*15*	7926	*15*	30	*30*	30	*30*	7932	*15*	*15*	*30*	7936	*30*	*16*
7940	*15*	30	30	*46*	*30*	*15*	30	30	*30*	7948	*30*	7950	30	*16*	*30*	*18*	*15*	*72*	30	*22*
7960	*30*	30	*30*	7962	30	*28*	30	*30*	*30*	30	*15*	*15*	*30*	*30*	*30*	*15*	30	*30*	*30*	*78*
7980	*30*	*22*	*15*	*30*	30	*30*	30	*48*	30	*30*	*22*	*60*	*30*	7992	30	*30*	*28*	*30*	30	*30*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
8000	*63*	30	30	*52*	*30*	*15*	30	*30*	*30* 8008		*30* 8010		30	18	*30*	*30*	*30* 8016		30	*30*
8020	*30*	*15*	*30*	*70*	*30*	*30*	*30*	*22*	*30*	*15*	30	*30*	*31*	*30*	*30*	*15*	30	*30*	*30* 8038	
8040	*30*	*15*	30	*30*	30	*30*	*30*	*15*	*30*	*30*	*30*	*82*	*15* 8052		30	*15*	*30*	*30*	*15* 8058	
8060	*15*	*30*	30	*30*	*30*	*15*	*15*	*30*	*30* 8068		*30*	*15*	30	*30*	*30*	*30*	*30*	*40*	30	*15*
8080	*30* 8080		*15*	*58*	30	*30*	30 8086		*30* 8088		*15*	*15*	*30* 8092		*30*	*30*	*31*	*18*	*30*	*30*
8100	*15* 8100		30	*30*	*30*	*30*	*30*	*66*	*15*	*30*	*15* 8110		*15*	*25*	*15*	*30*	*30* 8116		*30*	*22*
8120	*15*	*15*	*15* 8122		*30*	*15*	*15*	*30*	*63*	*62*	*30*	*46*	59	*30*	*30*	*30*	*30*	*78*	53	*15*
8140	51	*17*	*15*	*16*	30	*27*	*30* 8146		*30*	*28*	41	*22*	39	*30*	*30*	*26*	30	*28*	33	*40*
8160	*31* 8160		*29*	*30*	*30*	*36*	*30* 8166		23	*40*	21 8170		*18*	*15*	17	*46*	*22*	*48*	*30* 8178	
8180	*26*	*80*	*28*	*48*	30	*30*	30	*58*	*26*	*60*	*30* 8190	8191	*30*	*30*	30	*30*	*15*	15	24	
8200	*30*	*58*	*30*	30	*15*	30	*30*	*28*	*30* 8208		*30*	30	*30*	*42*	*30*	*22*	*15*	*30*	*30* 8218	
8220	*30* 8220		*15*	*30*	*31*	30	*30*	*18*	*15*	30	*15* 8230		*30* 8232		*30*	30	*30* 8236		*15*	*57*
8240	*15*	*15*	*30* 8242		*15*	*15*	*15*	30	*15*	*72*	*30*	*36*	*15*	30	*30*	*15*	*62*	*22*	15	30
8260	*30*	30	*30* 8262		*15*	*15*	*30*	*18*	*15* 8268		*15*	30	*15* 8272		*30*	*24*	15	*15*	*30*	30
8280	*30*	*48*	*14*	*15*	*30*	30	*15* 8286		*15*	30	*30* 8290		*30* 8292		*15*	30	*15* 8296		*15*	*42*
8300	15	30	*30*	30	*30*	*16*	15	*15*	*15*	*15*	*30* 8310		*15*	30	*15*	30	*30* 8316		*15*	30
8320	*30*	*52*	*30*	*15*	*15*	17	*30*	*25*	*15* 8328		*15*	*15*	*30*	30	*30*	*15*	*15*	*15*	*14*	*30*
8340	*30*	*18*	15	*80*	*30*	30	*30*	*16*	15	30	*30*	30	*30* 8352		*14*	30	*16*	*60*	*18*	*15*
8360	*14*	*57*	*22* 8362		*30*	30	*26*	30	*28* 8368		30	*30*	30	30	*15*	*66*	*30* 8376		30	30
8380	*30*	30	*30*	*82*	*63*	30	*30* 8386		*30* 8388		*15*	30	*30*	22	*30*	16	*30*	30	*30*	*36*
8400	*30*	*30*	*30*	*30*	*30*	30	*30*	30	15	*30*	*30*	30	*30*	*46*	*15*	30	*31*	30	*30* 8418	
8420	*30*	30	*30* 8422		*22*	*24*	*24*	*15*	*30* 8428		*28* 8430		30	*30*	30	30	*30*	30	*30*	30
8440	*30*	30	*30* 8442		*30*	30	*30* 8446		*30*	30	*30*	30	*30*	*78*	*30*	*15*	15	30	*15*	30
8460	*30* 8460		*30*	30	*30*	*30*	*30* 8466		*30*	16	*30*	*42*	*30*	*36*	*30*	30	*30*	*48*	*30*	*60*
8480	*30*	30	*30*	30	*30*	*15*	*22*	30	*30*	30	*30*	30	*28*	*15*	*29*	30	*30*	30	*30*	30
8500	*29* 8500		*30*	*15*	*30*	30	*30*	*46*	*30*	*66*	*65*	16	*30* 8512		*30*	*15*	*29*	*15*	*30*	56
8520	*30* 8520		*30*	*15*	*29*	*15*	*30* 8526		*30*	*30*	*30*	44	*30*	42	*29*	30	*30* 8536		*30* 8538	
8540	*30*	*31*	*29* 8542		*29*	30	*36*	30	*15*	*82*	*40*	30	*42*	*15*	*15*	20	*46*	*42*	*48*	30
8560	*29*	30	*52* 8562		*30*	30	*30*	30	*58*	30	*60*	30	*30* 8572		*30*	*24*	*66*	30	*30*	28
8580	*30* 8580		*30*	*15*	*29*	22	*15*	*30*	*30*	18	*30*	*70*	*30*	30	*30*	*30*	*30* 8596		*30* 8598	
8600	*30*	*15*	*30*	30	*16*	30	*18*	*15*	*31* 8608		*22*	*78*	*30*	30	*29*	30	*28*	30	30	*30*
8620	30	*36*	*15* 8622		*30*	*16*	30 8626		*30* 8628		*30*	*15*	*29*	*88*	*30*	30	*30*	30	*15*	*52*
8640	*30* 8640		*30*	16	*30*	30	*30* 8646		*30*	*15*	*15*	*40*	*30*	30	*30*	16	*29*	*30*	*30*	30
8660	*30*	*15*	*29* 8662		*30*	30	*30*	*80*	*30* 8668		*30*	*30*	*31*	*15*	*15*	*24*	*30* 8676		*15*	*15*
8680	*15* 8680		*15*	30	*30*	*15*	*15*	30	*30* 8688		*30*	*15*	*15* 8692		*30*	30	*30*	*15*	*15* 8698	
8700	*30*	*18*	*15*	16	*16*	30	*15* 8706		*30*	*15*	*15*	*30*	*30* 8712		*30*	*30*	*15*	30	*30* 8718	
8720	*15*	30	*15*	30	*30*	30	*30*	30	*16*	30	*18* 8730		*15*	30	*22*	30	*30* 8736		*30*	30
8740	*28* 8740		30	*30*	*30*	*15*	*15* 8746		*30*	30	*30*	30	*30* 8752		*30*	30	*30*	*15*	*30*	30
8760	*30* 8760		*15*	30	*30*	*15*	*30*	30	*63*	30	*30*	*48*	*30*	*30*	*30*	*30*	*15*	*66*	*30* 8778	
8780	*30*	30	*30* 8782		*30*	30	*30*	30	*15*	30	*30*	*58*	*30*	30	*30*	30	*22*	30	*30*	30
8800	*31*	30	*28* 8802		30	*30*	30 8806		*30*	30	*30*	30	*30*	30	*30*	30	*30*	30	*30* 8818	
8820	*30* 8820		*30*	30	*30*	30	*30*	30	*30*	*80*	*30* 8830		*30*	*72*	*30*	*15*	*30* 8836		*30* 8838	
8840	*30*	*15*	*30*	*36*	*30*	30	*30*	30	*30* 8848		*30*	*52*	*30*	30	*30*	30	*30*	*16*	*30*	30
8860	*30* 8860		*30* 8862		*31*	*15*	*15* 8866		*30*	*48*	*30*	30	*15*	30	*30*	*70*	*30*	30	*30*	30
8880	*30*	*82*	*30*	*15*	*30*	*28*	*30* 8886		*15*	*15*	*30*	30	*30* 8892		*30*	16	*63*	*15*	*30*	30
8900	*30*	*30*	*30*	30	*30*	30	*15*	30	*30*	*58*	*30*	30	*30*	30	*15*	30	*15*	*36*	*15*	30
8920	*15*	30	*30* 8922		*30*	*15*	*15*	*78*	*15* 8928		*30*	30	*15* 8932		*30*	30	*30*	30	*30*	30
8940	*30* 8940		*30*	30	*30*	*40*	*30*	*22*	*15*	30	*30* 8950		*30*	30	*30*	*15*	*15*	*52*	*15*	*30*
8960	*30*	30	*30* 8962		*30*	30	*30*	*30*	*30* 8968		*30* 8970		*30*	18	*30*	30	*16*	*46*	*18*	*15*
8980	*30*	30	*30*	30	*30*	30	*26*	30	*30*	*88*	30	*36*	*31*	30	*15*	30	*30*	*15*	30 8998	

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
9000	30	9000	30	15	15	30	30	9006	30	30	15	9010	30	9012	30	16	30	70	69	30
9020	30	66	15	30	30	30	30	60	15	9028	30	30	30	15	16	30	30	30	30	48
9040	30	9040	30	9042	30	15	28	82	30	9048	30	15	15	34	36	30	31	30	40	9058
9060	42	16	30	24	46	30	48	9066	30	18	52	46	30	42	15	15	58	30	60	30
9080	30	63	15	30	66	30	30	30	70	60	30	9090	15	30	15	30	30	30	30	30
9100	16	30	18	9102	15	30	22	30	30	9108	30	30	28	30	30	30	30	15	15	30
9120	30	30	30	30	30	72	30	9126	30	16	30	30	30	9132	15	30	30	9136	30	30
9140	30	30	30	40	30	15	15	30	15	30	30	9150	63	80	30	30	30	9156	30	30
9160	15	9160	30	16	30	30	30	88	15	52	30	30	30	9172	15	24	15	30	15	66
9180	30	9180	30	30	30	30	30	9186	30	30	30	30	30	28	15	15	30	30	30	9198
9200	30	30	30	9202	30	30	15	15	30	9208	30	60	15	15	30	30	30	30	15	30
9220	30	9220	30	22	15	30	15	9226	30	18	30	30	30	30	30	15	30	15	15	9238
9240	30	9240	30	30	15	30	30	16	31	30	30	30	30	18	15	15	30	9256	15	46
9260	15	26	30	58	30	16	15	15	15	15	15	72	71	15	30	68	30	9276	15	30
9280	63	9280	30	9282	15	30	15	36	16	15	18	30	15	9292	30	48	24	15	26	16
9300	28	70	30	31	15	17	30	40	36	30	30	9310	40	66	42	30	30	26	46	9318
9320	48	30	30	9322	52	24	30	15	15	30	58	17	60	30	30	63	68	9336	66	30
9340	30	9340	70	9342	72	30	30	15	15	9348	15	40	30	46	30	15	16	15	15	48
9360	30	15	15	15	30	15	30	16	15	26	15	9370	30	15	15	15	31	9376	15	82
9380	15	15	15	17	15	15	15	15	15	40	15	9390	15	15	15	15	15	9396	15	15
9400	15	15	15	9402	15	15	15	22	15	9408	15	15	15	9412	15	15	15	15	15	9418
9420	15	9420	15	26	15	15	15	15	15	15	15	9430	15	9432	15	15	15	9436	15	9438
9440	15	15	15	15	15	15	15	15	15	15	15	15	15	29	15	16	15	48	15	15
9460	15	9460	15	9462	15	15	15	9466	15	16	15	15	36	9472	15	24	15	18	15	9478
9480	15	18	15	15	15	23	15	52	15	16	15	9490	15	15	15	22	15	9496	15	26
9500	15	28	15	30	31	18	15	15	15	36	15	9510	15	17	15	15	15	30	30	15
9520	15	9520	15	88	15	15	15	30	15	30	15	26	15	9532	16	30	63	15	15	9538
9540	22	15	24	15	26	30	28	9546	30	30	30	9550	15	40	30	15	15	30	30	78
9560	30	15	15	72	30	30	30	30	31	30	30	17	15	15	15	30	30	60	30	15
9580	15	30	15	30	30	15	15	9586	30	42	30	15	15	52	15	30	30	15	30	30
9600	30	9600	15	15	15	15	30	30	15	15	15	30	15	9612	30	15	15	58	30	9618
9620	30	15	15	9622	30	30	30	15	15	9628	30	9630	31	15	15	30	15	30	30	15
9640	15	30	30	9642	30	30	15	30	30	9648	15	30	15	48	30	30	30	30	16	30
9660	18	9660	15	30	63	30	30	30	30	30	28	30	30	30	30	15	15	9676	30	9678
9680	30	30	30	30	30	30	30	15	30	9688	30	30	15	30	30	17	30	9696	30	30
9700	30	88	30	30	30	30	15	30	30	30	30	30	30	30	30	30	30	30	15	9718
9720	30	9720	30	30	30	30	22	70	30	30	30	36	28	9732	30	30	30	30	30	9738
9740	30	30	30	9742	30	30	30	30	30	9748	30	48	30	30	30	30	30	30	30	30
9760	30	42	30	30	30	16	30	9766	30	9768	30	16	30	30	30	30	30	30	30	30
9780	30	9780	30	30	30	30	30	9786	30	30	30	9790	30	30	30	16	15	96	30	40
9800	30	80	15	9802	30	15	30	30	30	30	30	9810	30	15	30	15	30	9816	15	15
9820	30	30	30	30	31	16	15	30	30	9828	30	30	30	9832	30	30	15	30	30	9838
9840	30	30	30	30	16	30	18	42	15	30	22	9850	30	58	30	30	28	9856	30	9858
9860	30	30	15	30	30	30	30	30	30	70	30	9870	30	30	30	78	30	30	17	30
9880	30	40	30	9882	30	30	30	9886	30	15	15	30	30	30	30	30	30	30	30	30
9900	30	9900	30	30	30	30	30	9906	30	30	30	30	30	30	30	30	30	46	30	15
9920	16	30	30	9922	30	24	30	30	30	9928	30	9930	30	30	30	30	30	39	15	15
9940	30	9940	30	60	30	30	30	30	30	9948	17	15	31	36	30	30	15	16	30	46
9960	30	30	15	40	30	30	30	9966	15	30	15	58	30	9972	30	30	30	30	30	30
9980	30	15	15	66	30	30	30	30	15	30	30	96	30	30	30	30	30	18	15	15

3.88 Table Unknown sets of k MOLS, $k \leq 15$. Under the entry k are given the sides for which k MOLS are unknown, but $k-1$ MOLS are known.

k	Missing Orders													
2	2	6												
3	3	10												
4	4	14	18	22										
5	5	15	20	26	30	34	38	46	60					
6	12	21	28	33	35	39	42	44	51	52	54	58	62	66
	68	74												
7	7	45	50	55	63	69	70	76	77	78	84	85	86	87
	90	92	93	94	95	98	102	106	108	110	111	114	116	118
	119	122	123	124	126	130	132	134	138	140	142	146	148	150
	156	159	162	164	166	170	172	174	175	178	180	182	183	186
	188	190	194	196	198	202	204	206	212	214	218	220	222	226
	228	230	234	236	238	242	244	246	250	252	258	260	274	278
	282	284	286	290	291	292	294	295	306	322	326	330	335	338
	340	346	348	354	358	362	366	426	430	434	436	478	482	486
	490	492	494	498	506	510	566	570						
8	8	24	40	56	57	65	72	75	88	91	96	104	105	115
	120	129	133	135	136	141	145	147	152	155	158	161	165	168
	184	192	195	200	203	213	215	216	231	232	235	237	240	245
	248	249	255	264	266	268	270	280	287	296	300	301	302	303
	308	309	310	312	314	316	318	327	328	332	334	339	344	345
	356	363	364	370	372	374	376	378	380	382	386	388	390	392
	394	395	398	399	402	406	410	418	420	422	424	427	428	438
	440	442	444	446	450	452	453	454	456	458	460	462	466	470
	472	476	485	488	495	500	504	508	514	530	534	542	545	546
	548	550	552	553	554	555	556	558	561	562	564	565	567	568
	572	573	578	579	580	582	584	586	588	591	596	597	604	610
	616	618	626	630	632	634	636	638	642	644	645	646	650	651
	652	654	655	658	660	662	664	666	668	670	674	678	680	682
	686	690	694	696	698	702	706	710	712	716	728	734	735	740
	741	742	744	746	748	750	760	782	790	834	836	852	858	866
	872	874	876	886	888	930	932	933	934	936	938	940	942	946
	948	952	954	956	982	994	1000	1006	1016	1018	1020	1022	1026	1032
	1034	1070	1074	1076	1118	1122	1124	1126	1130	1138	1140	1142	1144	1146
	1150	1154	1162	1218	1220	1224	1226	1228	1230	1236	1238	1240	1245	1252
	1253	1254	1258	1260	1263	1326	1412	1418	1422	1430	1432	1436	1438	1442
	1448	1450	1452	1592	1614	1622	1624	1626	1628	1630	1638	1640	1642	1646
	1650	1658	1678	1718	1726	1734	1736	1738	1814	1926	2408	2410	2418	2668
	2766													
9	9	36	48	82	99	100	117	153	154	171	189	201	205	207
	217	225	261	262	265	324	333	336	350	360	393	396	405	408
	412	468	469	484	516	518	520	526	532	536	549	576	581	585
	594	598	612	614	620	622	627	628	633	635	639	648	676	684
	692	700	708	718	722	738	747	754	756	758	762	764	766	770
	772	774	778	780	796	802	804	806	808	810	812	814	818	819
	820	822	824	826	828	830	835	840	842	844	846	868	878	882
	884	890	894	898	902	903	904	906	908	914	921	927	958	964
	966	968	970	996	1012	1036	1042	1044	1046	1048	1050	1052	1054	1058
	1059	1060	1062	1064	1066	1078	1082	1084	1086	1090	1092	1094	1096	1098

k	Missing Orders
	1100 1102 1106 1108 1110 1112 1114 1116 1128 1132 1141 1156 1180 1182
	1186 1188 1190 1192 1194 1196 1198 1202 1204 1206 1208 1210 1212 1214
	1222 1234 1242 1244 1246 1248 1250 1251 1255 1256 1257 1274 1292 1304
	1306 1310 1316 1318 1320 1322 1324 1330 1332 1336 1342 1378 1380 1382
	1384 1386 1388 1390 1394 1396 1402 1404 1405 1406 1410 1419 1460 1462
	1464 1466 1478 1492 1496 1540 1545 1554 1557 1558 1564 1570 1572 1576
	1578 1580 1582 1586 1587 1588 1590 1594 1596 1598 1602 1604 1606 1608
	1610 1612 1618 1620 1634 1636 1702 1704 1706 1708 1714 1720 1730 1732
	1742 1746 1748 1750 1758 1762 1766 1768 1770 1772 1774 1780 1782 1784
	1786 1788 1790 1796 1798 1800 1802 1806 1810 1812 1864 1868 1874 1880
	1883 1884 1885 1886 1890 1894 1896 1898 1900 1906 1912 1930 1935 1942
	1946 1948 1954 1956 1958 1960 1962 1964 1966 1970 1972 1974 2018 2022
	2028 2030 2038 2040 2042 2044 2046 2050 2052 2054 2056 2060 2066 2068
	2070 2072 2076 2082 2084 2086 2092 2098 2132 2180 2194 2204 2210 2216
	2222 2246 2252 2258 2270 2278 2284 2340 2342 2346 2348 2350 2354 2360
	2362 2364 2366 2372 2374 2378 2380 2382 2386 2388 2390 2392 2394 2402
	2404 2412 2420 2422 2428 2434 2500 2504 2518 2594 2618 2628 2630 2636
	2638 2642 2650 2660 2674 2676 2678 2682 2686 2690 2694 2696 2702 2708
	2714 2738 2740 2742 2746 2750 2756 2762 2774 2810 2822 2828 2844 2846
	2852 2856 2858 2860 2872 2876 2878 2890 2904 2906 2908 2916 2920 2990
	3014 3076 3110 3114 3116 3122 3126 3128 3134 3140 3196 3642 3678
10	80 160 177 185 254 279 329 355 357 415 502 640 721 870
	1014 1028 1030 1038 1135 1233 1266 1268 1270 1276 1278 1286 1338 1348
	1354 1366 1372 1398 1413 1414 1416 1420 1426 1428 1434 1444 1446 1454
	1502 1506 1508 1510 1512 1514 1515 1516 1518 1521 1522 1524 1526 1527
	1528 1533 1534 1682 1688 1694 1698 1700 1722 1724 1740 1752 1754 1756
	1764 1778 1794 1804 1816 1818 1820 1822 1826 1828 1832 1834 1836 1838
	1844 1850 1925 1929 1976 1978 1980 1982 1986 1988 1998 2004 2005 2008
	2010 2062 2074 2116 2134 2140 2142 2146 2148 2150 2152 2158 2162 2164
	2166 2168 2174 2178 2182 2184 2186 2188 2190 2196 2200 2206 2266 2298
	2302 2308 2314 2318 2326 2332 2338 2344 2356 2358 2365 2406 2436 2438
	2440 2452 2454 2456 2458 2470 2488 2494 2506 2514 2526 2532 2546 2550
	2556 2562 2568 2580 2607 2612 2662 2664 2666 2670 2680 2684 2698 2700
	2712 2722 2724 2732 2744 2748 2754 2758 2764 2780 2794 2798 2804 2814
	2824 2834 2836 2854 2866 2884 2886 2898 2914 2918 2924 2926 2930 2936
	2942 2946 2948 2950 2952 2954 2956 2958 2962 2964 2966 2968 2970 2972
	2980 2984 2986 2988 2994 2996 2998 3000 3002 3006 3010 3012 3022 3028
	3042 3046 3052 3058 3062 3064 3070 3082 3084 3092 3098 3100 3102 3106
	3108 3112 3118 3124 3130 3138 3146 3166 3170 3208 3238 3244 3256 3258
	3270 3284 3292 3298 3310 3314 3316 3320 3322 3324 3326 3338 3382 3386
	3434 3464 3466 3470 3478 3490 3492 3500 3508 3512 3518 3608 3614 3618
	3622 3628 3638 3640 3646 3652 3656 3658 3668 3670 3676 3688 3718 3726
	3730 3736 3738 3740 3748 3754 3772 3806 3814 3816 3850 3866 3868 3870
	3882 3896 3910 3926 3930 3932 3940 3944 4012 4014 4022 4024 4028 4030
	4036 4054 4070 4100 4106 4126 4152 4156 4214 4216 4222 4246 4252 4268
	4286 4298 4312 4316 4606 4614 4616 5032 5048 5414 5542 5544 5564 5804
11	11 143 144 187 210 219 267 276 297 298 315 319 341 342
	365 414 429 474 522 538 583 649 724 737 749 786 845 892
	910 917 972 1068 1134 1243 1282 1397 1400 1408 1468 1530 1654 1716
	1902 1941 1992 2058 2088 2122 2154 2170 2212 2236 2274 2343 2359 2367
	2370 2373 2379 2396 2442 2444 2446 2460 2566 2658 2692 2706 2710 2716

k	Missing Orders
	2718 2726 2728 2730 2734 2770 2850 2910 2932 2974 2982 3004 3016 3018
	3094 3142 3182 3186 3250 3262 3268 3278 3286 3300 3302 3304 3306 3308
	3332 3352 3356 3362 3372 3374 3394 3436 3444 3471 3474 3484 3494 3496
	3502 3506 3510 3514 3538 3554 3558 3578 3580 3588 3590 3598 3602 3620
	3624 3634 3636 3650 3666 3672 3674 3682 3686 3690 3692 3694 3698 3714
	3716 3720 3722 3732 3734 3742 3746 3750 3756 3762 3766 3786 3790 3796
	3802 3820 3826 3828 3836 3838 3842 3844 3846 3862 3874 3878 3880 3884
	3886 3890 3992 3994 4002 4006 4042 4066 4072 4082 4116 4118 4130 4138
	4146 4148 4178 4180 4198 4210 4218 4228 4234 4242 4258 4262 4282 4292
	4302 4324 4414 4450 4468 4482 4484 4492 4498 4500 4502 4504 4514 4516
	4518 4520 4526 4532 4534 4536 4538 4546 4548 4550 4552 4554 4566 4568
	4580 4582 4584 4586 4594 4596 4600 4602 4618 4774 4776 4792 4804 4810
	4822 4836 4838 4840 4852 4854 4858 4870 4882 4888 4906 4918 4924 4942
	4952 4954 4958 4972 4982 4986 4990 4996 5002 5010 5014 5020 5022 5026
	5028 5030 5034 5036 5038 5042 5046 5050 5052 5058 5062 5064 5068 5074
	5098 5110 5116 5118 5122 5128 5138 5158 5332 5350 5368 5458 5482 5506
	5516 5518 5522 5524 5528 5534 5538 5540 5546 5556 5558 5560 5570 5606
	5614 5666 5668 5702 5726 5730 5746 5786 5788 5794 5798 5810 5816 5818
	5820 5826 5830 5832 5834 5836 5842 5844 5846 5850 5852 5858 5860 5862
	5866 5868 5878 5880 5882 5884 5942 6082 6118 6438 6606 6610 6766 7222
12	209 404 447 1652 2036 3493 3505 3542 3548 3560 3566 3572 3594 3596
	3626 3630 3644 3660 3662 3724 3914 4124 4136 4154 4442 4466 4530 4562
	4564 4578 4612 4772 4842 4850 4856 4860 4872 4874 4878 4922 4932 4936
	4962 4984 5000 5012 5044 5060 5108 5140 5144 5354 5420 5432 5448 5450
	5468 5554 5604 5626 5704 5710 5734 5740 5752 5754 5758 5764 5766 5770
	5772 5782 5796 5800 5802 5806 5812 5828 5848 5864 5870 5876 5894 5972
	5978 6116 6158 6172 6184 6226 6404 6452 6504 6520 6534 6548 6552 6580
	6586 6596 6598 6604 6616 6618 6626 6628 6632 6634 6636 6646 6652 6658
	6660 6664 6676 6694 6706 6712 6716 6724 6728 6730 6742 6746 6770 7286
13	13 221 247 253 259 285 299 325 351 381 413 501 517 524
	533 540 559 602 637 723 726 788 832 850 923 949 950 974
	1080 1158 1160 1261 1284 1314 1340 1346 1417 1470 1532 1574 1656 1842
	2090 2156 2172 2198 2214 2276 2353 2426 2462 2484 2524 2586 2587 2588
	2772 2934 2978 3020 3144 3188 3206 3330 3368 3498 3516 3524 3563 3565
	3654 3758 3764 3950 4200 4250 4260 4322 4386 4402 4420 4428 4438 4452
	4456 4470 4486 4506 4522 4540 4556 4558 4570 4572 4588 4598 4604 4622
	4658 4674 4738 4786 4826 4828 4834 4844 4866 4876 4902 4930 4966 4978
	5066 5092 5164 5330 5362 5398 5418 5428 5474 5510 5548 5562 5588 5618
	5624 5814 5854 5886 5908 5956 6068 6074 6076 6106 6142 6182 6470 6502
	6518 6536 6554 6670 6674 6682 6684 6696 6702 6726 6744 6764 6788 7288
14	112 224 275 377 411 445 896 1010 1490 2034 2398 2863 3355 3442
	3453 3495 3603 4238 4254 4364 4366 4394 4396 4404 4408 4424 4426 4444
	4454 4458 4460 4462 4472 4474 4476 4478 4488 4490 4494 4508 4510 4524
	4542 4574 4590 4610 4628 4766 5130 5146 5148 5242 5426 5594 5822 5838
	5874 5890 5892 5896 5898 5900 5902 5906 5910 5912 5914 5916 5918 5924
	5926 5928 5930 5932 5934 5960 5966 5976 5990 6038 6040 6098 6434 6454
	6484 6486 6498 6514 6530 6790 7154 7190 7192 7258 7274 7314 7316 7618
	7740 7838 7858 7874
15	176 208 600 913 935 1509 2165 2171 2424 3328 4664 4670 4676 4684
	4694 4796 4814 4862 5384 5508 5756 6550 6686 6700 6718 7244 7674 7720
	7722 7738 7754 7780 7786 7826 7844 8282 8338 8354 8360

3.7 Maximal Sets of MOLS

3.89 A k Max MOLS(n) is a set of k MOLS of side n that is maximal (cannot be extended to a set of $k+1$ MOLS of side n).

3.90 **Example** 1 Max MOLS(5), 1 Max MOLS(7), and 2 Max MOLS(8).

1	2	5	3	4
4	1	2	5	3
2	3	1	4	5
3	5	4	1	2
5	4	3	2	1

1	2	3	4	5	6	7
2	1	4	5	6	7	3
3	4	5	7	1	2	6
4	5	7	6	3	1	2
5	6	2	3	7	4	1
6	7	1	2	4	3	5
7	3	6	1	2	5	4

1	2	3	4	5	6	7	8
2	3	4	1	8	5	6	7
3	4	1	2	7	8	5	6
4	1	2	3	6	7	8	5
5	6	7	8	1	2	3	4
6	7	8	5	4	1	2	3
7	8	5	6	3	4	1	2
8	5	6	7	2	3	4	1

1	3	6	8	2	4	5	7
2	4	5	7	3	1	8	6
3	1	8	6	4	2	7	5
4	2	7	5	1	3	6	8
5	7	2	4	6	8	1	3
6	8	1	3	7	5	4	2
7	5	4	2	8	6	3	1
8	6	3	1	5	7	2	4

3.91 **Example** 2 Max MOLS(7) and 3 Max MOLS(8).

1	2	3	4	5	6	7
2	3	4	5	6	7	1
3	4	5	6	7	1	2
4	5	6	7	1	2	3
5	6	7	1	2	3	4
6	7	1	2	3	4	5
7	1	2	3	4	5	6

1	4	7	2	6	5	3
2	5	1	3	7	6	4
3	6	2	4	1	7	5
4	7	3	5	2	1	6
5	1	4	6	3	2	7
6	2	5	7	4	3	1
7	3	6	1	5	4	2

1	5	2	6	3	7	4	8
5	1	6	2	7	3	8	4
2	6	3	7	4	8	1	5
6	2	7	3	8	4	5	1
3	7	4	8	1	5	2	6
7	3	8	4	5	1	6	2
4	8	1	5	2	6	3	7
8	4	5	1	6	2	7	3

1	8	6	3	4	5	7	2
5	4	2	7	8	1	3	6
2	5	7	4	1	6	8	3
6	1	3	8	5	2	4	7
3	6	8	1	2	7	5	4
7	2	4	5	6	3	1	8
4	7	5	2	3	8	6	1
8	3	1	6	7	4	2	5

1	4	7	8	2	3	6	5
5	8	3	4	6	7	2	1
2	1	8	5	3	4	7	6
6	5	4	1	7	8	3	2
3	2	5	6	4	1	8	7
7	6	1	2	8	5	4	3
4	3	6	7	1	2	5	8
8	7	2	3	5	6	1	4

3.92 **Theorem** If there exists an $(n, r; 1)$-difference matrix D (see §VI.17) for which $mD = (D \dots D)$ (that is, m consecutive copies of D) is maximal and if either $m = 1$ or there exist $r-1$ MOLS of side m, then there exists an $r-1$ Max MOLS(nm).

3.93 **Theorem** If n does not divide m and there exists a projective plane of order n and $n-1$ MOLS of side m, then there exists an $n-1$ Max MOLS(nm).

3.94 **Theorem** If $n = mp^r$, p a prime, $\gcd(m, p) = 1$, and either $m = 1$ or there exist $p-1$ MOLS of side m, then there exists a $p-1$ Max MOLS(n).

3.95 **Theorem** [1226, 1596] Let $d = n-1-k$, $b(x) = \frac{1}{2}x^4 + x^3 + x^2 + \frac{1}{2}x$, and $m(x) = 8x^3 - 18x^2 + 8x + 4 - 2R(x^2 - x - 1) + 9R(R-1)(x-1)/2$, where $R \in \{0, 1, 2\}$, $R \equiv d+1 \pmod 3$. If there exists a k Max MOLS(n), then either $k = n-1$ (corresponding to a projective plane of order n), or $b(d-1) \geq n$ (Bruck's bound) and $m(d) \geq 3n$ (Metsch's bound).

3.96 **Theorem** If G is a group of order n with a unique element of order 2, then the Cayley table of G is a 1 Max MOLS(n).

3.97 **Theorem** [801, 2123] For all $n > 3$, there exists a 1 Max MOLS(n), a *bachelor square*.

3.98 **Construction** When $n \equiv 1, 2 \pmod 4$, let L be a latin square of side $4t+2$ (alternatively $4t+1$) with a subsquare of side $2t+1$ ($2t$) in which all entries are from a set of $2t+1$ ($2t$) except for t ($\frac{t-1}{2}$) or fewer cells. Then L is a 1 Max MOLS(n).

3.99 **Theorem** If $n = q_1 \cdots q_r$ is the factorization of n into prime powers that are relatively prime with $q_1 < \cdots < q_r$, then there exists a $q_1 - 1$ Max MOLS(n).

3.100 **Theorem** Let $p \geq 7$ be a prime. If $p \equiv 3 \pmod 4$, then there exists a $(p-3)/2$ Max MOLS(p). If $p \equiv 1 \pmod 4$, then there exists a $(p-1)/2$ Max MOLS(p).

3.101 **Theorem** If $q = p^r$, p a prime, then there exists a k Max MOLS(q^2) for $k = q^2 - q - 1$, and if $p \geq 5$, for $k = q^2 - q - 2$ and $q^2 - q$ [1226, 1229].

3.102 Table The values of k for which a k Max MOLS(n) is known to exist. B_n is the best known bound for which no k Max MOLS(n), $B_n \le k < n-1$, exists. This extends the table in [1226], using results in [751, 938] as well. There do not exist 4 Max MOLS(8) [750].

n	B_n	k	n	B_n	k	n	B_n	k
2		1	22	19	1	42	38	1,2
3	1	2	23	20	1,10,22	43	39	1,2,20,42
4	2	1,3	24	20	1,2,5	44	40	1,3
5	2	1,4	25	21	1,2,4,12,18–20,24	45	41	1,2,4
6	2	1	26	22	1	46	42	1,2,4
7	3	1,2,6	27	23	1,2,12,26	47	43	1,2,22,46
8	4	1–3,7	28	24	1–3	48	44	1,2
9	6	1–3,5,8	29	25	1,2,14,28	49	45	1,3,5,6,24,40–42,48
10	7	1,2	30	26	1,2	50	46	1,6
11	8	1–4,10	31	27	1,2,14,30	51	47	1,2
12	9	1–3,5	32	28	1,31	52	48	1–3
13	10	1–4,6,12	33	29	1–3	53	49	1,26,52
14	11	1	34	30	1,2	54	50	1
15	12	1,2,4	35	31	1,4	55	51	1,2,4
16	13	1,2,7,8,11,15	36	32	1–4	56	52	1,3,6
17	14	1,3,4,8,16	37	33	1,2,18,36	57	53	1–3,7
18	15	1	38	34	1	58	54	1
19	16	1,3,6,8,18	39	35	1,2	59	55	1,28,58
20	17	1,3,4	40	36	1,4	60	56	1–4
21	18	1,2,4	41	37	1,20,40	61	57	1,2,4,30,60

3.8 Related Problems

3.103 Two latin squares on the same set of symbols are *r-orthogonal* if, when superimposed, there are exactly r distinct ordered pairs.

3.104 Theorem [586, 2215] For n a positive integer, two r-orthogonal latin squares of side n exist if and only if $r \in \{n, n^2\}$ or $n+2 \le r \le n^2-2$, except when

1. $n = 2$ and $r = 4$;
2. $n = 3$ and $r \in \{5, 6, 7\}$;
3. $n = 4$ and $r \in \{7, 10, 11, 13, 14\}$;
4. $n = 5$ and $r \in \{8, 9, 20, 22, 23\}$;
5. $n = 6$ and $r \in \{33, 36\}$.

3.105 An *orthogonal latin square graph* of *order* n (OLSG(n)) is a graph with vertex set V and edge set E, where V corresponds to a set of latin squares of side n, and an edge connects two vertices exactly when the corresponding latin squares are orthogonal. A graph is *n-realizable* when it isomorphic to an OLSG(n).

3.106 Theorem (see [725]) Let G be a graph. There exists an integer n_G depending only upon G, such that G is n-realizable for all $n > n_G$.

3.107 Theorem (see [725]) The 6-cycle is n-realizable by the six conjugates of a single latin square of side n for all $n \ge 43$. The complete graph on 6 vertices is n-realizable by the six conjugates of a single latin square of side n whenever a PBD of order n exists whose block sizes are prime powers at least 8, and, hence, for all $n \ge 1803$ (see Table IV.3.24).

3.108 Theorem [353] Two orthogonal diagonal latin squares of side s exist if and only if $s \neq 2$, 3, or 6. (See §III.1.10.)

3.109 Theorem [755] Three orthogonal diagonal latin squares of side s exist except when $s \in \{2, 3, 4, 5, 6\}$ and possibly when $s \in \{10, 14, 15, 18, 21, 22, 26, 30, 33, 34, 46\}$.

3.110 Suppose L and M are idempotent, symmetric latin squares of the same order. Then L and M are *orthogonal-symmetric* latin squares if, for any two elements x and y, there exists at most one ordered pair (i, j) with $i < j$ such that $L(i, j) = x$ and $M(i, j) = y$.

3.111 Remark Orthogonal-symmetric latin squares are not orthogonal latin squares, but they are as "orthogonal" as possible, given that they are symmetric.

3.112 Remark The existence of a set of t pairwise orthogonal-symmetric latin squares of order n is equivalent to the existence of a Room t-cube of side n (§VI.50) and to the existence of t pairwise orthogonal 1-factorizations of K_{n+1} (§VII.5).

3.113 Remark Orthogonal-symmetric latin square graphs (OSLSG) can be defined in a similar manner to orthogonal latin square graphs. Theorems similar to Theorems 3.106 and 3.107 for OSLSG are discussed in [725]. In that survey, such graphs are termed *orthogonal one-factorization graphs* (OOFG) with underlying graph K_n.

3.114 Let V be a set of $2n + 1$ elements. A *golf design of order* $2n + 1$ is a set of $2n - 1$ symmetric idempotent latin squares, $L_1, L_2, \ldots, L_{2n-1}$, defined on V such that L_i and L_j are disjoint off the main diagonal; that is, for $x, y \in V$, $L_i(x, y) \neq L_j(x, y)$ for $i, j = 1, 2, \ldots, 2n - 1$.

3.115 Remark Examples of golf designs as well an existence result are given in §VI.51.7.

▷ Mutually orthogonal latin rectangles

3.116 Two latin rectangles are *orthogonal* if when superimposed no ordered pair of symbols appears more than once. A set of $m \times n$ latin rectangles is *mutually orthogonal*, or a *MOLR*(m, n), if every two latin rectangles in the set are orthogonal. The maximum number of MOLR(m, n) is denoted $N(m, n)$.

3.117 Remarks $N(n, m) \leq n-1$ for $2 \leq m \leq n$. $N(n, n) = N(n)$ and hence $N(m, n) = n-1$ when $m \leq n$ and n is a prime power. For small n not a prime power, current lower bounds are given in Table 3.118.

3.118 Table [1065] $N(m, n)$ lower bounds.

$n\backslash m$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
6	4	4	4	1														
10	8	8	8	6	6	5	4	2										
12	11	11	11	11	8	8	7	5	5	5								
14	12	12	11	10	8	7	6	5	5	4	3	3						
15	14	14	11	10	10	10	10	10	10	4	4	4	4					
18	16	16	14	13	12	10	9	8	7	6	5	4	4	4	3	3		
20	19	19	16	15	13	11	10	9	8	7	6	6	5	4	4	4	4	4

▷ Packing arrays: Mutually orthogonal partial latin squares

3.119 A *packing array* $\Pi A(N; k, v)$ is an $N \times k$ array with entries from a v-set, so that every $N \times 2$ subarray contains every ordered pair of symbols at most once. The *packing array number* $\Pi AN(k, v)$ is the largest N for which a $\Pi A(N; k, v)$ exists.

3.120 Remark A $\Pi\mathrm{A}(N;k,v)$ is equivalent to a set of $k-2$ mutually orthogonal partial latin squares of order v, each having the same N cells filled. Hence, a $\Pi\mathrm{A}(v^2;k,v)$ is a $\mathrm{TD}(k,v)$.

3.121 Theorem (see [1960]) If $k > \binom{v+1}{2}$, then $\Pi\mathrm{AN}(k,v) = v$.

3.122 Theorem (Plotkin bound, see [1960]) A $\Pi\mathrm{A}(N;k,v)$ exists only if, for all $M = \alpha v+\beta \le N$ with $0 \le \beta < v$, one finds that $k((v-\beta)\alpha^2+\beta(\alpha+1)^2) < (M-1+k)M$. Moreover, this bound is met with equality when $k \ge 2v+1$.

3.123 Table Bounds for packing array numbers [1960]; **bold** is exact. In each case the upper bound is given; when no lower bound is given, the lower bound from the cell to the right is the best known. The bound $\Pi\mathrm{AN}(6,6) \ge 30$ is a consequence of $N(5,6) = 4$.

k	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3		**9**	**6**	**4**												
4			**16**	**9**	**8**	**4**										
5				**25**	**15**	**10**	**10**	**7**								
6	**36**	**34**	34	30–34	16–34	19	14	**12**	**12**	**9**						
7						**49**	**28**	**21**	15	**14**	**14**	**10**				
8							**64**	22–34	25	19	17	**16**	**16**	**12**		
9								**81**	45	30	**27**	21	19	**18**	**18**	**14**

▷ Ordered pairs of symbols in sets of latin squares

3.124 Remark Consider the problem of constructing sets of s latin squares of order m such that the total number of different ordered pairs obtained by superimposing all pairs of the s squares is as large as possible. The interesting cases occur when $s \ge N(m)$.

3.125 Suppose that L_1 and L_2 are latin squares of order m. Define $P(L_1,L_2)$ to be the number of different ordered pairs that are obtained when L_1 and L_2 are superimposed. Now suppose that $L_1,\ldots,L_s$ are latin squares of order m, where $s > 2$; define $P(L_1,\ldots,L_s) = \sum_{1\le i<j\le s} P(L_i,L_j)$. The maximum value of $P(L_1,\ldots,L_s)$ over all possible sets of s latin squares of order m is denoted $\mathsf{P}(s,m)$.

3.126 Proposition $\mathsf{P}(s,m) \le \binom{s}{2}m^2$, with equality if and only if there exist s MOLS(m).

3.127 Theorem [728] Suppose that $s = a(m-1)+b$, $a \ge 0$, and $0 \le b \le m-2$. Then $\mathsf{P}(s,m) \le m^2\binom{s}{2} - (m^2-m)\left(b\binom{a+1}{2} + (m-1-b)\binom{a}{2}\right) \doteq \Pi(s,m)$.

3.128 Remark The bound in Theorem 3.127 is stronger than the bound in Proposition 3.126 whenever $s \ge m$.

3.129 Theorem [728] If m is a prime power, then $\mathsf{P}(s,m) = \Pi(s,m)$.

3.130 Conjecture [728] Suppose that $s \ge m-1$ and $L_1,\ldots,L_s$ are standardized latin squares of order m such that $P(L_1,\ldots,L_s) = \Pi(s,m)$. Then $\{L_1,\ldots,L_s\}$ contains a subset of $m-1$ MOLS of order m, and the list $L_1,\ldots,L_s$ consists only of copies of these $m-1$ orthogonal latin squares, where each copy occurs either $\lfloor \frac{s}{m-1} \rfloor$ or $\lceil \frac{s}{m-1} \rceil$ times.

▷ Simple orthogonal multi-arrays (SOMAs)

3.131 A *simple orthogonal multi-array*, $\mathrm{SOMA}(k,n)$, is an $n \times n$ array in which each cell contains a k-subset of a set X of size kn, every symbol of X occurs once in every row and once in every column, and every 2-subset of X appears as a subset of the set in at most one cell.

3.132 Remark (see [1934]) A TD(k,n) yields a SOMA$(k-2,n)$. Indeed superimposing $k-2$ MOLS on disjoint sets of symbols is a SOMA (such a SOMA is a *trojan square*).

3.133 Remark (see [1934]) A SOMA(k,n) exists only if $k \leq n-1$. A SOMA$(n-1,n)$ exists if and only if a TD$(n+1,n)$ exists. There exist a SOMA(3,6), a SOMA(3,10), and a SOMA(4,14).

See Also

§II.1, 7	BIBDs, resolvable and near-resolvable designs.
§III.5	Self-orthogonal latin squares (SOLS).
§VI.17	Difference matrices, quasi-difference matrices and $V(m,t)$ vectors are used to construct MOLS.
[543]	Details on constructing MOLS tables.
[544]	A lengthy survey of constructions of MOLS.
[725]	Information on orthogonal latin square graphs is in §15.
[800]	Contains implicit difference matrix constructions of maximal sets of MOLS.
[1230]	An overview of results on maximal sets of MOLS.
[1647]	Proposes existence of projective planes and MOLS as a successor to the Fermat problem.

References Cited: [2, 6, 10, 25, 26, 27, 38, 47, 49, 92, 224, 334, 353, 502, 526, 543, 544, 586, 725, 728, 750, 751, 755, 800, 801, 938, 1065, 1206, 1226, 1229, 1230, 1499, 1596, 1608, 1647, 1669, 1710, 1790, 1819, 1847, 1934, 1960, 2037, 2038, 2117, 2123, 2160, 2161, 2215]

4 Incomplete MOLS

R. Julian R. Abel
Charles J. Colbourn
Jeffrey H. Dinitz

4.1 One Hole

4.1 Two incomplete latin squares (ILS$(n;b_1,b_2,\ldots,b_s)$) are *orthogonal* if upon superimposition all ordered pairs in $(B \times B) \setminus \cup_{i=1}^{k}(B_i \times B_i)$ result. Two such squares are denoted IMOLS$(n;b_1,b_2,\ldots,b_s)$ (or IPOLS$(n;b_1,b_2,\ldots,b_s)$). Similarly, r-IMOLS$(n;b_1,b_2,\ldots,b_s)$ denotes a set of r ILS$(n;b_1,b_2,\ldots,b_s)$ that are pairwise orthogonal.

4.2 $N(n;b_1,b_2,\ldots,b_s)$ denotes the maximum r for which there exist a set of r-IMOLS$(n;b_1,b_2,\ldots,b_s)$.

4.3 Example [798] $N(6;2) = 2$. (The missing subsquares are on the symbols 5 and 6.)

5	6	3	4	1	2
2	1	6	5	3	4
6	5	1	2	4	3
4	3	5	6	2	1
1	4	2	3		
3	2	4	1		

1	2	5	6	3	4
6	5	1	2	4	3
4	3	6	5	1	2
5	6	4	3	2	1
2	4	3	1		
3	1	2	4		

4.4 **Example** [1966] $N(8;2) = 3$. In the matrix shown, replace each column by the five (columnwise) cyclic shifts of the column, and develop each of the resulting columns modulo $(3, -)$. The result is an incomplete orthogonal array with a hole on $\{\infty_0, \infty_1\}$.

$$\begin{pmatrix} \infty_0 & \infty_0 & \infty_1 & \infty_1 \\ (0,1) & (2,0) & (1,0) & (2,1) \\ (2,0) & (2,1) & (2,1) & (0,0) \\ (2,0) & (1,1) & (2,0) & (2,1) \\ (1,0) & (1,1) & (0,0) & (0,1) \end{pmatrix}$$

4.5 **Example** [341] $N(10,2) = 4$. In the matrix, each column $(a,b,c,d,e,f)^T$ is replaced by $(a,b,c,d,e,f)^T$, $(c,a,b,f,d,e)^T$, and $(b,c,a,e,f,d)^T$. Develop each column modulo (2,4) to obtain an incomplete orthogonal array with a hole on $\{\infty_0, \infty_1\}$.

$$\begin{pmatrix} (0,0) & (0,0) & (0,0) & (0,0) \\ (0,2) & (0,1) & (0,0) & (0,3) \\ (1,0) & \infty_0 & (1,1) & \infty_1 \\ (1,1) & (0,2) & (0,0) & (1,3) \\ (1,2) & (0,2) & (0,3) & (1,1) \\ \infty_0 & (1,1) & \infty_1 & (0,3) \end{pmatrix}$$

4.6 **Theorem** If there exists a set of r orthogonal ILS$(n;k)$, then $n \geq (r+1)k$.

4.7 **Remark** Examples 4.3, 4.4, and 4.5 satisfy the bound in Theorem 4.6 with equality.

4.8 **Theorem** (see [1079]) For $k \geq 1$, $N(n;k) \geq 2$ if and only if $n \geq 3k$, and $(n,k) \neq (6,1)$.

4.9 **Example** Two orthogonal ILS$(7;2)$ are given in Example 5.20.

4.2 Equivalent Objects

4.10 An *incomplete transversal design* of *order* or *groupsize* n, *blocksize* k, *index* λ, and *holesizes* $b_1, \ldots, b_s$, denoted $\mathrm{ITD}_\lambda(k, n; b_1, \ldots, b_s)$, is a quadruple $(V, \mathcal{G}, \mathcal{H}, \mathcal{B})$, where

1. V is a set of kn elements;
2. $\mathcal{G}$ is a partition of V into k classes (*groups*), each of size n;
3. $\mathcal{H}$ is a set of disjoint subsets $H_1, \ldots, H_s$ of V, with the property that, for each $1 \leq i \leq s$ and each $G \in \mathcal{G}$, $|G \cap H_i| = b_i$;
4. $\mathcal{B}$ is a collection of k-subsets of V (*blocks*);
5. every unordered pair of elements from V is
   - contained in a hole and contained in no blocks;
   - contained in a group and contained in no blocks; or
   - contained in neither a hole nor a group, and contained in λ blocks.

Again, when $\lambda = 1$, it can be omitted from the notation. An $\mathrm{ITD}(k, n; b_1, \ldots, b_s)$ is also denoted as a $\mathrm{TD}(k,n) - \sum_{i=1}^{s} \mathrm{TD}(k, b_i)$.

4.11 **Theorem** r-IMOLS$(n; b_1, \ldots, b_s)$ is equivalent to

1. an incomplete transversal design $\mathrm{ITD}(r+2, n; b_1, \ldots, b_s)$;
2. an incomplete orthogonal array $\mathrm{IOA}(r+2, n; b_1, \ldots, b_s)$.

4.12 **Remark** r-IMOLS$(n;1)$ and r-IMOLS$(n;0)$ are equivalent to r MOLS of side n.

4.3 Existence

4.13 **Remark** Table 4.14 of lower bounds for $N(n;k)$ is produced using the same program [543] as Table 3.87, the table of lower bounds for $N(n)$.

4.14 **Table** Lower bounds for $N(n;k)$ for $1 \le n \le 1000$ and $0 \le k \le 50$. (* denotes $n-1$ when $n > 100$.)

$h \to$	0										1										2										3										4										5
$n \downarrow$	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
4	3																																																	
5	4																																																		
6	1	2																																																
7	6	2																																																
8	7	3																																																
9	8	3	2																																															
10	2	4	2																																															
11	10	3	2																																															
12	5	3	3	2																																														
13	12	3	3	2																																														
14	3	3	3	2																																														
15	4	4	4	2	2																																													
16	15	3	4	3	2																																													
17	16	4	3	3	2																																													
18	3	3	3	3	2	2																																											
19	18	4	5	3	2	2																																											
20	4	3	3	4	3	2																																											
21	5	3	3	4	3	2	2																																									
22	3	3	4	3	3	2	2																																									
23	22	3	3	4	3	2	2																																									
24	7	3	4	3	3	3	2	2																																								
25	24	3	4	4	4	3	2	2																																								
26	4	3	3	4	4	3	2	2																																								
27	26	3	3	4	4	3	2	2	2																																							
28	5	4	4	4	3	3	3	2	2																																							
29	28	4	3	5	3	3	3	2	2																																							
30	4	3	4	4	5	4	3	2	2	2																																							
31	30	3	3	4	4	4	3	2	2	2																																							
32	31	3	3	3	4	3	3	3	2	2																																							
33	5	4	3	5	3	4	3	3	2	2	2																																						
34	4	3	4	4	3	3	3	3	2	2	2																																						
35	5	4	3	4	4	4	4	3	2	2	2																																						
36	8	3	4	3	6	5	4	3	3	2	2	2																																					
37	36	3	3	4	3	5	4	3	3	2	2	2																																					
38	4	3	3	3	4	3	4	3	3	2	2	2																																					
39	5	3	3	5	3	4	3	3	3	2	2	2	2																																				
40	7	4	5	4	4	4	4	4	3	3	2	2	2																																				
41	40	5	3	3	4	5	3	4	3	3	2	2	2																																				
42	5	3	4	4	3	3	5	3	3	3	2	2	2	2																																			
43	42	5	3	4	4	6	5	4	3	3	2	2	2	2																																			
44	5	3	3	3	5	3	4	3	3	3	3	2	2	2																																			
45	6	3	4	5	5	4	4	3	4	3	3	2	2	2	2																																		
46	4	3	5	4	4	4	4	4	4	3	3	2	2	2	2																																		
47	46	5	3	4	3	5	3	4	3	3	3	2	2	2	2																																		
48	8	3	3	3	3	4	3	5	4	3	3	3	2	2	2	2																																	
49	48	3	3	3	3	7	6	5	4	3	3	3	2	2	2	2																																	
50	6	4	3	3	4	5	6	5	3	4	3	3	2	2	2	2																																	

$h \to$	0	1	2	3	4	5
$n \downarrow$	1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0
51	5 5 3 3 4 5 4 4 4	4 3 3 2 2 2 2 2				
52	5 4 5 5 3 3 3 3 4	3 3 3 3 2 2 2 2				
53	52 4 4 5 3 3 3 4 3	4 3 3 3 2 2 2 2				
54	5 3 3 4 5 3 4 4 5	3 3 3 3 2 2 2 2 2				
55	6 5 3 3 4 5 4 5 5	4 4 3 3 2 2 2 2 2				
56	7 4 4 3 4 4 6 6 3	3 4 3 3 3 2 2 2 2				
57	7 4 4 4 3 5 6 6 5	3 3 3 3 3 2 2 2 2 2				
58	5 6 4 4 5 3 5 5 5	4 3 3 3 3 2 2 2 2 2				
59	58 5 6 4 5 4 4 4 4	4 4 3 3 3 2 2 2 2 2				
60	4 4 5 6 4 4 4 4 3	5 3 4 3 3 3 2 2 2 2	2			
61	60 4 4 5 6 4 4 4 4	5 3 4 3 3 3 2 2 2 2	2			
62	5 4 3 4 5 6 4 5 4	3 3 3 3 3 3 2 2 2 2	2			
63	6 4 5 3 4 5 6 6 6	4 3 3 3 3 3 2 2 2 2	2 2			
64	63 5 5 5 4 4 6 7 6	4 3 3 3 3 3 3 2 2 2	2 2			
65	7 6 5 5 5 4 6 7 6	4 3 3 4 3 3 3 2 2 2	2 2			
66	5 6 6 5 5 5 5 5 5	5 5 3 4 3 3 3 2 2 2	2 2 2			
67	66 5 6 6 5 5 5 5 5	5 4 3 3 3 3 3 2 2 2	2 2 2			
68	5 5 5 6 6 5 5 5 5	3 4 4 3 3 3 3 3 2 2	2 2 2			
69	6 4 5 5 6 6 6 6 6	3 3 4 4 3 3 3 3 2 2	2 2 2 2			
70	6 4 4 5 5 6 6 6 6	4 3 3 3 4 3 3 3 2 2	2 2 2 2			
71	70 5 5 4 5 5 6 6 6	6 4 3 3 4 3 3 3 2 2	2 2 2 2			
72	7 6 5 5 4 5 6 7 7	5 3 5 3 3 3 3 3 3 2	2 2 2 2 2			
73	72 6 6 5 5 5 6 7 7	5 4 5 4 3 3 3 3 3 2	2 2 2 2 2			
74	5 7 6 6 5 5 5 5 5	6 4 3 3 3 3 3 3 3 2	2 2 2 2 2			
75	7 4 7 6 6 5 5 5 5	4 5 3 3 3 4 3 3 3 2	2 2 2 2 2 2			
76	6 4 4 7 6 6 5 5 5	3 4 4 3 3 4 3 3 3 3	2 2 2 2 2 2			
77	6 4 3 4 7 6 6 6 6	4 6 3 4 3 3 3 3 3 3	2 2 2 2 2 2			
78	6 3 3 3 3 7 6 6 6	3 6 5 5 4 3 3 3 3 3	2 2 2 2 2 2 2			
79	78 6 4 3 3 5 7 6 6	4 6 4 4 3 4 3 3 3 3	2 2 2 2 2 2 2			
80	9 6 6 3 4 3 6 7 7	6 6 3 3 3 4 4 3 3 3	3 2 2 2 2 2 2			
81	80 6 6 6 3 3 6 7 8	7 6 3 3 3 3 4 3 3 3	3 2 2 2 2 2 2 2			
82	8 6 6 6 6 3 5 5 8	5 5 5 3 3 3 3 3 3 3	3 2 2 2 2 2 2 2			
83	82 5 6 6 6 6 5 5 5	5 5 4 4 3 3 3 3 3 3	3 2 2 2 2 2 2 2			
84	6 5 5 6 6 6 6 6 5	5 6 5 3 5 3 3 3 3 3	3 3 2 2 2 2 2 2 2			
85	6 5 5 5 6 6 6 6 6	5 6 5 5 5 3 3 4 3 3	3 3 2 2 2 2 2 2 2			
86	6 6 5 5 5 6 6 6 6	6 6 5 3 4 3 4 3 3 3	3 3 2 2 2 2 2 2 2			
87	6 6 6 6 6 6 6 6 6	6 6 4 4 3 4 3 3 3 3	3 3 2 2 2 2 2 2 2 2			
88	7 6 6 6 6 6 7 6 6	7 5 4 3 4 4 3 3 3 3	3 3 3 2 2 2 2 2 2 2			
89	88 6 6 6 6 6 6 7 7	6 7 5 4 3 4 3 4 3 3	3 3 3 2 2 2 2 2 2 2			
90	6 7 5 6 6 6 6 6 6	7 6 5 5 3 5 3 3 4 3	3 3 3 2 2 2 2 2 2 2 2	2		
91	7 5 7 5 6 6 6 7 7	6 7 5 6 4 4 3 3 4 3	3 3 3 2 2 2 2 2 2 2 2	2		
92	6 5 5 7 5 6 6 6 6	6 6 6 6 4 4 4 3 3 3	3 3 3 3 2 2 2 2 2 2 2	2		
93	6 6 5 5 7 6 6 6 6	6 6 5 6 3 4 3 3 3 3	3 3 3 3 2 2 2 2 2 2 2	2 2		
94	6 6 6 5 5 7 6 6 6	6 6 5 6 4 4 4 3 3 3	3 3 3 3 2 2 2 2 2 2 2	2 2		
95	6 6 6 6 5 5 7 6 6	6 6 5 6 4 4 3 4 3 4	3 3 3 3 2 2 2 2 2 2 2	2 2		
96	7 6 6 6 6 5 6 7 7	6 7 6 6 3 4 4 3 4 3	3 3 3 3 3 2 2 2 2 2 2	2 2 2		
97	96 6 6 6 6 6 6 7 7	6 7 6 6 4 4 5 4 3 4	3 3 3 3 3 2 2 2 2 2 2	2 2 2		
98	6 6 6 6 6 6 6 6 5	7 5 5 6 5 4 4 3 4 3	3 3 3 3 3 2 2 2 2 2 2	2 2 2		
99	8 5 6 6 6 6 6 6 8	4 8 5 6 4 4 3 3 3 4	3 3 3 3 3 2 2 2 2 2 2	2 2 2 2		
100	8 6 5 6 6 6 6 6 6	6 8 5 6 3 4 4 3 3 3	4 3 3 3 3 3 2 2 2 2	2 2 2 2		

$h\to$	0	1	2	3	4	5
$n\downarrow$	1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0
101	* 6 6 5 6 6 6 6 6	9 6 5 6 4 4 4 4 3 3	4 3 3 3 3 3 2 2 2 2	2 2 2 2		
102	6 6 6 6 5 6 6 6 6	6 6 6 6 5 4 3 3 4 3	3 3 3 3 3 3 2 2 2 2	2 2 2 2 2		
103	* 6 7 6 6 6 6 6 6	6 6 6 6 4 4 3 3 4 4	3 3 3 3 3 3 2 2 2 2	2 2 2 2 2		
104	7 6 6 6 6 6 6 7 6	6 6 6 7 5 4 4 3 3 3	3 3 3 3 3 3 3 2 2 2	2 2 2 2 2		
105	7 6 6 6 6 6 6 7 7	6 6 6 7 6 4 3 4 3 3	4 4 3 3 3 3 3 2 2 2	2 2 2 2 2 2		
106	6 7 5 6 5 6 6 6 6	7 6 6 6 5 6 4 3 4 3	3 4 3 3 3 3 3 2 2 2	2 2 2 2 2 2		
107	* 5 7 5 6 6 6 7 7	6 7 6 7 4 4 4 4 4 4	3 3 3 3 3 3 3 2 2 2	2 2 2 2 2 2		
108	6 5 5 7 5 6 6 6 6	6 6 7 6 5 4 3 4 4 3	4 3 3 3 3 3 3 3 2 2	2 2 2 2 2 2 2		
109	* 5 5 5 7 6 6 7 7	6 6 6 7 5 4 4 4 4 4	3 4 3 3 3 3 3 3 2 2	2 2 2 2 2 2 2		
110	6 5 5 5 5 7 6 6 6	6 6 6 6 6 4 4 4 3 4	3 4 4 3 3 3 3 3 2 2	2 2 2 2 2 2 2		
111	6 4 5 5 5 6 7 6 6	5 6 6 6 4 5 4 4 3 3	4 4 4 3 3 3 3 3 2 2	2 2 2 2 2 2 2 2		
112	13 4 4 5 5 5 6 7 7	6 5 6 7 3 4 6 4 3 3	3 4 3 3 3 3 3 3 3 2	2 2 2 2 2 2 2 2		
113	* 4 4 4 5 5 6 7 7	5 6 5 7 4 4 6 5 3 3	3 3 4 3 3 3 3 3 3 2	2 2 2 2 2 2 2 2		
114	6 6 4 4 4 5 6 6 6	7 5 6 5 4 4 6 4 4 3	3 3 3 3 3 3 3 3 3 2	2 2 2 2 2 2 2 2 2		
115	7 6 6 4 4 4 6 7 7	6 7 5 7 4 4 6 4 4 5	4 3 3 4 3 3 3 3 3 2	2 2 2 2 2 2 2 2 2		
116	6 6 6 6 4 4 6 6 6	6 6 7 5 4 4 6 4 3 3	4 3 3 3 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2		
117	8 6 6 6 6 4 6 6 8	6 6 6 8 4 4 6 4 3 4	4 4 3 3 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2		
118	6 6 6 6 6 6 6 6 6	6 6 6 6 4 4 6 4 4 4	3 4 4 3 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2		
119	6 6 6 6 6 6 6 6 6	6 6 6 6 6 4 6 6 4 4	4 3 3 4 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2		
120	7 6 6 6 6 6 7 6 6	6 6 6 6 6 6 6 3 4 4	3 4 3 4 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2	2	
121	* 6 6 6 6 6 6 6 6	6 10 9 6 6 6 6 6 4 4	5 4 3 3 4 3 3 3 3 3	3 2 2 2 2 2 2 2 2 2	2	
122	6 6 6 6 6 6 6 6 6	6 6 5 5 5 5 6 6 4 4	3 4 4 3 3 3 3 3 3 3	3 2 2 2 2 2 2 2 2 2	2	
123	6 6 6 6 6 6 6 6 6	6 6 6 5 5 4 6 6 4 4	4 4 3 3 3 3 3 3 3 3	3 2 2 2 2 2 2 2 2 2	2 2	
124	6 6 6 6 6 6 6 6 6	6 6 6 6 5 5 6 6 3 4	4 4 4 3 3 3 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2 2	
125	* 6 6 6 7 6 6 6 6	6 6 6 6 6 5 6 6 3 4	4 4 4 4 4 4 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2 2	
126	6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 4 3	3 4 4 3 3 4 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2 2 2	
127	* 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 4	4 4 3 4 4 4 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2 2 2	
128	* 6 6 6 6 6 6 7 6	6 6 6 6 6 6 7 6 3 4	4 3 3 3 4 3 3 3 3 3	3 3 3 2 2 2 2 2 2 2	2 2 2	
129	7 6 6 6 6 6 7 7	6 6 6 6 6 6 7 6 4 4	4 4 3 3 3 4 3 3 3 3	3 3 3 2 2 2 2 2 2 2	2 2 2 2	
130	6 7 6 6 6 6 6 6	7 6 6 6 6 6 6 5 4	4 4 4 3 3 4 4 3 3 3	3 3 3 2 2 2 2 2 2 2	2 2 2 2	
131	* 6 7 6 6 6 6 7 7	6 7 6 6 6 6 7 6 4 5	4 3 3 4 3 3 3 3 3 3	3 3 3 2 2 2 2 2 2 2	2 2 2 2	
132	6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 3 3	5 4 4 3 4 3 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2 2 2 2 2	
133	7 6 6 6 7 6 6 7 7	6 6 6 7 6 6 7 6 4 6	4 5 4 3 4 4 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2 2 2 2 2	
134	6 6 6 6 6 7 6 6 6	6 6 6 6 7 6 6 6 4 6	4 4 5 3 3 3 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2 2 2 2 2	
135	7 6 6 6 6 6 7 7 7	6 7 6 6 6 7 6 6 4 6	4 4 3 4 4 4 3 4 3 3	3 3 3 3 2 2 2 2 2 2	2 2 2 2 2 2	
136	7 6 6 6 6 6 6 7 7	6 6 6 6 6 6 7 7 5 6	4 4 4 3 4 4 4 4 3 3	3 3 3 3 3 2 2 2 2 2	2 2 2 2 2 2	
137	* 6 6 6 6 6 6 7 7	6 6 6 6 6 6 7 7 5 6	4 4 3 4 4 4 3 3 3 3	3 3 3 3 3 2 2 2 2 2	2 2 2 2 2 2	
138	6 7 6 6 6 6 6 6 7	6 6 6 6 6 6 6 5 6	4 4 4 3 4 3 4 3 3 3	3 3 3 3 3 2 2 2 2 2	2 2 2 2 2 2 2	
139	* 6 7 6 6 6 6 7 7	6 7 6 6 6 6 7 7 4 6	4 4 4 3 4 4 3 4 3 3	3 3 3 3 3 2 2 2 2 2	2 2 2 2 2 2 2	
140	6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 5 6	4 4 4 4 4 3 4 4 4 3	3 3 3 3 3 3 2 2 2 2	2 2 2 2 2 2 2	
141	7 6 6 6 7 6 6 7 7	6 6 6 7 9 6 7 7 5 6	4 4 4 4 4 4 3 4 4 3	3 3 3 3 3 3 2 2 2 2	2 2 2 2 2 2 2 2	
142	6 6 6 6 6 7 6 6 6	6 6 6 6 7 6 6 6 5 6	4 4 4 4 3 4 3 4 3 3	3 3 3 3 3 3 2 2 2 2	2 2 2 2 2 2 2 2	
143	10 6 6 6 6 6 7 6 6	6 10 6 10 6 7 6 6 4 6	4 4 3 4 4 4 4 4 3 3	3 3 3 3 3 3 2 2 2 2	2 2 2 2 2 2 2 2	
144	10 6 6 6 6 6 6 7 8	6 6 6 10 6 6 8 7 6 6	4 4 4 3 4 4 3 4 3 3	3 3 3 3 3 3 3 2 2 2	2 2 2 2 2 2 2 2 2	
145	7 6 6 6 6 6 6 7 7	6 6 11 6 6 6 7 7 7 6	4 4 4 3 5 4 4 3 4 4	3 3 3 3 3 3 3 2 2 2	2 2 2 2 2 2 2 2 2	
146	6 7 6 6 6 6 6 6 6	7 6 6 6 6 6 6 6 6 6	5 4 4 3 3 4 4 4 3 4	3 3 3 3 3 3 3 2 2 2	2 2 2 2 2 2 2 2 2	
147	7 6 9 6 6 6 6 7 7	6 7 6 6 6 6 6 7 4 6	4 5 3 3 3 4 3 4 4 3	3 3 3 3 3 3 3 2 2 2	2 2 2 2 2 2 2 2 2 2	
148	6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 4 6	5 6 4 4 4 4 3 4 4 4	3 3 3 3 3 3 3 3 2 2	2 2 2 2 2 2 2 2 2 2	
149	* 6 6 6 7 6 6 7 7	6 6 6 7 6 6 6 7 4 6	4 5 4 3 4 4 3 3 3 4	3 3 3 3 3 3 3 3 2 2	2 2 2 2 2 2 2 2 2 2	
150	6 6 6 6 6 7 6 6 6	6 6 6 6 7 6 6 6 6 6	4 4 5 4 4 4 4 3 3 3	4 3 3 3 3 3 3 3 2 2	2 2 2 2 2 2 2 2 2 2	2

$h \to$	0	1	2	3	4	5
$n \downarrow$	1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0
151	* 6 6 6 6 6 7 6 6	6 6 6 6 6 7 6 6 6 6	4 4 3 5 4 5 3 3 3 3	4 3 3 3 3 3 3 3 2 2	2 2 2 2 2 2 2 2 2 2	2
152	7 6 6 6 6 6 6 7 7	6 7 6 6 6 6 7 7 6 7	5 4 4 3 5 4 4 4 4 3	3 3 3 3 3 3 3 3 3 2	2 2 2 2 2 2 2 2 2 2	2
153	8 6 6 6 6 6 6 7 8	6 7 6 6 6 6 6 8 6 7	5 4 3 4 4 5 3 4 3 3	3 3 3 3 3 3 3 3 3 2	2 2 2 2 2 2 2 2 2 2	2
154	8 7 5 6 6 6 6 6 6	7 6 6 6 6 6 6 8 6 6	5 4 4 4 4 4 4 4 4 3	3 3 3 3 3 3 3 3 3 2	2 2 2 2 2 2 2 2 2 2	2
155	7 5 7 5 6 6 6 7 7	6 7 6 6 6 6 6 6 6 7	4 4 4 4 3 4 3 4 4 4	4 4 3 3 3 3 3 3 3 2	2 2 2 2 2 2 2 2 2 2	2
156	6 5 5 7 5 6 6 6 6	6 6 7 6 6 6 6 6 6 6	5 4 4 4 4 4 4 4 4 3	4 4 3 3 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2	2
157	* 5 5 5 7 6 6 7 7	6 6 6 7 6 6 6 6 6 7	5 4 4 3 4 4 5 4 4 4	3 4 3 3 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2	2
158	7 5 5 5 5 7 6 7 7	6 7 6 6 7 6 7 6 6 6	5 4 4 4 3 4 4 3 4 3	4 3 3 3 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2	2
159	6 4 5 5 5 6 7 6 6	6 6 6 6 6 7 6 6 6 6	4 4 4 4 4 4 4 4 3 4	3 4 3 3 3 3 3 3 3 3	2 2 2 2 2 2 2 2 2 2	2
160	9 4 5 5 5 6 6 7 7	6 6 6 6 6 6 7 6 6 7	4 4 4 4 4 4 4 4 4 3	4 3 4 3 3 3 3 3 3 3	3 2 2 2 2 2 2 2 2 2	2
161	7 4 5 4 7 6 6 7 7	5 7 6 6 6 6 6 7 6 7	5 4 4 6 4 4 4 3 4 4	3 4 4 3 3 3 3 3 3 3	3 2 2 2 2 2 2 2 2 2	2
162	6 4 5 4 4 6 6 6 6	7 5 6 6 6 6 6 6 7 6	5 4 4 6 5 3 4 4 4 4	4 3 3 3 3 3 3 3 3 3	3 2 2 2 2 2 2 2 2 2	2
163	* 6 5 4 4 6 6 7 7	5 7 5 6 6 6 6 6 6 7	4 4 4 6 4 4 3 4 4 4	4 4 3 3 3 3 3 3 3 3	3 2 2 2 2 2 2 2 2 2	2
164	6 6 6 4 4 6 6 6 6	6 5 7 5 6 6 6 6 6 6	6 4 4 6 4 4 3 4 4 4	3 4 3 3 3 3 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2
165	7 6 6 6 4 6 7 7 7	6 6 5 7 4 6 6 6 6 7	4 5 4 6 4 4 4 4 3 4	4 4 4 4 3 3 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2
166	6 6 6 6 6 4 6 6 6	6 6 6 5 7 $_{10}$ 6 6 6 6	4 4 5 6 4 4 4 4 4 3	4 4 3 4 3 3 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2
167	* 6 6 6 6 6 6 6 6	6 6 6 6 4 7 4 6 6 6	4 4 4 6 4 4 4 4 4 3	4 4 4 3 3 3 3 3 3 3	3 3 2 2 2 2 2 2 2 2	2
168	7 6 6 6 6 6 7 7 7	6 7 6 6 6 4 7 4 6 7	4 5 4 6 6 4 4 4 4 3	3 3 4 3 3 3 3 3 3 3	3 3 3 2 2 2 2 2 2 2	2
169	* 6 6 6 6 6 6 7 7	6 7 6 $_{12}$ 6 6 4 7 4 7	4 4 4 6 6 5 4 4 4 4	4 4 3 4 3 3 3 3 3 3	3 3 3 2 2 2 2 2 2 2	2
170	6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 4 7 4	4 4 4 6 5 4 4 4 4 3	4 3 3 4 4 3 3 3 3 3	3 3 3 2 2 2 2 2 2 2	2
171	8 6 6 6 6 6 6 6 8	6 7 6 6 6 6 6 7 4 8	4 4 4 6 4 4 4 5 4 3	4 4 3 3 4 3 3 3 3 3	3 3 3 2 2 2 2 2 2 2	2
172	6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 4	4 4 4 6 5 4 4 4 4 4	3 3 3 4 3 3 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
173	* 6 6 6 6 6 6 7 6	6 6 6 7 6 6 6 6 6 6	4 4 4 6 5 4 4 4 4 4	4 3 3 4 3 3 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
174	6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 4 4 6 5 4 4 4 4 4	4 4 3 4 3 3 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
175	6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 4 6 6 6 4 4 4 4	4 4 4 3 3 4 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
176	$_{14}$ 6 6 6 6 6 6 6 6	6 $_{10}$ 6 6 6 6 $_{10}$ 6 6 6	6 6 6 6 6 6 4 4 4 4	4 4 4 4 3 4 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
177	9 6 6 6 6 6 6 6 6	6 9 6 6 6 6 9 9 6 6	6 6 6 6 6 6 4 4 4 4	4 4 4 4 4 4 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
178	6 9 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 8 5	5 5 5 6 5 6 4 4 4 4	4 4 3 4 4 3 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
179	* 6 9 6 6 6 6 6 6	6 7 6 6 6 6 7 7 6 7	4 4 4 6 6 6 4 4 4 5	4 4 4 4 3 4 3 3 3 3	3 3 3 3 2 2 2 2 2 2	2
180	6 6 6 9 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 4 4 6 5 6 4 4 4 4	5 4 4 4 3 4 4 3 3 3	3 3 3 3 3 3 2 2 2 2	2
181	* 6 6 6 9 6 6 6 6	6 6 6 6 6 6 6 6 9 6	6 6 4 6 6 6 4 4 4 4	5 4 4 4 4 4 3 3 3 3	3 3 3 3 3 3 2 2 2 2	2
182	6 6 6 6 6 9 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 5 6 4 4 4 4	4 4 4 4 4 4 3 3 3 3	3 3 3 3 3 3 2 2 2 2	2
183	6 6 6 6 6 9 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 5 6 6 4 4 4	4 4 4 4 3 4 4 3 3 3	3 3 3 3 3 3 2 2 2 2	2
184	7 6 6 6 6 6 9 6 6	6 7 6 7 6 6 7 7 6 6	6 6 6 7 6 6 4 4 4 4	4 4 4 4 4 3 3 3 3 3	3 3 3 3 3 3 2 2 2 2	2
185	9 6 6 6 6 6 6 7 9	6 9 6 9 6 6 8 9 6 6	6 6 6 7 6 6 4 4 4 4	4 4 4 4 4 4 4 4 3 3	3 3 3 3 3 3 3 2 2 2	2
186	6 7 6 6 6 9 6 6 6	9 6 6 6 6 6 6 6 6 6	6 6 6 6 5 6 5 4 4 4	4 4 4 4 4 3 4 4 3 3	3 3 3 3 3 3 3 2 2 2	2
187	$_{10}$ 6 7 6 6 6 6 7 7	6 $_{10}$ 6 7 6 6 6 $_{10}$ 6 6	6 6 6 7 6 6 6 4 5 4 4	4 5 3 4 4 4 4 4 3 3	3 3 3 3 3 3 3 2 2 2	2
188	6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 6 6	6 6 6 6 5 6 4 4 5 4	4 4 4 4 4 4 4 3 3 3	3 3 3 3 3 3 3 3 2 2	2
189	8 6 6 6 7 6 6 7 7	6 6 6 7 6 6 6 6 6 6	6 6 6 7 5 6 4 6 4 5	4 4 3 4 4 4 4 4 3 3	3 3 3 3 3 3 3 3 2 2	2
190	6 6 6 6 6 7 6 6 6	6 6 6 6 7 6 6 6 6 6	6 6 6 6 5 6 4 6 5 4	4 4 4 4 4 4 4 3 4 3	3 3 3 3 3 3 3 3 2 2	2
191	* 6 6 6 6 6 7 6 7	6 7 6 6 6 7 6 6 6 7	6 6 6 6 6 6 4 6 4 4	4 5 4 3 3 4 4 4 3 3	3 3 3 3 3 3 3 3 2 2	2
192	7 6 6 6 6 6 6 7 7	6 6 6 6 6 6 7 6 6 6	6 6 6 7 7 6 4 6 4 4	4 4 4 4 4 4 4 3 4 3	3 3 3 3 3 3 3 3 3 2	2
193	* 6 6 6 6 6 6 7 7	6 6 6 6 6 6 6 7 6 6	6 6 6 7 6 6 4 6 4 4	4 4 4 4 4 4 4 4 3 3	3 3 3 3 3 3 3 3 3 2	2
194	6 6 6 6 6 6 6 6 6	7 6 6 6 6 6 6 7 6 6	6 6 6 6 5 6 5 6 4 4	4 4 4 4 4 4 3 3 4 3	3 3 3 3 3 3 3 3 3 2	2
195	7 6 6 6 6 6 6 7 7	6 7 6 6 6 6 6 6 6 7	6 6 6 7 6 6 4 6 4 4	4 4 4 4 3 4 4 4 3 4	3 3 3 3 3 3 3 3 3 2	2
196	6 6 6 6 6 6 6 6 6	6 6 7 6 6 6 6 6 6 6	7 6 6 6 5 6 4 6 5 4	4 4 4 4 4 4 4 4 3 4	3 3 3 3 3 3 3 3 3 3	2
197	* 6 6 6 6 6 6 7 7	6 6 6 7 6 6 6 6 6 6	6 7 6 7 6 6 4 6 6 5	4 4 4 4 4 4 4 4 3 3	3 3 3 3 3 3 3 3 3 3	2
198	6 6 6 6 6 9 6 6 6	6 6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 4 6 5 4	4 4 4 4 3 4 4 3 4 3	3 3 3 3 3 3 3 3 3 3	2
199	* 6 6 6 6 6 9 7 7	6 6 6 6 6 7 6 6 6 6	6 6 6 7 6 6 4 6 4 4	4 4 4 4 3 4 4 4 3 4	3 3 3 3 3 3 3 3 3 3	2
200	7 6 6 6 6 6 6 7 7	6 7 6 7 6 6 7 6 6 6	6 6 6 7 6 7 5 6 5 4	4 4 4 4 3 4 4 4 4 4	4 3 3 3 3 3 3 3 3 3	3

$h \to$	0										1										2										3										4										5
$n \downarrow$	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
201	8	6	6	6	6	6	6	7	8	6	7	6	7	6	6	6	8	6	6	9	6	6	7	6	7	5	6	5	4	4	4	4	4	3	4	4	4	3	4	3	3	3	3	3	3	3	3	3	3	3
202	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	5	6	5	4	4	4	4	4	4	4	4	3	3	4	3	3	3	3	3	3	3	3	3	3	3
203	7	6	7	6	6	6	6	7	7	6	7	6	6	6	6	6	6	7	6	6	6	6	7	6	7	4	6	5	6	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3	3	3	3	3	3	3
204	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	5	6	5	6	4	4	4	4	3	4	4	4	3	4	3	3	3	3	3	3	3	3	3	3	3
205	8	6	6	6	7	6	6	7	8	6	6	6	8	6	6	6	6	8	6	6	7	6	6	6	7	5	6	5	6	5	4	4	4	4	4	4	4	3	3	4	4	3	3	3	3	3	3	3	3	3
206	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	5	6	5	6	5	5	4	4	3	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3
207	8	6	6	6	6	7	6	8	6	6	6	6	6	8	6	6	6	6	6	6	6	8	6	6	4	6	5	6	4	5	5	5	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3
208	14	6	6	6	6	6	7	7	6	6	6	12	6	6	12	6	6	6	6	6	6	7	7	6	6	5	6	4	4	4	5	4	4	4	3	3	4	4	3	3	3	3	3	3	3	3	3	3	3	3
209	11	7	6	6	6	6	7	7	6	10	6	11	6	6	11	11	6	10	6	6	6	6	7	6	6	5	6	4	4	4	5	5	4	4	4	3	4	4	4	3	3	3	3	3	3	3	3	3	3	3
210	10	11	7	6	6	6	6	6	7	6	6	6	6	6	6	6	10	10	6	6	6	6	6	6	5	6	5	6	5	6	4	4	4	4	4	5	4	4	3	3	4	4	4	3	3	3	3	3	3	3
211	*	6	11	7	6	6	6	7	7	6	7	6	9	6	6	9	9	6	9	6	6	6	6	7	4	6	5	6	6	6	4	4	4	4	4	4	4	4	3	3	4	4	3	3	3	3	3	3	3	3
212	6	6	6	11	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	8	6	6	6	6	5	6	5	6	6	4	4	4	4	4	4	4	4	3	4	4	3	3	3	3	3	3	3	3	3	3
213	7	6	6	6	11	7	6	7	7	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	7	4	6	5	6	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3
214	6	6	6	6	6	11	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	5	6	4	4	4	4	4	4	4	3	4	4	4	3	3	3	3	3	3	3	3	3	3
215	7	6	6	6	6	11	7	7	6	6	6	6	6	7	6	6	6	6	6	6	6	7	7	6	6	5	6	4	4	4	4	4	4	4	4	3	4	4	4	4	3	3	3	3	3	3	3	3	3	3
216	7	6	6	6	6	6	11	7	6	6	6	7	6	6	7	7	6	6	6	6	6	6	7	7	6	5	6	4	4	4	4	4	4	4	4	3	3	4	4	4	3	3	3	3	3	3	3	3	3	3
217	8	6	6	6	6	6	7	11	6	6	6	8	6	6	8	8	9	6	6	6	6	6	7	7	6	7	5	6	4	6	4	4	4	4	5	4	3	3	4	4	4	3	3	3	3	3	3	3	3	3
218	6	7	6	6	6	6	6	6	11	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	5	6	4	6	5	4	4	4	4	4	4	3	3	4	4	3	3	3	3	3	3	3	3	3	3
219	10	6	7	6	6	6	6	7	7	6	11	6	10	6	6	10	10	6	7	6	6	6	6	7	6	7	5	6	4	6	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3
220	6	6	6	7	6	6	6	6	6	6	6	11	6	6	6	6	6	6	6	7	6	6	6	6	6	6	5	6	4	6	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3
221	12	6	6	6	7	6	6	7	7	6	6	6	12	6	6	6	12	6	6	6	7	9	6	6	6	7	5	6	4	6	4	4	4	4	4	4	3	4	4	3	3	3	3	3	3	3	3	3	3	3
222	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	5	6	5	6	4	4	4	4	5	4	4	3	4	3	4	4	3	3	3	3	3	3	3
223	*	6	6	6	6	6	7	7	7	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	7	6	6	5	6	4	6	4	4	4	4	4	5	4	4	4	4	4	4	3	3	3	3	3	3	3
224	13	6	6	6	6	6	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	7	6	7	6	6	6	4	6	6	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3
225	8	6	6	6	6	6	7	9	6	8	6	8	6	6	6	7	6	8	6	6	6	6	6	8	6	7	7	6	5	6	6	5	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3
226	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	5	6	5	6	6	4	5	4	4	4	4	4	4	3	4	3	4	4	3	3	3	3	3	3	3
227	*	6	6	6	6	6	7	7	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	5	6	4	6	6	4	4	5	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3
228	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	5	6	4	6	6	4	4	4	5	4	4	4	4	3	4	3	3	3	3	3	3	3	3	3	3
229	*	6	6	6	6	6	7	7	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	7	5	6	4	6	6	4	4	4	4	5	5	4	4	3	3	4	4	4	3	3	3	3	3	3
230	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	5	6	6	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3
231	7	6	6	6	6	6	7	7	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	7	6	6	6	4	6	6	5	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3
232	7	6	6	6	6	6	7	7	6	6	6	6	6	7	6	6	6	6	6	10	6	6	7	6	6	7	6	7	5	6	6	6	4	4	4	4	4	4	4	3	4	4	3	4	3	3	3	3	3	3
233	*	6	6	6	6	6	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	7	6	7	5	6	6	5	4	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3
234	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	5	6	6	4	5	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3
235	7	6	7	6	6	6	6	7	7	6	7	6	6	6	7	6	6	6	7	6	6	6	6	6	6	7	6	7	5	6	6	5	4	5	4	4	4	4	4	4	3	4	3	4	3	3	3	3	3	3
236	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	5	6	6	5	4	4	5	4	4	4	4	4	4	3	4	3	3	3	3	3	3
237	7	6	6	6	7	6	6	7	7	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	5	6	6	5	5	4	4	5	4	4	4	4	4	4	3	3	3	3	3	3	3
238	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	5	6	6	5	4	5	4	5	4	4	4	4	4	4	4	3	3	3	3	3	3
239	*	6	6	6	6	6	7	7	7	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	7	6	6	4	6	6	5	4	4	5	4	4	5	4	4	4	4	4	4	4	4	3	3	3	3	3
240	7	6	6	6	6	6	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	7	6	7	6	6	5	6	6	5	4	4	4	5	4	5	4	4	4	4	4	3	4	3	3	3	3
241	*	6	6	6	6	6	7	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	7	6	7	7	6	6	5	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	3	3	3
242	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	5	6	6	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3
243	*	6	6	6	6	6	7	8	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	8	6	7	4	6	6	5	4	5	4	4	4	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3
244	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	5	6	6	5	4	4	5	4	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3
245	7	6	6	6	6	6	7	7	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	4	6	6	5	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	3
246	6	6	6	6	6	6	6	6	6	6	6	6	6	7	9	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	5	4	6	5	4	4	4	4	4	3	4	4	3	4	4	3	4	4	3
247	12	6	6	6	6	6	7	7	6	6	6	12	6	7	6	6	6	12	6	6	6	7	6	6	6	6	6	7	6	6	6	5	4	4	5	5	4	5	4	4	4	4	4	4	3	4	4	4	4	3
248	7	6	6	6	6	6	7	7	6	6	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	7	6	7	6	5	4	4	4	4	4	4	4	4	4	3	4	4	4	3	4	3	4	3
249	7	6	6	6	6	6	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	7	6	7	6	5	4	4	4	4	4	4	4	5	4	4	4	3	4	4	3	4	4	3
250	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	7	6	5	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4

$h\to$	0	1	2	3	4	5
$n\downarrow$	1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0
251	* 6 7 6 6 6 6 7 7	6 7 6 6 6 6 6 6 6 7	6 6 6 6 6 6 6 7 6 7	6 7 6 5 5 5 4 4 4 4	4 5 4 4 4 3 3 4 4 4	3
252	6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 6 6	7 6 6 6 6 6 6 6 7 6	6 6 6 5 4 6 6 4 4 4	4 4 5 4 4 4 4 3 4 4	3
253	$_{12}$6 6 6 7 6 6 7 7	6 $_{10}$6 $_{12}$6 6 $_{11}$6 6 6	6 7 6 $_{10}$6 6 6 6 6 7	6 7 6 5 4 5 6 5 4 4	4 4 5 4 4 4 4 3 4 4	4
254	9 6 6 6 6 7 6 6 6	6 9 6 9 7 6 9 6 6 6	6 6 7 7 7 6 6 6 6 6	6 6 6 5 4 5 6 5 4 4	4 4 4 4 4 4 4 3 3 4	3
255	7 7 6 6 6 6 7 7 7	6 7 6 6 6 7 6 6 6 6	6 6 6 7 7 7 6 6 6 7	6 6 6 5 4 4 5 4 5 4	4 4 4 4 4 4 3 4 4 4	4
256	* 7 7 6 6 6 6 7 7	6 7 6 6 6 6 $_{15}$6 6 6	6 6 6 7 7 7 7 6 6 7	6 7 7 5 4 5 5 4 4 5	4 4 4 4 4 4 4 3 4 4	3
257	* 7 7 7 6 6 6 7 7	6 7 6 $_{11}$6 6 $_{14}$$_{14}$6 6	6 6 6 6 6 7 6 6 6 7	6 7 7 5 4 5 5 4 4 4	5 4 4 4 4 4 4 4 4 3	3
258	6 $_{14}$7 7 7 6 6 6 6	7 6 6 6 6 6 6 6 $_{13}$6	6 6 6 6 6 7 6 6 6 6	6 6 6 5 5 5 5 5 4 4	4 5 4 4 4 4 4 4 4 4	4
259	$_{12}$5 $_{14}$7 7 7 6 7 7	6 7 6 6 6 6 $_{12}$$_{12}$6 $_{12}$6	6 6 6 6 6 6 7 6 7 7	6 7 7 5 5 5 6 6 4 4	4 4 5 5 4 4 3 3 4 4	3
260	6 5 5 $_{14}$7 7 7 6 6	6 6 7 6 6 6 6 6 6 6	$_{11}$6 6 6 6 6 6 6 7 6	6 6 6 5 4 5 6 6 4 4	4 4 4 5 4 4 4 4 4 4	4
261	8 6 5 5 $_{14}$7 7 7 8	6 7 6 7 6 6 6 6 6 6	6 $_{10}$6 7 7 6 6 6 6 8	6 7 7 5 4 5 6 6 4 4	4 4 4 4 4 4 4 4 4 4	4
262	8 6 6 5 6 $_{14}$7 7 7	6 7 6 6 7 6 6 6 6 6	6 6 9 7 7 7 6 6 6 8	6 6 6 5 4 5 6 6 4 4	5 4 4 4 4 4 4 4 4 3	3
263	* 7 7 7 7 6 $_{14}$7 7	7 7 6 6 6 7 8 8 6 8	6 6 6 8 7 7 7 6 6 6	6 7 6 5 4 5 6 6 5 4	4 4 4 4 4 4 4 4 4 4	4
264	7 7 7 7 7 7 6 $_{14}$7	7 7 6 6 6 6 7 7 6 6	6 6 6 6 7 7 7 6 6 6	6 7 7 5 4 5 6 6 5 5	4 4 4 4 4 4 4 4 4 4	4
265	8 7 7 7 7 7 7 7 $_{14}$	7 7 6 6 6 6 8 8 6 6	6 6 6 6 7 7 6 6 6 6	6 7 7 7 4 5 6 6 4 4	5 4 4 5 4 4 4 4 4 4	4
266	7 7 6 7 7 7 7 7 6 $_{14}$	6 6 6 6 6 6 6 7 6 6	6 6 7 6 6 6 7 6 6 6	6 6 6 5 5 5 6 6 4 4	4 5 4 4 4 4 4 4 4 4	4
267	$_{10}$6 7 6 7 7 7 7 7	6 $_{14}$6 6 6 6 $_{10}$$_{10}$6 7	6 6 7 6 7 7 6 7 6 6	6 7 7 5 4 5 6 6 6 4	4 4 5 4 4 4 4 4 4 4	4
268	7 6 6 7 6 7 7 7 7	7 6 $_{14}$6 6 6 6 6 6 6	7 6 7 6 6 6 6 6 7 6	6 6 6 5 4 5 6 6 4 4	4 4 4 5 4 4 4 4 4 4	4
269	* 6 6 6 7 6 7 7 7	7 7 6 $_{14}$6 6 $_{12}$$_{12}$6 6	6 7 7 7 7 7 6 6 6 7	6 7 7 5 4 5 6 6 5 4	4 4 4 4 5 4 4 4 4 4	4
270	7 6 6 6 6 7 6 7 7	7 7 6 6 $_{14}$6 6 6 6 6	6 6 7 7 7 7 6 6 6 6	7 6 6 5 5 5 6 6 5 5	4 4 4 4 4 5 4 4 3 4	4
271	* 6 6 6 6 6 7 7 7	7 7 6 6 6 $_{14}$6 6 6 6	6 6 6 7 7 7 6 6 6 6	6 7 7 5 4 5 6 6 5 5	5 4 4 4 4 4 4 4 4 4	4
272	$_{15}$6 6 6 6 6 6 7 7	7 7 6 6 6 6 $_{15}$$_{15}$6 6	6 6 6 6 7 7 6 6 6 6	6 7 7 5 4 5 6 6 4 4	5 4 4 4 4 4 4 4 4 4	4
273	$_{16}$6 6 6 6 6 6 7 7	6 7 6 6 6 6 $_{15}$$_{15}$6 6	6 6 6 6 7 7 6 6 6 6	6 7 7 5 7 5 6 6 4 5	4 5 5 4 4 4 3 4 4 4	4
274	6 $_{15}$6 6 6 6 6 6 6	7 6 6 6 6 6 6 6 $_{14}$6	6 6 6 6 6 6 7 6 6 6	6 6 6 5 5 5 6 6 4 5	5 4 4 4 4 4 4 3 4 4	4
275	$_{13}$6 $_{15}$6 6 6 6 6 7 7	6 $_{10}$6 6 6 6 $_{13}$$_{13}$6 $_{13}$	6 6 6 6 $_{10}$6 7 6 6	6 7 7 5 5 5 6 6 4 4	4 5 4 4 4 4 4 4 4 4	4
276	$_{10}$6 6 $_{15}$6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	$_{12}$6 6 6 6 $_{10}$6 6 7 6	6 6 6 5 5 5 6 6 4 4	4 4 4 4 4 4 4 4 4 4	4
277	* 6 6 6 $_{15}$6 6 7 7	6 9 6 9 6 6 6 6 6 6	6 $_{11}$6 9 6 6 6 6 6 7	6 7 7 5 4 5 6 6 4 4	4 4 4 4 4 4 4 4 4 4	4
278	6 6 6 6 6 $_{15}$6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 $_{10}$6 6 6 6 6 6 7	6 6 5 4 5 6 6 5 5	5 4 4 4 5 4 4 4 3 4	4
279	9 6 6 6 6 $_{15}$7 8	6 7 6 6 6 6 9 9 6 7	6 6 6 9 6 6 6 7 6 6	6 8 7 5 5 5 6 6 5 5	4 4 4 4 4 4 4 4 4 4	4
280	7 6 6 6 6 6 $_{15}$7	6 7 6 6 6 6 6 7 7 6 7	6 6 6 6 8 6 6 6 6 6	6 7 7 5 5 5 6 6 4 5	6 4 4 4 4 4 4 4 4 4	4
281	* 7 6 6 6 6 6 7 $_{15}$	6 6 6 6 6 6 8 8 6 6	6 6 6 6 6 7 6 6 6 6	6 6 7 6 5 5 6 6 4 5	6 5 4 4 4 4 4 4 4 4	4
282	6 6 7 6 6 6 6 6 6 $_{15}$	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 7 6 6 6	6 6 6 5 6 5 6 6 4 5	5 5 5 4 4 4 4 4 4 4	4
283	* 6 6 7 6 6 6 7 7	6 $_{15}$6 6 6 6 $_{10}$$_{10}$6 6	6 6 6 6 6 6 6 7 6 6	6 6 7 5 4 6 6 6 5 4	4 4 4 5 4 4 4 4 4 4	4
284	6 6 6 6 7 6 6 6 6	6 6 $_{15}$6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 7 6	6 6 6 5 5 5 6 6 4 5	5 4 4 5 5 4 4 4 4 4	4
285	$_{12}$6 6 6 6 7 6 7 7	6 6 6 $_{15}$6 6 $_{12}$$_{12}$6 6	6 6 6 6 6 6 6 6 6 7	6 6 7 6 4 5 6 6 5 5	5 4 4 4 4 5 4 4 4 4	4
286	6 6 6 6 6 6 7 6 6	6 6 6 6 $_{15}$6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	7 6 6 6 6 5 6 6 5 5	5 5 4 4 4 4 5 4 4 4	4
287	7 6 6 6 6 6 7 7	6 6 6 6 6 $_{15}$6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 7 7 6 6 6 6 6 4 5	6 6 5 4 4 4 4 4 4 4	4
288	$_{15}$6 6 6 6 6 6 7 8	6 6 6 6 6 6 $_{15}$$_{15}$6 6	6 6 6 6 6 6 6 6 6 6	6 6 8 6 6 6 7 6 5 4	6 6 5 5 4 4 4 4 5 4	4
289	* 6 6 6 6 6 6 7 7	6 6 6 6 6 6 6 $_{16}$6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 7 6 4 5	6 6 5 5 5 4 4 4 5 4	4
290	6 7 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 5 5 5 6 6 5 5	5 6 5 5 4 5 4 4 4 4	4
291	6 6 7 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 5 5 6 6 4 5	6 6 5 5 4 5 5 4 4 4	4
292	6 6 6 7 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 5 6 6 4 5	5 6 5 5 5 4 4 5 4 4	4
293	* 6 6 6 7 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 4 4	6 6 5 5 4 5 4 5 5 4	4
294	6 6 6 6 6 7 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 5 5	5 6 5 5 5 4 5 4 4 5	4
295	6 6 6 6 6 7 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 4 5	5 6 5 5 4 5 4 5 5 5	4
296	7 6 6 6 6 6 7 7	6 6 6 6 6 6 7 7 6 7	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 7 7 5 5	6 6 5 5 5 4 5 4 5 5	4
297	$_{10}$6 6 6 6 6 6 7 8	6 $_{10}$6 6 6 6 6 8 6 6	6 6 6 6 6 6 $_{10}$6 6	6 6 6 6 6 6 7 7 5 5	6 6 5 5 4 4 4 5 4 5	4
298	$_{10}$7 6 6 6 6 6 6 6	7 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 $_{10}$6 6	6 6 6 6 6 6 6 6 5 5	5 6 5 5 4 4 4 4 5 5	4
299	$_{12}$6 7 6 6 6 6 7 7	6 7 6 $_{12}$6 6 6 6 6 6	6 6 6 $_{12}$6 6 6 6 6 6	6 6 6 6 6 6 7 7 5 4	6 6 5 5 4 4 4 4 4 5	4
300	7 6 6 7 6 6 6 6 6	6 6 7 7 6 6 6 6 6 6	6 6 6 7 7 6 6 6 6 6	6 6 6 6 6 6 6 6 5 5	5 6 5 5 5 4 4 4 4 5	5

$h\to$	0										1										2										3										4										5
$n\downarrow$	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
301	7	7	6	6	7	6	6	7	7	6	6	6	7	6	6	6	6	6	6	6	7	6	7	7	7	6	6	6	6	9	6	6	6	6	6	7	7	5	4	5	6	6	6	4	5	4	4	4	5	5
302	7	7	7	6	6	7	6	6	6	6	6	6	7	7	6	6	6	6	6	6	6	6	7	7	7	7	6	6	6	6	6	6	6	6	6	6	5	4	5	6	5	6	5	4	5	4	4	4	5	5
303	7	7	7	7	6	6	7	6	6	6	6	6	7	6	9	6	6	6	6	6	6	7	7	7	7	7	6	6	6	6	6	6	6	6	6	6	4	4	6	6	5	6	5	4	4	5	4	5	4	4
304	$_{15}$7	7	7	7	6	6	7	8	6	8	6	7	6	6	$_{15}$	6	6	$_{15}$	6	6	7	7	7	7	7	7	6	6	6	7	6	6	6	7	7	5	4	6	6	5	6	4	5	5	4	5	5	4	4	4
305	$_{15}$7	7	7	7	7	6	7	7	6	7	6	6	6	6	$_{15}$	$_{15}$	6	$_{15}$	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	5	5	6	6	5	6	4	4	5	4	4	5	4
306	6	$_{15}$	7	7	7	7	7	6	6	7	6	6	6	6	6	6	6	6	$_{15}$	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	4	5	6	5	6	4	4	4	5	4	5	4	4
307	*	6	$_{15}$	7	7	7	7	7	7	6	7	6	7	6	6	$_{15}$	$_{15}$	6	$_{15}$	6	6	6	7	7	6	6	6	6	6	6	6	6	6	6	6	7	7	4	4	6	6	5	6	4	4	4	4	5	5	4
308	7	6	6	$_{15}$	7	7	7	7	7	6	6	7	7	6	6	6	6	6	6	$_{14}$	6	6	7	7	7	6	6	6	6	6	6	6	6	6	6	6	5	4	5	6	5	6	5	4	4	4	4	5	5	5
309	7	7	6	6	$_{15}$	7	7	7	7	7	6	6	7	6	6	6	6	6	6	6	$_{13}$	6	7	7	7	7	6	6	6	6	6	6	6	6	6	7	4	5	6	6	5	6	5	5	4	4	4	5	4	5	4
310	7	7	7	7	6	6	$_{15}$	7	7	7	7	6	7	7	6	6	6	6	6	6	6	$_{12}$	7	7	7	7	7	6	6	6	6	6	6	6	6	6	5	5	5	6	5	6	5	5	4	4	4	5	4	5	4
311	*	7	7	7	7	7	$_{15}$	7	7	7	7	7	7	6	7	$_{11}$	$_{11}$	6	$_{11}$	6	6	7	$_{11}$	7	7	7	7	7	6	6	6	6	6	6	7	7	4	5	6	6	5	6	4	4	4	4	4	5	4	5	4
312	7	7	7	7	7	7	7	$_{15}$	7	7	7	7	7	6	6	7	7	6	7	7	6	6	7	6	$_{10}$	7	7	7	7	6	6	6	6	6	6	7	7	5	5	6	6	5	6	5	4	4	4	5	5	4	5	4
313	*	7	7	7	7	7	7	7	$_{15}$	7	7	7	7	7	6	6	9	9	6	9	6	6	7	6	7	9	7	7	6	6	6	6	6	6	6	7	7	5	5	5	6	5	6	5	4	4	4	5	5	4	5	4
314	7	7	6	7	6	7	7	7	7	$_{15}$	7	7	7	6	6	6	6	7	6	6	6	7	6	6	6	8	7	7	6	6	6	6	6	6	6	6	5	5	5	6	5	6	5	4	4	4	4	5	5	5	5
315	$_{10}$6	7	6	7	6	7	7	7	$_{15}$	7	7	7	6	6	$_{10}$	$_{10}$	6	$_{10}$	6	6	6	7	7	7	7	6	7	6	6	6	6	6	6	6	6	7	7	4	4	5	6	5	6	5	6	4	4	4	5	4	5	4
316	7	6	6	7	6	7	6	7	7	7	7	$_{15}$	7	6	6	7	6	6	6	7	6	7	7	7	7	6	6	7	6	6	6	6	6	6	8	6	6	5	5	6	6	5	6	5	6	4	4	4	5	4	5	4
317	*	6	6	6	7	6	7	7	7	7	7	7	$_{15}$	6	6	$_{12}$	$_{12}$	6	$_{12}$	6	6	7	7	7	7	7	6	6	6	7	6	6	6	6	6	7	7	5	5	6	6	5	6	5	5	4	5	4	5	4	5	4
318	7	6	6	6	6	7	6	7	6	7	7	7	7	$_{15}$	6	6	6	6	6	6	6	7	7	7	7	6	6	6	6	7	6	6	6	6	6	6	5	5	6	5	6	5	5	5	4	4	5	4	5	4
319	$_{10}$6	6	6	6	6	7	7	7	6	$_{10}$	7	7	6	$_{15}$	6	6	6	6	6	6	7	7	7	7	7	6	6	6	$_{10}$	6	7	6	6	6	6	7	7	6	6	6	5	5	5	5	4	5	4	5	4
320	$_{15}$6	6	6	6	6	6	7	7	7	6	7	7	7	6	6	$_{15}$	$_{15}$	6	$_{15}$	6	6	6	6	7	7	6	6	6	6	6	6	7	6	6	6	6	7	7	6	6	6	5	5	5	4	5	5	4	5	5	4
321	$_{15}$6	6	6	6	6	6	7	7	7	6	7	6	7	6	6	$_{15}$	$_{15}$	6	$_{15}$	6	6	6	6	7	7	6	6	6	6	6	6	6	7	6	6	6	7	6	6	6	7	6	5	5	5	4	4	5	5	4	5	4
322	6	6	6	6	6	6	6	6	6	7	6	7	6	6	6	6	6	$_{15}$	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	5	5	6	5	6	5	5	4	5	4	5	4	5	4
323	$_{16}$6	6	6	6	6	6	7	7	6	7	6	7	6	6	6	$_{16}$	$_{16}$	6	$_{16}$	6	6	6	7	7	7	6	7	6	6	6	6	7	6	6	7	6	7	4	5	5	6	5	6	5	5	5	4	5	5	4	5	4
324	8	6	6	6	6	6	6	7	8	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	8	7	6	5	5	6	5	6	5	6	4	5	4	5	4	5	4
325	$_{12}$6	6	6	6	6	6	7	7	6	6	6	$_{12}$	6	6	6	6	$_{17}$	6	6	6	6	6	6	$_{12}$	6	6	7	6	6	6	6	6	6	7	7	6	6	5	6	5	6	5	5	5	4	4	5	5	5	4	5
326	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	5	5	5	5	4	5	4	5	4	5	4	4
327	7	6	$_{15}$	6	6	6	6	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	7	6	6	6	5	5	4	5	5	5	4	5	5	4
328	7	6	6	7	6	6	6	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	7	6	6	6	5	5	4	5	5	5	4	5	5	4
329	9	6	6	6	7	6	6	7	7	6	9	6	9	6	6	6	6	9	6	6	6	6	6	6	6	9	6	6	6	6	6	7	6	6	6	6	6	6	7	5	6	5	5	4	6	5	5	5	5	5
330	6	7	6	6	6	7	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	5	6	5	5	5	5	6	5	5	5	5
331	*	6	7	6	6	6	7	7	7	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	6	5	5	4	6	5	5	5	5	5
332	7	6	6	7	6	6	6	7	7	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	6	6	5	6	5	5	4	6	5	5	4
333	8	6	6	6	7	6	6	7	8	6	7	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	8	6	6	6	7	5	6	5	5	5	6	5	5	4
334	7	6	6	6	7	6	6	7	7	6	7	6	7	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	5	6	5	5	5	6	5	5	4
335	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	6	5	5	4	6	5	5	4
336	8	6	6	6	6	6	7	8	6	8	6	6	6	6	8	6	6	6	6	6	6	6	6	6	9	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	5	5	5	6	6	5	5	5	5
337	*	6	6	6	6	6	7	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	5	4	6	6	5	5	5	5
338	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	5	4	6	6	5	5	5	5
339	7	6	6	6	6	6	7	7	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	6	5	5	4	6	5	5	4
340	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	6	5	5	5	6	5	5	5
341	$_{10}$6	6	6	6	6	6	7	7	6	$_{10}$	6	7	6	6	9	6	6	6	6	6	7	6	6	6	6	6	6	6	6	$_{10}$	6	6	9	6	6	6	6	6	6	7	5	6	5	5	5	6	5	5	5
342	$_{10}$6	6	6	6	6	6	6	6	6	9	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	$_{10}$	9	6	6	6	6	6	6	6	6	5	6	5	6	5	5	6	5	5	5
343	*	9	6	6	6	6	6	7	7	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	8	6	6	6	6	6	6	6	7	6	6	5	5	5	6	6	6	5	5	5
344	7	6	9	6	6	6	6	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	5	5	4	6	6	6	5	5	5
345	7	6	6	9	6	6	6	7	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	5	5	4	6	5	6	5	5	5
346	6	7	6	6	9	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	6	4	6	6	6	5	5	5
347	*	6	7	6	6	9	6	7	7	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	5	5	6	6	6	6	5	5
348	6	6	6	7	6	6	9	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5	5	5	6	6	6	6	5	5
349	*	6	6	6	7	6	6	9	7	6	7	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	7	7	6	6	6	6	6	6	6	6	6	6	5	5	4	6	6	6	6	5	5
350	8	6	6	6	6	7	6	6	9	6	8	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	8	8	6	6	6	6	6	6	6	6	6	5	5	5	6	6	6	6	6	6

$h\to$	0									1									2									3									4									5
$n\downarrow$	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
351	$_{12}$6	6	6	6	6	7	7	7	9	6	6	$_{12}$6	7	6	6	6	6		6	6	6	7	6	6	6	$_{12}$6	6		6	7	6	6	6	6	6	6	6		6	7	6	6	5	5	5	6	6	6		6
352	$_{18}$6	6	6	6	6	7	7	7	6	$_{10}$6	6	6	6	7	6	6	6		6	6	6	7	6	6	6	6	6		6	$_{10}$6	6	6	6	6	6	8		6	7	6	7	5	5	5	6	6	6		5
353	*	6	6	6	6	6	7	7	6	7	6	6	6	6	6	7	6		6	6	6	6	6	7	6	6	6		6	6	6	7	6	6	6	6	6		6	7	6	7	5	5	5	6	6	6		5
354	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7		6	6	6	6	6	6	7	6	6		6	6	6	6	7	6	6	6	6		6	6	6	6	5	5	5	6	6	6		5
355	9	6	6	6	6	6	7	7	6	9	6	9	6	6	6	6	6		9	6	6	6	6	6	6	7	6		9	6	6	6	6	7	6	6	6		6	7	6	7	5	5	5	6	6	6		5
356	7	6	6	6	6	6	7	7	6	6	7	6	6	6	6	6	6		6	7	6	6	6	6	6	6	7		6	6	6	6	6	6	7	6	6		6	7	6	6	5	5	5	6	6	6		5
357	9	6	6	6	6	6	7	7	6	9	6	7	6	6	9	6	6		6	7	6	6	6	6	6	6	7		6	6	6	6	6	6	6	7	6		6	7	6	7	5	5	5	6	6	6		5
358	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6		6	6	7	6	6	6	6	6	6		7	6	6	6	6	6	6	7	6		6	6	6	6	5	5	5	6	6	6		5
359	*	6	6	6	6	6	7	7	6	6	6	6	6	7	6	6	6		6	6	7	6	6	6	6	6	6		6	7	6	6	6	6	6	7		6	7	6	7	5	5	5	6	6	6		5
360	8	6	6	6	6	6	7	8	6	6	6	8	6	6	8	6	6		6	6	6	7	6	6	8	6	6		6	6	7	6	6	6	6	6	6		7	7	6	7	5	6	5	6	6	6		5
361	*	6	6	6	6	6	7	7	6	6	6	6	6	6	6	7	6	$_{18}$	6	6	6	6	6	7	6	6	6	$_{11}$	6	6	7	6	6	6	6	6	6		7	7	6	7	5	5	5	6	6	6		5
362	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6		6	6	6	6	5	5	5	6	6	6		5
363	7	6	7	6	6	6	6	7	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6		6	6	6	6	7	5	5	5	6	6	6	5
364	7	6	6	7	6	6	6	7	7	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	$_{10}$6	6	7	6	6	6		6	7	6	6	5	5	5	6	6	6		5
365	$_{10}$6	6	6	7	6	6	7	7	6	6	6	$_{10}$6	6	6	$_{10}$6	6	6		6	7	6	6	6	6	6	6	7		6	6	6	6	6	6	6	7		6	7	6	7	5	5	5	6	6	6		5
366	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6		6	6	7	6	6	6	6	6	6		7	6	6	6	6	6	6	7	6		6	6	6	6	5	5	5	6	6	6		5
367	*	6	6	6	6	6	7	7	6	6	6	6	6	6	6	6	6		6	6	6	7	6	6	6	6	6		6	7	6	6	6	6	6	6	7		6	6	6	7	6	5	5	6	6	6		5
368	$_{15}$6	6	6	6	6	6	7	7	6	$_{10}$6	$_{10}$6	6	6	$_{15}$6	6	6			6	6	6	$_{15}$7	6	6	6	6	6		6	9	6	6	6	6	6	6		7	7	6	7	6	6	6	6	6	5		
369	$_{15}$6	6	6	6	6	6	7	8	6	6	6	6	6	6	$_{15}$	$_{15}$	6	6		6	6	6	$_{15}$7	7	6	6	6	6		6	6	7	6	6	6	6	6		6	8	6	7	5	6	6	6	6	5		
370	7	$_{15}$6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	$_{15}$	6		6	6	6	7	7	7	7	6	6		6	6	6	7	6	6	6	6		6	6	6	6	5	5	5	6	6	6		5
371	$_{15}$7	$_{15}$6	6	6	6	6	7	7	6	6	6	6	6	6	$_{15}$	$_{15}$	6	$_{15}$		6	6	6	$_{15}$7	7	7	7	6	6		6	6	6	6	7	6	6	6		6	6	7	5	5	5	6	6	6	5		
372	7	7	7	$_{15}$6	6	6	7	7	6	6	6	6	6	6	7	6	6	$_{15}$		6	6	7	7	7	7	7	7	6		6	6	6	6	6	7	6	6		6	6	7	6	5	5	6	6	6	5		
373	*	7	7	7	$_{15}$6	6	7	7	6	6	6	6	6	6	7	6	6	$_{15}$		6	$_{15}$6	7	7	7	7	7	7	7		6	6	6	6	6	7	6	6		6	6	7	6	5	6	6	6	6	5		
374	7	7	7	7	7	$_{15}$6	6	6	6	6	6	6	6	6	7	6	6	$_{15}$		6	6	$_{15}$7	7	7	7	7	7	7		7	6	6	6	6	6	7	6		6	6	6	6	6	6	6	6	6	5		
375	$_{15}$7	7	7	7	7	$_{15}$7	7	6	6	6	6	6	6	$_{15}$	$_{15}$	6	6		6	6	6	$_{15}$7	7	7	7	7	7	7		7	7	6	6	6	6	6	6		7	6	6	6	7	6	6	6	6	6		5
376	7	7	7	7	7	7	7	$_{15}$7	6	6	6	6	6	6	7	7	6	6		6	6	7	7	$_{14}$7	7	7	7	7		7	7	7	6	6	6	6	6		7	6	6	6	7	6	6	7	6	6		5
377	$_{13}$7	7	7	7	7	7	7	$_{15}$6	6	6	$_{12}$6	6	$_{13}$	$_{13}$	6	6		6	6	7	$_{13}$7	$_{13}$6	6	6	$_{12}$	6	6	7	6	6	6	6	6	6	6	6		6	7	6	6	6	7	6	6	7	6	6		5
378	7	7	7	7	7	7	7	7	$_{15}$6	6	6	6	6	6	7	6	6	6		6	6	6	7	7	$_{12}$6	6	6		6	6	6	6	7	6	6	6	6		6	7	6	6	6	6	6	6	6	6		5
379	*	7	7	7	7	7	7	7	7	$_{15}$6	6	6	6	$_{11}$	$_{11}$	6	6		6	6	7	$_{11}$7	7	7	$_{11}$6	6		6	6	6	6	6	7	6	6	6	6		6	6	7	6	6	7	6	6	6	5		
380	7	7	7	7	7	7	7	7	7	7	$_{15}$6	6	6	7	6	6	6		6	6	6	7	7	7	7	$_{10}$6		6	6	6	6	6	7	6	6	6	6		6	6	7	6	6	6	6	6	6	5		
381	$_{12}$7	7	7	7	7	7	7	$_{11}$7	7	7	$_{15}$6	6	$_{12}$	$_{12}$	6	6		6	9	7	$_{12}$7	7	7	7	7	9		6	6	6	6	6	6	7	6	6		6	6	7	6	6	7	6	6	5		
382	7	7	7	7	7	7	7	7	7	7	7	7	$_{15}$6	7	6	6	6		6	6	6	7	7	7	7	7	7	7	8	6	6	6	6	6	7	6		6	6	6	6	6	6	6	6	6	6		5
383	*	7	7	7	7	7	7	7	7	7	7	7	7	$_{15}$7	7	6	6		6	6	7	7	7	7	7	7	7	7	7	6	6	6	6	6	6	7		6	6	6	6	6	6	6	6	6	6		5
384	$_{15}$7	7	7	7	7	7	7	7	7	7	7	7	7	$_{15}$	$_{15}$	6	6		6	6	7	$_{15}$7	7	7	7	7	7	7		7	7	6	6	6	6	6	6		7	6	6	6	7	6	6	7	7	6		5
385	$_{15}$6	7	7	7	7	7	7	7	7	7	7	7	7	$_{15}$	$_{15}$	6	6		6	6	7	$_{15}$7	7	6	7	7	7	7		7	6	$_{11}$6	6	6	6	6	6		6	7	6	7	6	6	7	7	6	5		
386	7	7	6	6	7	6	7	7	7	7	7	7	7	7	7	6	$_{15}$	6		6	6	7	7	7	7	6	7	7		7	7	6	6	6	6	6	6		6	6	7	6	6	6	6	6	6	6		6
387	$_{15}$6	7	6	6	7	6	7	8	7	7	7	7	7	$_{15}$	$_{15}$	6	$_{15}$		6	6	7	$_{15}$7	7	6	7	6	7	7		7	7	6	6	6	6	6	6		6	6	8	6	6	7	6	6	6	5		
388	7	6	6	7	6	6	7	7	7	7	7	7	7	7	6	6	$_{15}$		6	6	7	7	7	6	6	7	6	7		7	7	6	6	6	6	6	6		6	6	6	6	6	6	6	6	6	5		
389	*	6	6	6	7	6	6	7	7	7	7	7	7	7	6	6	6		6	$_{15}$7	7	7	7	6	6	6	7		6	6	6	6	6	6	6	7	6		6	6	6	6	6	6	7	6	6	5		
390	7	6	6	6	6	7	6	6	7	6	7	7	7	7	7	6	6	6		6	6	$_{15}$7	7	7	6	6	6	6		7	6	6	6	6	6	6	6		6	6	6	6	6	6	6	6	6	5		
391	$_{16}$6	6	6	6	6	7	7	7	7	6	7	7	7	7	7	$_{16}$	6	6		6	6	7	$_{16}$7	7	6	7	6	6		6	7	6	6	6	6	6	6		6	6	6	6	6	6	6	7	6	6		6
392	7	6	6	6	6	7	6	7	7	6	7	6	7	7	7	7	7	6	6	6	6	6	7	7	7	6	6	6	6	6	6	7	6	6	6	6	6		6	6	6	6	6	6	6	7	7	7		6
393	8	7	6	6	6	7	6	7	8	6	6	7	6	7	7	7	8	6	6	6	9	6	7	7	7	7	6	6	6	6	6	6	6	6	6	6	6		6	6	6	6	6	6	7	6	7	7		6
394	7	7	7	6	6	6	6	6	6	7	6	6	7	6	7	7	7	7	6	6	6	9	7	7	7	7	6	6	6	6	6	6	6	6	6	6	6		6	6	6	6	6	6	6	6	6	6		6
395	7	7	7	7	6	7	6	7	7	6	7	6	6	7	6	7	7	6	7	6	6	6	7	7	7	7	7	6	6	6	6	6	6	6	6	6	6		6	6	6	6	6	6	6	6	7	7		5
396	8	7	7	7	7	6	6	6	6	8	7	6	6	7	6	7	6	6	6	7	6	6	7	7	7	7	7	7	6	6	6	6	6	6	6	8	6		6	6	6	6	6	6	6	6	6	6		5
397	*	7	7	7	7	7	6	7	7	6	8	6	7	6	6	7	7	6	6	6	7	6	7	7	7	7	7	7	7	6	6	6	6	6	6	8	8		6	6	6	6	6	6	7	7	7	5		
398	7	8	7	7	7	7	7	6	6	6	6	6	6	7	6	6	7	6	6	6	6	7	7	7	7	7	7	7	7	7	6	6	6	6	6	6	8		6	6	6	6	6	6	6	6	6	5		
399	7	7	8	7	7	7	7	7	7	6	6	7	6	6	7	6	7	6	6	6	6	6	7	7	7	7	7	7	7	7	7	6	6	6	6	6	7		6	6	6	6	6	6	7	6	6	6		6
400	$_{15}$7	7	8	7	7	7	7	7	6	$_{10}$6	$_{10}$6	6	6	$_{15}$7	6	6			6	6	6	7	7	$_{15}$7	7	7	7	7		7	7	9	6	6	6	6	6		6	6	6	6	6	6	6	7	7	7		6

$h\to$	0										1										2										3										4										5
$n\downarrow$	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
401	*	7	7	7	8	7	7	7	7	7	7	6	6	6	6	6_{15}	15_6	6	6	6	6	6	7	7_{15}	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	7	6
402	7	7_{15}	7	7	7	8	7	7	7	7	7	6	7	6	6	6	7	7_{15}	6	6	6	6	7	7	7	7	7	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5
403	15_7	7_{15}	7	7	7	7_{15}	7	7	7	7	7	7_{12}	6	6	15_{15}	6_{15}	6	6	6	6	7	7_{15}	7	7	7	6	6_{12}	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	7	6
404	11_7	7	7_{15}	7	7	7	8	7	7	7	7	7_{11}	6	6	6	7	6	6	15_6	6	6	7	7	7	7	7	7	7	6_{1111}	6	6	6	7	7	6	6	6	6	6	6	6	7	6	6	5					
405	8	8_{11}	7	7	7_{15}	7	7	7	8	7	8	7	7	7	6	6	7	7	6	6_{15}	6	7	7	7	7	7	7	7	7	7	6	6_{10}	6	6	8	8	6	6	6	6	6	6	6	7	6	7	6					
406	7	7	7_{11}	7	7	7_{15}	7	7	7	8	7	7	7	7	7	6	7	6	6	6	6_{15}	6	7	7	7	7	7	7	7	7	6	6	9	6	6	6	7	6	6	6	6	6	6	6	6	6	6	5				
407	15_7	7	7	7_{11}	7	7	7_{15}	7	7	7	7_{10}	7	7	7	7	15_{15}	6	6	6	6	7	7_{15}	7	7_{15}	7	7	7	7	7	7	6	6	8	6	10_6	7	6	6	6	6	6	6	7	7	7	6					
408	8	7	7	7	7_{11}	7	7	7_{15}	7	7	8	7	7	7	7	7	7	6	6	6	6	7	7	7_{15}	7	7	7	7	7	7	7	6	6	6	7	6	6	6	7	6	6	6	6	6	6	7	7	7	6		
409	*	7	7	7	7	7_{11}	7	7	7_{15}	7	7	7	7	7	7	7_{15}	15_6	15_6	6	6	6	7	7	7_{15}	7	6	7	7	7	7	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	7	7	6	
410	7	7	7	7	6	7	7_{11}	7	7	7_{15}	7	7	7	7	7	7	7	7	6	6	6	7	7	7	7	7_{14}	7	6	7	7	7	7	6	7	6	6	6	6	6	6	6	6	6	6	5						
411	13_6	7	7	7	7	7	7	11_7	7	7	7_{15}	7	7	7	7	13_{13}	6	7	6	6	7	7	7	13_6	13_7	6	7	7	7	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	7	7	7	6		
412	8	6	6	7	7	7	6	7	11_7	7	7	7_{15}	8	7	7	7	7	6	6	7	6	7	7	7	7	6	6	12_7	6	8	8	6	6	6	7	6	6	6	6	6	7	6	6	7	6	6	6				
413	12_6	6	6	6	7	7	7	7	11_7	7	7	7_{15}	7	7_{12}	12_6	6	6	6	7	7	7	7	12_6	6	6	11_7	7	6	6	6	6	6	6	7	6	6	6	6	6	7	6	7	7	7	5					
414	10_6	6	6	6	6	7	7	7	6	7	11_7	7	10_{15}	7	7	7	6	6	6	6	7	6	6	6	6	6	6	10_{10}	10_6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6					
415	9	6	6	6	6	7	7	7	7	6	7	11_7	7	7	15_9	9	9	6	6	6	7	7	7	9	6	6	6	6	9	7	6	6	6	6	6	7	6	6	6	6	6	6	7	7	7	6					
416	18_6	6	6	6	6	7	6	7	7	7	6	7	12_7	7	7	15_{15}	6	6	6	6	7	7	7	15_6	6	6	6	6	6_{12}	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	7	7	6			
417	15_6	6	6	6	6	7	6	7	7	7	7	6	7	7	7	15_{15}	6	6	6	6	7	7	7	15_6	6	6	6	6	7	6	6	7	6	6	6	6	6	6	7	6	6	6	6	7	6	7	6				
418	7	6	6	6	6	6	6	6	6	7	7	7	6	7	7	7	7	15_6	6	6	6	6	7	7	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	5		
419	*	6	6	6	6	7	6	7	7	6	7	7	7	6	7	15_{15}	6_{15}	6	6	7	6	7	15_6	7	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	7	6	6	6	7	6	6	
420	7	6	6	6	6	7	6	7	7	6	6	7	7	7	6	7	7	6	15_6	6	6	7	7	7	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	7	6	6	6	6	7	6	6	7	7	6	
421	*	6	6	6	6	7	6	7	7	6	6	6	7	7	7	7	11_6	6	6_{15}	6	6	7	7	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	9	6	6	7	6	6	7	7	6	
422	7	6	6	6	6	6	6	6	6	6	6	6	6	7	7	7	7	6	6	6	6_{15}	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6	7	6	6	6	6	6	7	6	6	
423	15_6	6	6	6	6	7	6	7	8	6	6	6	6	6	7	15_{15}	6	6	6	6	6	15_7	15_6	6	6	6	6	7	6	6	6	6	6	7	6	7	6	6	6	6	7	6	6	6	8	6	7	6			
424	7	6	6	6	6	7	6	7	7	6	6	6	6	6	6	7	7	6	6	6	6	6	15_7	6	7	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	7	7	7	6				
425	16_7	6	6	6	6	7	6	7	8	6	6	6	6	6	6	6	16_6	6	6	6	6	6	6	16_6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	7	7	6					
426	6	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	6			
427	7	6	7	7	6	7	6	7	7	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	7	7	6		
428	7	6	6	7	7	7	6	7	7	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	7	6	6	6	6	6	7	6		
429	10_6	6	6	7	7	6	7	7	7	6	6	6	10_6	6	6	6	10_6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	7	6	6	7	6	6	6	7	6		
430	6	6	6	6	6	7	7	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	7	6	6	6	6	6	7	6	6	
431	*	6	6	6	6	7	7	7	7	6	6	6	6	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	6	
432	15_6	6	6	6	6	7	6	7	8	6	7	6	6	6	6	15_6	6	6	6	6	6	6	6	6	6	15_6	6	6	6	7	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	8	7	6	
433	*	6	6	6	6	7	6	7	7	6	6	6	6	6	6	15_{15}	6	6	6	6	6	6	6	6	6	15_6	6	6	6	7	6	6_{11}	6	6	6	6	7	6	6	6	6	6	6	7	7	6			
434	6	6_{15}	6	6	6	6	6	6	7	6	6	6	6	6	6	6	15_6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6		
435	15_6	6	15_6	6	6	7	6	7	7	6	7	6	6	6	6	15_{15}	6_{15}	6	6	6	6	6	6	15_6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	7	7	6		
436	6	6	6	15_6	6	6	6	6	6	6	7	6	6	6	6	6	6	6	6	15_6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	6		
437	18_6	6	6	15_6	6	6	7	7	6	6	6	7	6	6	6	6	6	18_6	6_{15}	6_{18}	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6			
438	7	6	6	6	6	15_6	6	6	6	6	6	6	7	6	6	6	6	7	6	6	15_7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6			
439	*	7	6	6	6	7	15_7	7	7	6	6	6	6	6	7	15_{15}	6	7	6	6	6	15_7	7	6	15_6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	7	6			
440	7	7	7	6	6	7	6	15_7	7	6	7	6	6	6	6	6	7	7	6	7	6	15_7	7	7	7	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	6	6	6	7	7	6	
441	15_7	7	7	7	6	7	6	7	15_6	6	7	6	6	6	6	15_{15}	6	15_6	6	6	6	7	15_7	15_6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	6	6	9	6	6	6	8	6
442	7	7	7	7	7	6	6	6	15_6	6	6	6	6	6	6	6	7	7	6	6	6	6	7	7	15_7	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	6	6	7	6	6	6	6	6	6
443	*	7	7	7	7	7	6	7	7	6_{15}	6	6	6	6	15_{15}	15_6	6	7	6	6	6	6	7	7	7	15_7	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	6	7	6	6	6	6	6	6
444	7	7	7	7	7	7	7	6	6	6	6_{15}	6	6	6	6	6	6	7	7	6	6	7	7	7	7	14_7	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
445	13_7	7	7	7	7	7	7	7	7	6	6	6	15_6	6	6	13_{13}	6	7	6	7	6	7	7	7	7	13_7	7_{13}	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
446	7	7	7	7	7	7	7	7	7	6	6	6	6	15_6	6	6	6	7	6	6	7	7	7	7	7	7	7	7	12_7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
447	11_7	7	7	7	7	7	7	7	7	7	6	6	6	6	15_{11}	11_6	7	6	6	6	7	7	7	7	11_7	7	7	7_{11}	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
448	15_7	7	7	7	7	7	7	7	7	7	7	6	6	6	6	15_{15}	6	7	6	6	6	7	7	7	7	15_7	7	7	7	10_7	7	7	6	6	6	6	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6
449	*	7	7	7	7	7	7	7	7	7	7	7	6	6	6	15_{15}	6	7	6	6	6	7	7	7	7	15_7	7	6	6	6	9	6	6	6	6	6	6	7	7	6	6	6	6	6	6	6	6	6	6	6	6	6
450	7	7	7	7	7	7	7	7	7	7	7	7	7	6	6	6	15_7	7	6	6	6	6	7	7	7	7	7	7	7	7	6	6	6	6	8	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

$h\to$	0	1	2	3	4	5
$n\downarrow$	1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0
451	7_{15} 7 7 7 7 7 7 7 7	7_{10} 7 7 7 6_{15} 15_{15} 6_{15}	6 6 6 7 7 7 7_{15} 7 7	7 6 6 6 6 7 6 6 6 6	6_{10} 6 6 6 6 6 6 6 6	6
452	7 7 7 7 7 7 7 7 7	7 7 7 7 7 7 6 6 6 7	7_{15} 6 6 6 7 7 7 7 7 7	7 7 6 6 6 6 7 6 6 6	6 6 6 6 6 6 6 6 6 6	6
453	7 7 7 7 7 7 7 7 7	7 7 7 7 7 7 7 6 6 7	6_{15} 6 7 7 7 7 7 7 7	7 7 7 6 6 6 6 7 6 6	6 6 6 6 6 6 6 6 6 6	6
454	7 6 7 7 7 7 7 7 7	7 7 7 7 7 7 7 7 6 7	6 6 6_{15} 7 7 7 7 7 7 7	7 7 7 7 6 6 6 6 7 6	6 6 6 6 6 6 6 6 6 6	6
455	7_{15} 7 7 7 7 7 7 7 7	7 7 7 7 7 7 7_{15} 15_{15} 7 7	6 6 7 7_{15} 7 7 7 7_{15} 7 7	7 7 7 7 7 7 6 6 6 7	6 6 6 6 6 6 6 6 6 6	6
456	7 7 7 7 7 7 7 7 7	7 7 7 7 7 7 7 7 7 7	6 6 7 7 7_{15} 7 7 7 7 7	7 7 7 7 7 6 6 6 6 7	6 6 6 6 6 6 6 6 6 6	6
457	* 7 7 7 7 7 7 7 8	7 7 7 7 7 7 7_{15} 15_{15} 7 7	6 6 7 7 7 7_{15} 7 7_{15} 7 6	7 7 7 7 6 6 6 6_{11} 6	6 7 6 6 6 6 6 6 6 6	6
458	7 7 6 7 7 7 7 7 6	7 7 7 7 7 7 7 7 7 7	6 6 7 7 7 7 7_{15} 7 7 7	6 7 7 7 7 6 6 6 6 6	6 6 7 6 6 6 6 6 6 6	6
459	9_{16} 6 7 6 7 7 7 7 8	6 9 7 9 7 7 8 7_{16} 7 8	6 6 7 7 7 7 6 6_{16} 7 7	7 6 7 7 6 7 6 9 6 6	6 6 6 7 6 6 6 6 6 6	6
460	7 6 6 7 6 7 7 7 7	7 6 7 7 7 7 7 7 7 7	6 6 7 6 6 6 6 6 6_{14} 7	7 7 6 7 7 6 7 6 6 6	6 6 6 6 7 6 6 6 6 6	6
461	* 6 6 6 7 6 7 7 7	7 7 6 7_{10} 7 7 7 7_{10} 7 7	6 6 7 7 7 7 6 6 6 7	7 7 7 6 6 6 6 7 6 6	6 6 6 6 6 7 6 6 6 6	6
462	7 6 6 6 6 7 6 7 7	7 7 7 6 7 7 7 7 7 7	6 6 7 7 7 7 6 6 6 6	7 7 7 7 6 6 6 6 7 6	6 6 6 6 6 6 7 6 6 6	6
463	* 6 6 6 6 6 7 7 7	7 7 7 7 6 7 7 7 7 7	6 6 7 7 7 7 6 6 6 6	6 7 7 7 7 6 6 6 6 7	6 6 6 6 6 6 6 7 6 6	6
464	6_{15} 6 6 6 6 6 6 7 7	7 7 7 7 7 6 6_{15} 7 7 7	6 6 7 7 7 7 6 6 6 6_{15}	6 6 7 7 7 6 6 6 6 6	7 6 6 6 6 6 6 7 6 6	6
465	6_{15} 6 6 6 6 7 6 7 7	6 7 7 7 7 7 7_{15} 15_{15} 7 7	6 6 7 7 7 7 6 7 6 6_{15}	6 6 6 7 6 6 6 6 6 6	6 7 6 6 6 6 6 6 7 6	6
466	7 7_{15} 6 6 6 6 6 6 6	7 6 7 7 7 7 7 6 6_{15} 7	6 6 7 7 7 7 6 6 6 6	6 6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 6 7	6
467	* 6 6_{15} 6 6 6 6 7 7	6 7 6 7 7 7 7_{15} 15_{15} 6_{15}	6 6 7 7 7 7 6 6 6 6_{15}	6 6 6 6 6 7 6 6 6 6	6 6 6 7 6 6 6 6 6 6	6
468	8 6 6 6_{15} 6 6 6 6 6	6 6 7 8 7 7 7 7 7 7_{15}	6 7 6 6 6 6 6 6 6 6	6 6 6 6 6 6 8 6 6 6	6 6 6 6 7 6 6 6 6 6	6
469	8 6 6 6 6_{15} 6 6 7 7	6 6 6 8 6 7 7 7 7 7	6 6_{15} 7 7 7 7 6 6 6 6	6 6 6 6 6 6 8 8 6 6	6 6 6 6 6 7 6 6 6 6	6
470	7 8 6 6 6 6_{15} 6 6 6	6 6 6 6 6 7 6 7 7 7 7	6 6 6_{15} 7 7 7 6 6 6 6	6 6 6 6 6 6 6 6 8 6	6 6 6 6 6 6 7 6 6 6	6
471	6_{15} 6 8 6 6 6 6_{15} 7 7	6 6 6 6 6 7 7_{15} 15_{15} 7 7	6 6 6 6_{15} 7 7 6 6 6 6_{15}	6 6 6 6 6 6 6 6 6 8	6 6 6 6 6 6 6 7 6 6	6
472	7 6 6 8 6 6 6 6_{15} 7	6 6 6 7 6 6 7 7 7 7	6 6 6 6 6_{15} 7 6 6 6 7	6 7 6 6 6 6 7 7 6 6	8 6 6 6 6 6 6 7 6 6	6
473	6_{15} 6 6 6 8 7 6 7 7_{15}	6 6_{10} 6 7 6 6 6_{15} 15_{15} 6 7	6 6 6 6 7 7_{15} 6 6 6 6_{15}	6 6 6 6 6 6 7 7 6 6	6 7 6 6_{10} 6 6 6 6 7 6	6
474	6_{10} 7 6 6 6 8 6 6 6	6_{15} 6 6 6 6 6 6 6 7 6	6 6 6 6 6 6_{15} 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6_{10} 6 6 6 6 6 7	6
475	6_{18} 6 7 6 6 6 8 7 7	6 6_{15} 6 6 6 6 6_{15} 15_{15} 6_{18}	6 6 6 6 6 6_{18} 6 6_{15} 6 6_{15}	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
476	7 6 6 7 6 6 6 8 6	6 6 6_{15} 7 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6_{15} 6	6 6 6 6 6 6 7 7 6 6	6 6 6 6 6 6 6 6 6 6	6
477	7_{15} 6 6 6 7 6 6 7 8	6 6 6 6_{15} 6 6 6_{15} 15_{15} 6 6	6 6 6 6 6 6 6 6 6 6_{15}	6 6 6 6 6 6 8 8 6 6	6 6 6 6 6 6 6 6 6 6	6
478	6 6 6 6 6 7 6 6 6	8 6 6 6 6_{15} 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6_{14} 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
479	* 6 6 6 6 7 7 6 6	6_{15} 6 8 6 6_{15} 13_{13} 6 6_{10}	6 6 6 6 6 6 6 6_{10} 6 6_{13}	6_{13} 6 6 6 6 8 8 6 6	6 6 6 7 6 6 6 6 6 7	6
480	6_{15} 6 6 6 6 6 6 7 7	6 6 8 6 6 6 6_{15} 15_{15} 6 6	6 6 6 6 6 6 6 6 6 6_{15}	6 6 6_{12} 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
481	6_{15} 6 6 6 6 6 6 7 7	6 6 6 6_{12} 6 6 6_{15} 15_{15} 6 6	6 6 6 6 6 6 6 6 6 6_{15}	6 6 6 6_{11} 6 6 6_{12} 6 6	6 6 6 6 6 6 6 9 6 6	6
482	6 6 6 6 6 6 6 6 6	7 6 6 6 6 6 6 6 6_{15} 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6_{10} 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
483	6_{15} 6 6 6 6 6 6 7 7	6 7 6 6 6 6 6_{15} 15_{15} 6 6_{15}	6 6 6 6 6 6 6 6 6 6_{15}	6 6 6 6 6 9 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
484	8 6 6 6 6 6 6 6 6	6 6 7 6 6 6 6 8 8 6 6	6_{15} 6 6 6 6 6 6 6 6 8	6 6 6 6 6 6 8 6 6 6	6 6 6 6 6 6 6 6 6 6	6
485	7 6 6 6 6 6 6 7 7	6 6 7 7 6 6 7 7 6 6	6_{15} 6 6 6 6 6 6 6 7	6 6 6 6 6 6 6 7 6 6	6 6 6 6 6 6 6 6 6 6	6
486	6 6 6 6 6 6 6 6 6	6 6 6 6 7 6 6 6 6 6	6 6 6_{15} 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
487	* 6 6 6 6 6 6 7 7	6 6 6 6 6 7 7_{15} 15_{15} 6 6	6 6 6 6_{15} 6 6 6 6 6 6_{15}	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
488	7 6 6 6 6 6 6 7 7	6 6 6 6 6 6 7 7 6 6	6 6 6 6 6_{15} 6 6 6 6 7	6 7 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
489	6_{15} 6 6 6 6 6 6 7 8	6 6 6 6 6 6 6_{15} 15_{15} 6 6	6 6 6 6 6 6_{15} 6 6 6 6_{15}	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
490	6 7 6 6 6 6 6 6 6	7 6 6 6 6 6 6 6 7 6	6 6 6 6 6 6_{15} 6 6 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
491	* 6 7 6 6 6 6 7 7	6 7 6 6 6 6 6_{15} 15_{15} 7 7	6 6 6 6 6 6 6 6_{15} 6 6_{15}	6 6 6 6 6 6 6 6 6 6	6 6 6 7 6 6 6 6 6 6	6
492	6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 6 7	6 6 6 6 6 6 6 6 7_{15} 6	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
493	6_{16} 6 6 6 7 6 6 7 7	6 6 6 6_{10} 6 6 6 6_{16} 6 6	6 7 6 6 6 6 6 6 6 6_{16}	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
494	6 6 6 6 6 7 6 6 6	6 6 6 6 7 6 6 6 6 6	6 6 7 6 6 6 6 6 6 7	6 6 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
495	7 6 6 6 6 7 7 7 6	6 6 6 6 6 7 6 6 6 6	6 6 6 7 6 6 6 6 6 6	6 7 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
496	6_{15} 6 6 6 6 6 6 7 7	6 6 6 6 6 6_{15} 15_{14} 6 6	6 6 6 6 7 6 6 6 6 6	6_{15} 7 6 6 6 6 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
497	7_{15} 6 6 6 6 6 6 7 7	6 7 6 6 6 6 6_{15} 15_{15} 6 6	6 6 6 6 7 7 6 6 6 6	6_{15} 14_{14} 7 6 6 6 6 6 6 6	6 6 6 7 6 6 6 6 6 6	6
498	6 6_{15} 6 6 6 6 6 6 6	7 6 6 6 6 6 6 6 6_{15} 6	6 6 6 6 6 7 6 6 6	6 6 6 6_{13} 7 6 6 6 6	6 6 6 6 6 6 6 6 6 6	6
499	* 6 6_{15} 6 6 6 6 7 7	6 7 6 6 6 6 6_{15} 15_{15} 6_{15}	6 6 6 6 6 6 6 7 6 6	6 6_{15} 6 6 6_{12} 7 6 6 6 7	6 6 6 6 6 6 6 6 6 6	6
500	7 6 6 6_{15} 6 6 6 7 7	6 6 7 6 6 6 6 6 6 6	6_{15} 6 6 6 6 6 6 6 7 6	6 6 6 6 6_{11} 7 6 6 6	6 6 6 6 6 6 6 6 6 6	6

4.15 Table r-IMOLS$(n;s)$ not known (but $r-1$ are known) for $r = 4, 5, 6$, $1 \le s \le 50$. This table is derived from Table 4.14.

	Number of Incomplete Squares Not Known		
hole	4	5	6
1	14 18 22	15 20 26 30 34 38 46 60	12 21 28 33 35 39 42 44 51 52 54 58 62 66 68 74
2	11 12 13 14 16 18 20 21 22 23 24 25 26 27 30 31 32 34 36 37 38 39 42 44 45 46 48 49 54 78	15 17 19 28 29 33 35 40 50 52 53 56 57 60 61 62 63 69 70 75 76 77 111 112 113 159 160 161 162	41 43 47 51 55 59 64 67 68 71 83 84 85 91 92 99 107 108 109 110 155 156 157 158 259 260
3	17 18 20 21 23 26 27 29 31 32 33 35 37 38 39 41 43 44 47 48 49 50 51 54 55 62 77 78	22 24 25 28 30 34 36 42 45 53 56 57 58 61 70 76 79 112 113 114	40 46 52 60 63 64 65 68 69 71 72 84 85 86 90 92 93 100 106 108 109 110 111 154 156 157 158 159 160 161 162 163 260 261
4	22 24 32 36 38 41 44 48 49 50 51 55 56 63 78 79 80	25 26 27 28 30 31 34 35 37 40 42 43 46 47 54 57 58 59 62 71 77 113 114 115 161 162 163 164	29 33 39 45 52 53 61 64 65 66 69 70 72 73 85 86 91 93 94 101 107 109 110 111 112 155 157 158 159 160 261 262
5	28 29 33 34 37 39 42 47 48 49 52 53 57 78 79 81	31 32 35 38 40 41 43 46 50 51 55 56 60 63 64 72 80 114 115 116 162 163 164 165	44 45 54 58 59 62 65 66 67 70 71 73 74 86 92 94 95 102 106 108 110 111 112 113 156 158 159 160
6	32 34 38 42 44 52 53 54 58 80 81 82	39 40 45 46 48 56 59 60 61 64 65 115 116 117 166	47 50 51 55 57 63 66 67 68 71 72 73 74 75 79 95 96 112 113 114
7	39 41 47 48 52 53	44 45 46 51 54 55 59 60 61 62	58 66 67 68 74 75 76 82 83
8	42 44 45 52	51 53 54 59 60 61	58 62 66 67 68 74 75 76 82 83
9	47 50 53 56 60	59 61 62	66 67 68 74 75 76 83 84 98
10	52 54 56 57 62 68 69 76 78	63 64 65 70 75 77 79 99	72 73 82 83 84 85 111 113 161 163
11	57 58 60 61 62 63 64 65 69 70 72	67 68 71 73 74 76	82 83 98 112 114 162 164
12	62 63 64 65 66 67 70 71 74 75 77 80 81	76 79 83 87	84 85 86 88 89 90 91 93 94 95 98 99 100 101 113 115 122 163 165
13	67 68 70 71 72 74 75 76 80 81 82 84 86	79 83 87 88 89	114 116 122 123 164 166
14	72 73 74 75 76 77 79 80 81 82 83 87 88 89 90 93 96 100 112	86 91 92 94 95 97 99 101 103 107 111 113 114 115 116 117 118 165 167	98 102 104 106 108 109 122 123 124
15	77 78 81 82 83 84 85 86	91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 107 108 109 110 112 113 114 115 116 117 118 119 123 168	111 122 124 125
16	82 83 84 85 87 89 90 91 93 95 99 102 103 105 108	96 98 100 101 104 106 107 109 110 111 167 169	

	Number of Incomplete Squares Not Known		
hole	4	5	6
17	86 87 88 90 91 92 93 94 96 98 99 100 102 103 104 106	105 107 108 109 110 111 112 114 115 116 117 118 168 170	
18	92 93 94 95 97 99 100 101 104 105 110 111 112 113 116 117 120 124 125 128 132	108 109 114 115 118 119 121 122 123 126 129 131 133 134 135 139 143 147 148 149 169 171	130 136 137 138 140 141 142
19	96 98 100 101 102 104 105 106 108 111 112 113 114 116 126 132	117 118 119 120 121 122 123 124 125 127 128 129 130 170 172	178
20	102 103 104 106 107 109 110 112 113 114 118 122 126	120 123 124 125 127 128 129 130 131 133 134 135 136 137 138 139 140 141 142 143 144 145 147 149 150 151 155 159 160 163 165 166 167 168 169 170 171 172 173 179	146 148 152 153 154 156 157 158 161 162 178
21	107 108 113 114 115 116 119 120 128 131	126 127 129 130 132 134 135 136 137 138 139 140 141 142 143 144 145 146 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 166 167 169 170 171 172 173 174 179 180	147 149 165 168 178
22	112 114 115 116 117 119 121 123 127 128 129 131 135 137 143 147 151 153	132 133 136 138 139 140 141 142 144 145 146 148 149 152 154 155 156 157 158 159 160 161 162 163 164 165 167 168 169 170 171 172 173 174 175 179 180 181	166 178
23	116 117 118 120 121 122 123 124 126 128 129 130 132 133 134 136 138 139 144 145 146 147 149 152 157	140 141 142 143 148 150 153 154 155 156 158 159 160	
24	122 123 124 126 129 130 131 134 142 146 147 155 158	144 148 149 150 151 153 154 156 157 159 160 161 163 164 165 166 167 171	170 172 173 174 178 180 182 183 186 188 189 190 194 196
25	128 131 132 134 138 140 162	150 152 154 155 156 157 158 159 160 161 163 164 165 166 167 168 170 171 172 173 174	
26	131 132 133 134 135 137 139 141 142 144 147 148 149 151 153 155 163 164	156 158 159 160 161 162 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 184 185 187 188 189 190 191 192 193 195 196 197 198 199 203 207 211 213	186 194 200 201 202 204 205 206 210 212

	Number of Incomplete Squares Not Known		
hole	4	5	6
27	137 138 145 149 150 151 158 161	162 163 164 165 166 167 168 169 170 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 188	
28	142 143 144 146 149 150 151 153 159 165	168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 189 191 192 193 194 195 199	196 198 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 226 227 228 229
29	147 150 151 152 153 154 156 158 160 166 167 168 170 171	174 175 176 177 178 180 181 182 183 184 185 186 187 188 190 191 192 193 194 195 196 198 199 200 201 202	
30	152 153 154 157 159 161 164 168 172	182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 207 208 209 210 212 213 214 215 216 217 218 219 220 221 223 224 227 228 229 231 239 243 245	222 225 226 230 232 233 234 235 236 237 238 242 244
31	158 160 162 168 170 172 173	186 188 189 190 192 193 194 195 196 197 198 199 200 201 202 203 204 205 208 209 210 211 212 213 214 215 216	
32	162 163 164 166 169 170 171 172 173 174 178 187 189	192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 208 209 210 211 212 213 214 215 216 217 219 220 221 222 223	
33	167 168 171 175 191	198 199 200 201 202 203 204 205 206 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 226 227 228 229 230 234	231 233 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 282 283 284 290
34	172 173 174 175 176 179 180 183 191 195 198 199 200 201 204 206	205 207 208 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 227 228 229 230 231 232 233 235 236 238 239 240 241 243 244 245 246 247 248 249 250 252 253 254 255 256 257 260 261 262 263 264 265 267 268 269 271 272 277 278 283 285	242 251 258 259 266 270 274 275 276 279 280 281 284 290 291
35	178 184 186	211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 228 229 230 231 232 233 234 236 237 239 240 241 242 244 247 248 249 250 255	245 251 253 254 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 284 285 286 290 291 292

	Number of Incomplete Squares Not Known		
hole	4	5	6
36	182 184 194	216 218 219 220 221 223 224 225 226 227 229 230 231 232 233 234 235 237 238 240 241 242 243 245 248 249 250 251	255 256 257 258
37	188 190 192 194 198 202 208 214	222 224 225 226 227 228 230 231 232 233 234 235 236 238 239 241 242 243 244 246 248 249 250 251 252 255 256 257	
38	191 193 195 196 197 199 201 202 203 204 205 208 209 210 212 215 216 217 221	228 230 231 232 233 234 235 236 237 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 256 257 258 259 260 261 262 265 266 268 272 273 274 275 276 277 280 281 282 284 287 289 291 292 293 295 303 307 309 311 315 323	269 270 271 278 279 283 285 286 288 290 294 296 297 298 299 300 301 302 304 305 306 308 310 312 313 314 316 317 322
39	197 198 205 210 211 216 217 222	234 235 236 237 238 240 241 242 243 244 245 246 248 250 251 252 253 254 255 257 258 259 260 261 262 263 265 266 267 268 269 272 275 276 277 283 288 293 299 301 302 303 304 306 307 308 315	273 274 278 279 280 281 282 284 285 286 287 289 290 291 292 294 295 296 297 298 300 305 309 310 311 312 313 314 316 317 318 322 323 324
40	203 204 211 218	241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 258 259 260 261 263 264 266 267 268 269 270 273 275 276 277 279 283	282 284 285 286 290 292 294 295 298 300 301 302 306 308 310 313 314 315 318 322 323 324 325
41	206 207 208 212 214 218 222 226 229 232	246 247 248 249 250 252 253 254 255 256 257 259 260 261 262 263 264 265 267 268 269 270 271 272 274 276 277 278 279 280 283 284 285	
42	213 221	254 255 256 257 258 260 261 262 263 264 265 266 268 269 270 271 272 274 275 276 277 278 279 280 281 283 284 285 286	294 295 296 297 298 299 300 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 339 340 341
43	220 221 226 228 248	258 261 262 263 264 266 267 269 270 271 272 273 274 275 276 277 278 279 280 281 282 285 286 287	
44	222 232 235 246 249 250	264 265 266 267 268 270 271 272 273 274 275 276 277 279 280 281 282 283 285 286 287 288 290 291 293 295 297 298 299 301 304 305 306 307 311	308 309 310 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 369 370 371

hole	Number of Incomplete Squares Not Known		
	4	5	6
45	228 236 251	271 272 273 274 275 276 277 278 279 280 281 282 283 284 286 287 288 289 292 294 296 297 298 299 300 302 303 305 306 307 308 311 312 313 314	317 318 319 320 321 322 323 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 343 344 345 347 348 349 350 351 352 353 354 355 356 357 358 359 361 362 363 364 365 366 370 371 372
46	231 232 233 234 235 237 247 251 255 259	276 277 278 279 280 281 282 283 284 285 287 288 289 290 292 293 295 297 298 299 300 301 303 306 307 308 309 310 311 312 313 314 315 316 317 322 324 327 328 329 331 332 335 337 338 339 344 345 346 349	325 326 330 333 334 336 340 341 342 343 348 350 351 352 353 354 355 357 358 359 360 361 362 363 364 365 366 367 370 371 372 373
47	236 237 238 240 241 243 244 246 248 249 252 253 254 256 259 273 274	282 283 284 285 286 287 288 289 290 291 294 296 298 299 300 301 302 304 305 307 308 309 310 311 312 313 314 315 316 318 320 321 325	
48	242 254 270 278	290 291 292 294 297 299 300 301 302 303 305 306 308 309 310 311 313 314 315 316 317 318 319 321 322 324 325 326	339 340 341 342
49	248	302	
50	251 252 254 256 257 259 262	303 304 305 306 307 309 310 311 312 313 315 316 317 318 319 320 321 322 323 324 326 327 328 332 333 334 335 339	352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 387 388 389 390 395 396 397 398 402 404 406 410 413 418

4.16 **Theorem** [1085] For $n > h > 0$, an ITD$(4, n; h)$ exists if and only if $n \geq 3h$, $(n, h) \neq (6, 1)$.

4.17 **Theorem** [28] For $n > h > 0$, an ITD$(5, n; h)$ exists if and only if $n \geq 4h$ except when $(n, h) = (6, 1)$, and possibly when $h = 1$ and $n = 10$.

4.4 MOLS with Holes

4.18 If $b_1 = b_2 = \cdots = b_s = b$ and if $b_1 + b_2 + \cdots + b_s = n$, then an ILS$(n; b_1, b_2, \ldots, b_s)$ (or a set of IMOLS$(n; b_1, b_2, \ldots, b_s)$) is *uniform* of *type* b^s. In this case, $N(b^s)$ denotes $N(n; b_1, b_2, \ldots, b_s)$. A set of k orthogonal *HMOLS* (holey MOLS) of type b^s is a set of k orthogonal IMOLS$(n; b_1, b_2, \ldots, b_s)$ with $b_1 = b_2 = \cdots = b_s = b$.

4.19 **Remark** Incomplete latin squares of type 1^n are equivalent to idempotent latin squares of side n. So the best lower bounds for $N(1^n)$ are found in Table 3.87 by using Theorem 4.20, when the entry in that table is not italicized.

4.20 **Theorem** $N(n) - 1 \leq N(1^n) \leq N(n)$.

4.21 **Remark** Theorem 4.22 is an analogue to MacNeish's Theorem 3.26 for uniform IMOLS.

4.22 **Theorem** For any divisor a of h, $N(h^n) \geq \min\{N(a^n), N(\frac{h}{a})\}$.

4.23 **Theorem** [1980] $N(h^n) \geq 2$ if and only if $h \geq 1$, $n \geq 4$, and $(h, n) \neq (1, 6)$.

4.24 **Theorem** [197, 869] $N(h^n) \geq 3$ if and only if $h \geq 1$, $n \geq 5$, and $(h, n) \neq (1, 6)$, except possibly for $(h, n) = (1, 10), (3, 6), (3, 18), (3, 28), (3, 34)$, and $(6, 18)$.

4.25 **Remark** [13, 14, 48] At present, the only values of h for which $N(h^6) \geq 4$ is known are those of the form $m \cdot b$ where $N(m) \geq 4$, $b \leq 13$, and $b \notin \{1, 3\}$. For $n \geq 7$, $N(h^n) \geq 4$ if (h, n) is not in the following table:

h	n
1	$10, 14, 18, 22, 26$
2	$28, 30, 32, 33, 34, 35, 38, 39, 40$
3	$6, 12, 18, 24, 28, 46, 54, 62$
4	$20, 22, 24, 28, 30, 32, 33, 34, 35, 38, 39, 40$
5	$18, 22, 26$
6	$18, 22, 24, 26$

h	n
9	$10, 18, 22$
10	$32, 33, 35, 38$
11	$10, 15$
14	34
17	$10, 18, 22$
22	$33, 34, 35, 39, 40$

4.26 **Table** Lower bounds for $N(h^n)$ for $1 \leq h \leq 20$ and $4 \leq n \leq 50$. See [14].

	Size h of Groups																			
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
4	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
6	1	4	2	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	3	4
7	5	5	4	5	4	4	5	5	5	4	5	5	5	5	4	5	5	5	5	4
8	6	6	4	4	4	6	6	6	6	5	6	5	6	6	5	6	6	6	6	4
9	7	5	4	6	4	4	7	7	7	6	7	6	7	6	6	7	7	6	7	4
10	2	4	4	5	4	4	6	8	3	4	3	4	4	5	4	4	3	4	4	4
11	9	5	4	6	4	5	6	7	8	4	9	5	9	5	4	9	9	5	9	4
12	4	4	3	4	4	6	6	7	4	10	4	4	4	5	4	4	4	4	4	4
13	11	5	5	6	4	7	6	7	8	4	10	5	11	5	4	11	11	5	11	4
14	3	4	4	4	4	5	6	7	5	4	5	12	4	5	4	4	4	4	4	4
15	4	4	5	4	4	5	5	6	4	4	4	5	4	4	4	6	4	4	4	4
16	14	4	4	4	4	4	6	7	8	4	10	5	12	4	4	14	14	4	14	4
17	15	5	4	6	4	4	6	7	8	4	10	5	12	6	15	15	15	14	15	4
18	3	4	2	4	3	2	6	7	3	4	5	5	4	5	4	16	3	4	4	4
19	17	5	5	6	4	5	6	7	8	7	10	5	12	5	4	15	16	5	17	4
20	4	4	4	3	4	5	6	7	5	4	5	5	4	5	4	15	4	18	4	4
21	4	4	5	4	4	5	5	4	7	4	4	14	4	4	4	4	4	4	4	4
22	3	4	4	3	3	3	4	4	3	4	4	4	4	4	4	4	3	4	4	4
23	21	5	4	6	4	4	6	7	8	4	10	9	12	5	4	15	16	5	18	4
24	6	4	3	3	4	3	6	7	6	4	6	5	6	5	4	15	6	4	6	4
25	23	6	5	6	4	4	6	7	8	4	10	5	12	6	5	15	16	6	18	4
26	3	4	4	4	3	3	6	7	4	4	5	5	4	5	4	15	4	4	4	4
27	25	5	4	6	4	4	6	7	8	4	10	5	12	5	4	15	16	5	18	4
28	4	3	2	3	4	5	6	7	4	4	5	5	4	5	4	15	4	4	4	4
29	27	6	5	6	4	5	6	7	8	4	10	5	12	6	4	15	16	6	18	5
30	4	3	5	3	4	5	6	7	4	4	5	5	4	5	4	15	4	4	4	5
31	29	5	7	6	4	5	6	7	8	4	10	5	12	5	4	15	16	5	18	23
32	30	3	6	3	4	5	6	7	8	3	10	5	12	5	4	15	16	4	18	4
33	4	3	7	3	4	5	6	7	4	3	5	5	4	6	14	15	4	4	4	4
34	4	3	4	3	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4
35	4	3	4	3	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4

	Size h of Groups																			
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
36	7	4	4	4	4	5	6	7	7	4	7	5	7	4	4	7	7	4	7	4
37	35	6	7	6	4	4	6	7	8	4	10	5	12	6	4	15	16	6	18	4
38	4	3	4	3	4	4	6	7	4	3	5	5	4	5	4	15	4	4	4	4
39	4	3	5	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
40	6	3	4	3	4	4	6	6	6	4	6	5	6	5	4	6	6	4	6	4
41	39	6	4	6	4	4	6	7	8	4	10	5	12	6	4	15	16	6	18	4
42	4	4	4	4	4	4	6	7	4	4	5	5	4	5	4	15	4	4	4	4
43	41	5	7	6	4	5	6	7	8	4	10	5	12	5	4	15	16	5	18	4
44	4	4	4	4	4	4	6	7	4	4	5	5	6	5	4	15	4	5	6	4
45	5	3	4	4	4	4	5	5	5	4	5	5	5	4	4	5	5	6	5	4
46	4	4	3	4	4	4	5	5	4	4	5	5	4	4	4	4	4	4	4	4
47	45	5	4	6	4	4	6	7	8	4	10	5	12	5	4	15	16	5	18	4
48	7	4	4	4	4	4	6	7	7	4	7	5	7	5	4	15	7	4	7	4
49	47	6	4	6	4	5	6	7	8	4	10	5	12	6	4	15	16	6	18	4
50	5	5	4	4	4	5	6	7	5	5	5	5	5	5	5	15	5	5	5	4

See Also

§III.3	Incomplete MOLS are used to construct MOLS.
§III.6	Orthogonal arrays of higher index are analogues of transversal designs and OAs of index one.
§IV.1, §IV.2	TDs and ITDs provide numerous ingredients for the construction of PBDs and GDDs.
§VI.17	Difference matrices, quasi-difference matrices, and $V(m,t)$ vectors are used to construct MOLS and IMOLS.
[543]	Contains a discussion of construction methods for IMOLS.
[721]	The first paper on MOLS with holes.
[1079]	Contains a nice section on MOLS with holes.

References Cited: [13, 14, 28, 48, 197, 341, 543, 721, 798, 869, 1079, 1085, 1966, 1980]

5 Self-Orthogonal Latin Squares (SOLS)

Norman J. Finizio
L. Zhu

5.1 Definitions, Examples and Equivalent Objects

5.1 A *self-orthogonal* latin square (SOLS) is a latin square that is orthogonal to its transpose.

5.2 **Theorem** A self-orthogonal latin square of order n (SOLS(n)) is equivalent to (1) an orthogonal array of strength two and index one, OA(4,n) that is invariant under the row permutation (12)(34) (see §3.2), (2) a $(2,1,3)$-conjugate orthogonal latin square (or quasigroup) of order n (a latin square that is orthogonal to its $(2,1,3)$-conjugate) (see §2), and (3) a spouse avoiding mixed doubles round robin tournament (SAMDRR) with n couples (see §VI.51.11 and Construction VI.51.79).

5.3 **Examples** Self-orthogonal latin squares of orders 4, 5, 7, 8, 9. A SOLS(11) is given in Example 1.117.

1 3 4 2	1 5 4 3 2	1 7 6 5 4 3 2	1 4 7 6 3 5 8 2	1 5 9 6 2 4 8 7 3
4 2 1 3	3 2 1 5 4	3 2 1 7 6 5 4	7 2 1 3 6 8 5 4	8 2 6 9 7 3 5 1 4
2 4 3 1	5 4 3 2 1	5 4 3 2 1 7 6	6 8 3 1 7 2 4 5	2 1 3 7 9 8 4 6 5
3 1 2 4	2 1 5 4 3	7 6 5 4 3 2 1	8 6 5 4 2 7 1 3	7 3 2 4 8 9 1 5 6
	4 3 2 1 5	2 1 7 6 5 4 3	4 1 2 8 5 3 6 7	6 8 4 3 5 1 9 2 7
		4 3 2 1 7 6 5	2 7 4 5 8 6 3 1	3 7 1 5 4 6 2 9 8
		6 5 4 3 2 1 7	5 3 8 2 4 1 7 6	9 4 8 2 6 5 7 3 1
			3 5 6 7 1 4 2 8	4 9 5 1 3 7 6 8 2
				5 6 7 8 1 2 3 4 9

5.4 **Remark** A self-orthogonal latin square has at least one transversal, its main diagonal. So, any self-orthogonal latin square can be made idempotent by renaming the symbols.

5.2 Existence and Basic Constructions

5.5 **Remark** Any self-orthogonal latin square of order 4 or 5 is isotopic to those in Example 5.3.

5.6 **Examples** SOLS(10) and SOLS(14) generated as 1-diagonally cyclic latin squares. In the SOLS(14), 10, 11, and 12 are replaced by a, b, and c, respectively.

0	2	8	6	x	7	1	5	4	3
5	1	3	0	7	x	8	2	6	4
7	6	2	4	1	8	x	0	3	5
4	8	7	3	5	2	0	x	1	6
2	5	0	8	4	6	3	1	x	7
x	3	6	1	0	5	7	4	2	8
3	x	4	7	2	1	6	8	5	0
6	4	x	5	8	3	2	7	0	1
1	7	5	x	6	0	4	3	8	2
8	0	1	2	3	4	5	6	7	x

0	8	3	c	9	2	5	a	6	b	1	4	x	7
x	1	9	4	0	a	3	6	b	7	c	2	5	8
6	x	2	a	5	1	b	4	7	c	8	0	3	9
4	7	x	3	b	6	2	c	5	8	0	9	1	a
2	5	8	x	4	c	7	3	0	6	9	1	a	b
b	3	6	9	x	5	0	8	4	1	7	a	2	c
3	c	4	7	a	x	6	1	9	5	2	8	b	0
c	4	0	5	8	b	x	7	2	a	6	3	9	1
a	0	5	1	6	9	c	x	8	3	b	7	4	2
5	b	1	6	2	7	a	0	x	9	4	c	8	3
9	6	c	2	7	3	8	b	1	x	a	5	0	4
1	a	7	0	3	8	4	9	c	2	x	b	6	5
7	2	b	8	1	4	9	5	a	0	3	x	c	6
8	9	a	b	c	0	1	2	3	4	5	6	7	x

5.7 **Theorem** If q is a prime power ($q \neq 2$), then there exists a SOLS(q) that can be constructed directly in $\mathbb{F}_q$. (See Constructions 5.44 and 5.45).

5.8 **Theorem** If a SOLS(m) and a SOLS(n) exist, then a SOLS(mn) also exists.

5.9 **Theorem** Suppose that a PBD($v, K, 1$) exists and that, for each $k \in K$, a SOLS(k) exists. Then a SOLS(v) exists.

5.10 **Theorem** [322] Self-orthogonal latin squares exist for all orders $n \notin \{2, 3, 6\}$.

5.11 **Remark** Because a PBD($v, \{4, 5, 7, 8, 9, 11\}, 1$) exists for all $v \geq 4$, where $v \notin \{6, 10, 12, 14, 15, 18, 19, 23, 26, 27, 30\}$ (see Table VI.3.23), the proof of Theorem 5.10 can be reduced to orders $v \in \{10, 12, 14, 15, 18, 26, 30\}$. SOLS($v$) for $v \in \{12, 15, 18, 26, 30\}$ are presented in §5.8. SOLS(10) and SOLS(14) are given in Example 5.6.

5.12 **Theorem** Let G be an additive abelian group of order m and let $X = \{x_1, x_2, \ldots, x_n\}$ be an n-set disjoint from G. Consider the elements of X as infinite elements ($x + g = x$

for any $x \in X$ and $g \in G$). Suppose that vector $\mathbf{e} = (e_1, e_2, \ldots, e_m)$ based on $G \bigcup X$ and vectors $\mathbf{f} = (f_1, f_2, \ldots, f_n)$ and $\mathbf{g} = (g_1, g_2, \ldots, g_n)$ based on G satisfy

1. $\{e_1, e_2, \ldots, e_m\} \bigcup \{f_1, f_2, \ldots, f_n\} = G \bigcup X$,
2. $\{e_1 - 1, e_2 - 2, \ldots, e_m - m\} \bigcup \{g_1, g_2, \ldots, g_n\} = G \bigcup X$, and
3. $\{e_{m-i} - e_i + i : 1 \le i \le m, e_i, e_{m-i} \in G\} \bigcup \{\pm(f_i - g_i) : 1 \le i \le n\} = G$.

Then there is a SOLS$(m+n)$ missing a sub-SOLS(n), denoted by ISOLS$(m+n, n)$. Further, if a SOLS(n) exists, then a SOLS$(m+n)$ also exists.

5.13 **Remark** In Theorem 5.12, if $G = \mathbb{Z}_m$ and $X = \emptyset$, then the SOLS is diagonally cyclic. If $G = \mathbb{Z}_m$ and $|X| = 1$, the SOLS is 1-diagonally cyclic (see §1.11).

5.3 Holey SOLS

5.14 A *holey* SOLS (or *frame* SOLS) is a self-orthogonal latin square of order n with n_i missing sub-SOLS (*holes*) of order h_i $(1 \le i \le k)$, which are disjoint and spanning (that is, $\sum_{1 \le i \le k} n_i h_i = n$). It is denoted by HSOLS$(h_1^{n_1} \ldots h_k^{n_k})$, where $h_1^{n_1} \ldots h_k^{n_k}$ is the *type* of the HSOLS.

5.15 **Example** HSOLS(2^4), HSOLS$(2^4 1^1)$, and HSOLS$(2^5 1^1)$. (An HSOLS(2^5) is given in Example 5.53.)

	7	6	8	4	3	5
	5	7	3	8	4	6
6	8			7	1	5	2
8	5			2	7	6	1
3	7	1	8			2	4
7	4	8	2			1	3
5	6	2	1	4	3		
4	3	6	5	1	2		

	6	8	9	7	3	5	4
	7	5	8	9	6	4	3
8	6			7	1	9	2	5
5	7			2	8	1	9	6
4	9	1	7			2	3	8
9	3	8	2			4	1	7
6	4	5	9	3	2			1
3	5	9	6	1	4			2
7	8	2	1	4	3	5	6	

	5	6	b	9	a	3	7	8	4
	6	5	a	7	3	4	8	b	9
b	a			8	2	5	9	6	1	7
8	9			2	b	1	6	5	7	a
9	7	b	8			4	a	2	3	1
3	b	7	a			9	1	4	2	8
4	6	a	b	9	1			3	5	2
a	5	2	9	1	4			b	6	3
6	3	1	7	4	8	b	2			5
5	4	8	1	7	3	2	b			6
7	8	9	2	3	a	6	5	1	4	

5.16 **Example** HSOLS$(1^6 3^1 2^1)$ [2212] and an HSOLS$(2^4 3^1)$. The HSOLS$(2^4 3^1)$ is based on $\mathbb{Z}_8 \bigcup \{a, b, c\}$ constructed 3-diagonally cyclic modulo 8. The holes are based on $\{0, 4\}$, $\{1, 5\}$, $\{2, 6\}$, $\{3, 7\}$, and $\{a, b, c\}$.

	7	5	2	a	9	4	b	3	6	8
6		8	7	3	a	1	5	b	4	9
9	4		a	8	1	b	2	6	5	7
5	b	9		7	2	6	a	1	8	3
7	6	b	3		8	2	4	a	9	1
b	8	4	9	1		a	3	5	7	2
3	a	6	1	b	5				2	4
4	1	a	6	2	b				3	5
a	5	2	b	4	3				1	6
8	9	7	5	6	4	3	1	2		
2	3	1	8	9	7	5	6	4		

	7	3	c		2	b	a	1	6	5
a		0	4	c		3	b	2	7	6
b	a		1	5	c		4	3	0	7
5	b	a		2	6	c		4	1	0
	6	b	a		3	7	c	5	2	1
c		7	b	a		4	0	6	3	2
1	c		0	b	a		5	7	4	3
6	2	c		1	b	a		0	5	4
2	3	4	5	6	7	0	1			
3	4	5	6	7	0	1	2			
7	0	1	2	3	4	5	6			

5.17 **Example** HSOLS$(2^5 u^1)$ for $u = 3$ or 4. The square is based on $\mathbb{Z}_{10} \bigcup X$, where $X = \{a, b, c\}$ or $\{a, b, c, d\}$. It is constructed 3- or 4-diagonally cyclic modulo 10. The holes are based on $\{0, 5\}$, $\{1, 6\}$, $\{2, 7\}$, $\{3, 8\}$, $\{4, 9\}$, and X.

	3	8	7	1		9	c	b	a	2	4	6
a		4	9	8	2		0	c	b	3	5	7
b	a		5	0	9	3		1	c	4	6	8
c	b	a		6	1	0	4		2	5	7	9
3	c	b	a		7	2	1	5		6	8	0
	4	c	b	a		8	3	2	6	7	9	1
7		5	c	b	a		9	4	3	8	0	2
4	8		6	c	b	a		0	5	9	1	3
6	5	9		7	c	b	a		1	0	2	4
2	7	6	0		8	c	b	a		1	3	5
1	2	3	4	5	6	7	8	9	0			
8	9	0	1	2	3	4	5	6	7			
9	0	1	2	3	4	5	6	7	8			

	7	a	b	3		c	8	6	d	2	9	1	4
d		8	a	b	4		c	9	7	3	0	2	5
8	d		9	a	b	5		c	0	4	1	3	6
1	9	d		0	a	b	6		c	5	2	4	7
c	2	0	d		1	a	b	7		6	3	5	8
	c	3	1	d		2	a	b	8	7	4	6	9
9		c	4	2	d		3	a	b	8	5	7	0
b	0		c	5	3	d		4	a	9	6	8	1
a	b	1		c	6	4	d		5	0	7	9	2
6	a	b	2		c	7	5	d		1	8	0	3
4	5	6	7	8	9	0	1	2	3				
2	3	4	5	6	7	8	9	0	1				
7	8	9	0	1	2	3	4	5	6				
3	4	5	6	7	8	9	0	1	2				

5.18 Theorem

1. If there exists an HSOLS($a^n b^1$), then $n \geq 1 + 2b/a$.
2. [2174] For $n \geq 4$ and $a \geq 2$, an HSOLS($a^n b^1$) exists if $0 \leq b \leq a(n-1)/2$ with possible exceptions for $n \in \{6, 14, 18, 22\}$ and $b = a(n-1)/2$.

5.4 Incomplete SOLS

5.19 An *incomplete* SOLS is a self-orthogonal latin square of order n missing a sub-SOLS of order k, denoted by ISOLS(n, k).

5.20 Example An ISOLS(7,2) is shown on the right.

0	2	4	x	y	1	3
y	1	3	0	x	2	4
x	y	2	4	1	3	0
2	x	y	3	0	4	1
1	3	x	y	4	0	2
3	4	0	1	2		
4	0	1	2	3		

5.21 Remark An ISOLS(n, k) is equivalent to an HSOLS($1^{n-k} k^1$). An ISOLS$(n,1)$ or an ISOLS$(n,0)$ is equivalent to a SOLS(n).

5.22 Remark If there exists an ISOLS(n, k), then $n \geq 3k + 1$.

5.23 Theorem [2174] There exists an ISOLS(n, k) for all values of n and k satisfying $n \geq 3k+1$, except for $(n, k) = (6, 1)$, $(8, 2)$ and possibly excepting $n = 3k + 2$ and $k \in \{6, 8, 10\}$.

5.5 SOLS with Additional Properties

5.24 If a SOLS is superimposed with its transpose and if pair (i, j) is in position (x, y) whenever the pair (x, y) is in position (i, j), then the SOLS has the *Weisner property.*

5.25 Example A SOLS(4) with the Weisner property. The second square is a superimposed SOLS(4) in which the Weisner property is readily seen.

1	3	4	2
4	2	1	3
2	4	3	1
3	1	2	4

11	34	42	23
43	22	14	31
24	41	33	12
32	13	21	44

5.26 Theorem The existence of a SOLS(n) with the Weisner property is equivalent to the existence of a Schröder quasigroup of order n (a quasigroup satisfying the identity $xy \cdot yx = x$) (see Proposition 2.47).

5.27 **Theorem** [201, 580] A SOLS(n) with the Weisner property exists for precisely all positive integers $n \equiv 0$ or $1 \pmod 4$ except for $n = 5$.

5.28 **Theorem** [201, 580] An idempotent SOLS(n) with the Weisner property exists for precisely all positive integers $n \equiv 0$ or $1 \pmod 4$ except for $n = 5$ and 9.

5.29 **Theorem** [201] An idempotent ISOLS($n, 2$) with the Weisner property exists for precisely all positive integers $n \equiv 2$ or $3 \pmod 4$, $n \geq 7$, except for $n = 10$.

5.30 A SOLS is *semisymmetric* if the quasigroup satisfies the identity $x(yx) = y$.

5.31 **Example** SOLS(n) with the semisymmetric property for $n = 4$ and 7.

1	3	4	2
4	2	1	3
2	4	3	1
3	1	2	4

0	3	6	2	5	1	4
5	1	4	0	3	6	2
3	6	2	5	1	4	0
1	4	0	3	6	2	5
6	2	5	1	4	0	3
4	0	3	6	2	5	1
2	5	1	4	0	3	6

5.32 **Remark** The existence of a SOLS(n) with the semisymmetric property is equivalent to the existence of a self-orthogonal Mendelsohn triple system of order n (see §VI.35).

5.33 **Theorem** [206] A SOLS(n) with the semisymmetric property exists for all positive integers $n \equiv 0$ or $1 \pmod 3$ except for $n \in \{3, 6, 9, 10, 12\}$ and possibly for $n = 18$.

5.6 SOLS with a Symmetric Orthogonal Mate (SOLSSOM)

5.34 A *SOLSSOM*(n) is a pair (S, M) such that S is a *SOLS*(n) and M is a symmetric latin square of order n that is orthogonal to both S and the transpose of S. A SOLSSOM(n) (S, M) is *regular* if M is (1) *idempotent* if n is odd and (2) *unipotent* with $m_{ii} = n$ if n is even.

5.35 A *transversal* SOLSSOM(n) is such that both S and M are diagonally cyclic if n is odd and 1-diagonally cyclic if n is even.

5.36 **Example** A regular, transversal SOLSSOM(5).

$$S = \begin{array}{|ccccc|}\hline 0&4&3&2&1\\ 2&1&0&4&3\\ 4&3&2&1&0\\ 1&0&4&3&2\\ 3&2&1&0&4\\ \hline\end{array} \qquad M = \begin{array}{|ccccc|}\hline 0&3&1&4&2\\ 3&1&4&2&0\\ 1&4&2&0&3\\ 4&2&0&3&1\\ 2&0&3&1&4\\ \hline\end{array}$$

5.37 **Example** A regular SOLSSOM(9).

$$S = \begin{array}{|ccccccccc|}\hline 1&9&5&8&4&3&6&2&7\\ 6&2&7&1&9&5&8&4&3\\ 8&4&3&6&2&7&1&9&5\\ 9&5&1&4&3&8&2&7&6\\ 2&7&6&9&5&1&4&3&8\\ 4&3&8&2&7&6&9&5&1\\ 5&1&9&3&8&4&7&6&2\\ 7&6&2&5&1&9&3&8&4\\ 3&8&4&7&6&2&5&1&9\\ \hline\end{array} \qquad M = \begin{array}{|ccccccccc|}\hline 1&3&2&7&9&8&4&6&5\\ 3&2&1&9&8&7&6&5&4\\ 2&1&3&8&7&9&5&4&6\\ 7&9&8&4&6&5&1&3&2\\ 9&8&7&6&5&4&3&2&1\\ 8&7&9&5&4&6&2&1&3\\ 4&6&5&1&3&2&7&9&8\\ 6&5&4&3&2&1&9&8&7\\ 5&4&6&2&1&3&8&7&9\\ \hline\end{array}$$

5.38 Example SOLSSOM(12).

$$S = \begin{array}{|cccccccccccc|}\hline 1&3&8&10&7&12&11&4&6&9&2&5\\ 4&2&9&7&11&8&3&12&10&5&6&1\\ 6&12&3&1&9&2&5&10&4&7&8&11\\ 11&5&2&4&1&10&9&6&8&3&12&7\\ 10&1&6&9&5&7&12&2&11&4&3&8\\ 2&9&10&5&8&6&1&11&3&12&7&4\\ 8&11&12&3&10&4&7&5&1&6&9&2\\ 12&7&4&11&3&9&6&8&5&2&1&10\\ 3&8&7&12&2&5&10&1&9&11&4&6\\ 7&4&11&8&6&1&2&9&12&10&5&3\\ 5&10&1&6&12&3&4&7&2&8&11&9\\ 9&6&5&2&4&11&8&3&7&1&10&12\\ \hline\end{array} \qquad M = \begin{array}{|cccccccccccc|}\hline 12&11&8&7&6&2&3&5&10&1&4&9\\ 11&12&7&8&1&6&5&4&2&10&9&3\\ 8&7&12&11&4&5&6&1&3&9&10&2\\ 7&8&11&12&5&3&2&6&9&4&1&10\\ 6&1&4&5&12&11&10&9&8&2&3&7\\ 2&6&5&3&11&12&9&10&1&8&7&4\\ 3&5&6&2&10&9&12&11&4&7&8&1\\ 5&4&1&6&9&10&11&12&7&3&2&8\\ 10&2&3&9&8&1&4&7&12&11&6&5\\ 1&10&9&4&2&8&7&3&11&12&5&6\\ 4&9&10&1&3&7&8&2&6&5&12&11\\ 9&3&2&10&7&4&1&8&5&6&11&12\\ \hline\end{array}$$

5.39 Example A regular, transversal SOLSSOM(4).

$$S = \begin{array}{|cccc|}\hline 0&\infty&1&2\\ 2&1&\infty&0\\ \infty&0&2&1\\ 1&2&0&\infty\\ \hline\end{array} \qquad M = \begin{array}{|cccc|}\hline \infty&2&1&0\\ 2&\infty&0&1\\ 1&0&\infty&2\\ 0&1&2&\infty\\ \hline\end{array}$$

5.7 Existence of SOLSSOMs

5.40 Theorem [17, 209] Regular SOLSSOM(n) do not exist for $n \in \{2, 3, 6\}$ but do exist for all other positive integers n with the possible exception of $n \in \{10, 14\}$.

5.41 Remarks Whenever a SOLSSOM(n) is known, a regular SOLSSOM(n) is also known. Hence, Theorem 5.40 gives the current existence result for SOLSSOM(n) as well. Authorities for the existence of SOLSSOM(n) for $n \leq 100$ are [140, 210, 756, 1458, 2117, 2210].

5.42 Theorem If there exists a SOLSSOM(m) and a SOLSSOM(n) with n odd, then there exists a SOLSSOM(mn).

5.43 Theorem [30, 38, 99] Let p and p_i denote primes of the form $4t + 1$. There exist transversal SOLSSOM(n) for the following cases:

1. $n = 6k \pm 1, k \geq 1$ ($S = (s_{ij}) = (2i - j) \pmod n$ and $M = (m_{ij}) = (\frac{i}{2} + \frac{j}{2}) \pmod n$);
2. $n = 3^{2m+1} + 1,\ m \geq 0$;
3. $n = 3^{4m},\ m \geq 1$;
4. $n = \prod_{i=1}^{k} p_i^{m_i},\ m_i \geq 1,\ k \geq 1$;
5. $n = 3\prod_{i=1}^{k} p_i^{m_i} + 1,\ m_i \geq 1$;
6. $n = 3qp^m,\ q \in \{4m+3 :\ 1 \leq m \leq 11\} \cup \{67, 87, 127, 147, 187, 247, 287, 307, 327\}$;
7. $n = q\prod_{i=1}^{k} p_i^{m_i} + 1,\ q \in \{4m + 3 :\ 1 \leq m \leq 24\} \setminus \{11, 87\}, p_i \geq 29,\ m_i \geq 1$;
8. $n \in \{4m :\ 1 \leq m \leq 33, m \neq 3\}$;
9. $n \in \{4m + 1 :\ 1 \leq m \leq 37, m \neq 2\}$.

5.44 Construction There exist idempotent SOLSSOM(q) for any odd prime power q. Let $S = (s_{ij}) = (ui + (1 - u)j)$ and $M = (m_{ij}) = (\frac{i}{2} + \frac{j}{2})$ where $i, j \in \mathbb{F}_q$ and $u \in \mathbb{F}_q \setminus \{0, 1, \frac{1}{2}\}$.

5.45 Construction There exist SOLSSOM(q) for any even prime power $q \geq 4$. Let $S = (s_{ij}) = (ui + (1 - u)j)$ and $M = (m_{ij}) = (i + j)$ where $i, j \in \mathbb{F}_q$ and $u \in \mathbb{F}_q \setminus \{0, 1\}$.

5.8 SOLSSOMs of Orders up to 30

5.46 Remark SOLSSOM(n) for $n = 4, 5, 9$, and 12 are given in §5.6. A direct construction for SOLSSOM(n) when $n = 6k \pm 1, k \geq 1$ is given in Theorem 5.43(1). A direct construction for a SOLSSOM(7) and a SOLSSOM(27) is given in Construction 5.44, and a direct construction for a SOLSSOM(8) and a SOLSSOM(16) is given in Construction 5.45. Direct constructions for the remaining orders of $n \leq 30$ for which SOLSSOMs are known to exist are given here.

5.47 Remark If (S, M) is a transversal SOLSSOM(n), then if n is odd both S and M can be determined by merely presenting their respective first rows. If n is even, then the entry in the cell s_{n1} may also be given (as the squares are 1-diagonally cyclic). Let $S_1 = (s_{11}s_{12}s_{13}\cdots s_{1n})$ and $M_1 = (m_{11}m_{12}m_{13}\cdots m_{1n})$ be the first rows of S and M.

5.48 Table Transversal SOLSSOM(n) for $n \in \{15, 20, 21, 24, 28\}$.

15: $S_1 = (0, 7, 3, 1, 14, 8, 10, 12, 4, 2, 9, 13, 6, 5, 11)$
$M_1 = (0, 2, 5, 10, 13, 11, 14, 4, 12, 8, 6, 9, 7, 3, 1)$

20: $S_1 = (1\ 10\ 14\ 8\ \infty\ 5\ 2\ 9\ 0\ 6\ 13\ 17\ 16\ 4\ 12\ 3\ 15\ 11\ 7\ 18)$ $s_{n1} = 14$
$M_1 = (\infty\ 1\ 13\ 12\ 8\ 3\ 16\ 6\ 15\ 14\ 5\ 7\ 18\ 10\ 17\ 4\ 9\ 11\ 0\ 2)$

21: $S_1 = (1\ 12\ 16\ 11\ 17\ 8\ 5\ 4\ 13\ 7\ 20\ 6\ 0\ 19\ 10\ 15\ 18\ 3\ 9\ 2\ 14)$
$M_1 = (1\ 0\ 19\ 10\ 9\ 13\ 12\ 18\ 2\ 4\ 3\ 14\ 16\ 15\ 11\ 6\ 8\ 5\ 7\ 17\ 20)$

24: $S_1 = (1\ 21\ 9\ 22\ 17\ 10\ 16\ 6\ 19\ 3\ 8\ \infty\ 14\ 2\ 20\ 18\ 7\ 12\ 4\ 0\ 5\ 13\ 15\ 11)$ $s_{n1} = 23$
$M_1 = (\infty\ 1\ 22\ 19\ 10\ 9\ 14\ 18\ 13\ 21\ 17\ 3\ 15\ 7\ 12\ 5\ 11\ 8\ 4\ 6\ 16\ 20\ 0\ 2)$

28: $S_1 = (1\ 7\ 17\ 19\ 4\ 3\ 23\ 21\ 13\ 11\ 14\ 10\ 24\ 9\ 22\ 6\ 2\ 26\ 25\ \infty\ 12\ 5\ 15\ 18\ 0\ 8\ 20\ 16)$ $s_{n1} = 24$
$M_1 = (\infty\ 23\ 21\ 11\ 1\ 18\ 10\ 12\ 14\ 7\ 26\ 20\ 0\ 3\ 17\ 15\ 9\ 16\ 25\ 6\ 5\ 4\ 13\ 24\ 8\ 19\ 22\ 2)$

5.49 Remark Some SOLSSOM(n) for orders n not covered in Remark 5.46 or Table 5.48 can constructed by choosing both S and M to be standard 4-diagonally cyclic latin squares. If (S, M) has this structure, then, as described in §III.1.11, it is only necessary to give the first rows S_1 and M_1 of each; cells $s_{\infty_1}, s_{\infty_2}, s_{\infty_3}, s_{\infty_4}$; and the corner subsquares S_∞ and M_∞ (described in Remark III.1.124).

5.50 Table Regular SOLSSOM(n) for $n \in \{18, 22, 26, 30\}$. Each of these squares is of the type described in Remark 5.49. To construct the matrix M, one further rule is applied: if $m_{ij} = \infty_2$, then $m_{i+1,j+1} = \infty_3$, and if $m_{ij} = \infty_3$, then $m_{i+1,j+1} = \infty_2$ $(0 \leq i, j \leq n-5)$. All arithmetic on subscripts is modulo $n-4$. Let

$S_\infty =$

∞_1	∞_4	∞_2	∞_3
∞_3	∞_2	∞_4	∞_1
∞_4	∞_1	∞_3	∞_2
∞_2	∞_3	∞_1	∞_4

$M_\infty =$

∞_4	∞_1	∞_2	∞_3
∞_1	∞_4	∞_3	∞_2
∞_2	∞_3	∞_4	∞_1
∞_3	∞_2	∞_1	∞_4

n = 18 :
$S_1 = (1\ 8\ 0\ 13\ 12\ 11\ 3\ 2\ 10\ \infty_4\ \infty_3\ \infty_2\ \infty_1\ 4\ 9\ 6\ 5\ 7)$,
$(s_{\infty_1}, s_{\infty_2}, s_{\infty_3}, s_{\infty_4}) = (0, 4, 13, 3)$,
$M_1 = (\infty_4\ \infty_2\ 13\ 6\ 9\ 7\ 4\ \infty_1\ 12\ 2\ 5\ 3\ 11\ \infty_3\ 0\ 10\ 8\ 1)$.
n = 22 :
$S_1 = (1\ 10\ 0\ 17\ 16\ 15\ 9\ 7\ 12\ 2\ 5\ 8\ 14\ \infty_4\ \infty_1\ \infty_2\ \infty_3\ 6\ 3\ 4\ 11\ 13)$,
$(s_{\infty_1}, s_{\infty_2}, s_{\infty_3}, s_{\infty_4}) = (5, 6, 8, 17)$,
$M_1 = (\infty_4\ \infty_2\ 0\ 11\ 3\ 14\ 10\ 13\ 5\ \infty_1\ 15\ 6\ 4\ 9\ 17\ 8\ 16\ \infty_3\ 12\ 1\ 7\ 2)$.
n = 26 :
$S_1 = (1\ 10\ 0\ 21\ 20\ 19\ 16\ 13\ 11\ 14\ 17\ 2\ 12\ 15\ 9\ 8\ 6\ \infty_4\ \infty_3\ \infty_2\ \infty_1\ 18\ 5\ 4\ 7\ 3)$,
$(s_{\infty_1}, s_{\infty_2}, s_{\infty_3}, s_{\infty_4}) = (8, 11, 21, 4)$,
$M_1 = (\infty_4\ \infty_2\ 0\ 10\ 17\ 14\ 8\ 18\ 1\ 12\ 4\ \infty_1\ 16\ 3\ 15\ 11\ 2\ 9\ 13\ 7\ 20\ \infty_3\ 21\ 19\ 6\ 5)$.

$\mathbf{n = 30}$:
$S_1 = (1\ 8\ 0\ 25\ 24\ 23\ 5\ 12\ 16\ 19\ 22\ 13\ 15\ 2\ 9\ 21\ 20\ 14\ 18\ 6\ 11\ \infty_4\ \infty_3\ \infty_2\ \infty_1\ 10\ 3\ 4\ 7\ 17)$,
$(s_{\infty_1}, s_{\infty_2}, s_{\infty_3}, s_{\infty_4}) = (14, 9, 16, 19)$,
$M_1 = (\infty_4\ \infty_2\ 0\ 10\ 3\ 21\ 18\ 20\ 19\ 14\ 6\ 2\ 1\ \infty_1\ 15\ 17\ 22\ 5\ 11\ 13\ 12\ 16\ 25\ 7\ 24\ \infty_3\ 23\ 8\ 4\ 9)$.

5.9 Holey SOLSSOMs

5.51 A *holey* SOLSSOM (or *frame* SOLSSOM) is a holey self-orthogonal latin square S of order n and type $h_1^{n_1}...h_k^{n_k}$, together with a symmetric partitioned latin square M of order n and type $h_1^{n_1}...h_k^{n_k}$, satisfying the property that when superimposed, the ordered pairs are exactly those pairs of symbols that are from different holes. A holey SOLSSOM with this structure is denoted by HSOLSSOM $(h_1^{n_1}...h_k^{n_k})$, where $h_1^{n_1}...h_k^{n_k}$ is the *type* of the HSOLSSOM.

5.52 **Theorem** [209, 210, 869] An HSOLSSOM of type h^n with $h \geq 2$ can exist only if $n \geq 5$; in addition if h is odd, n must be odd. These necessary conditions are sufficient except possibly for $(h, n) \in \{(6, 12), (6, 18)\}$.

5.53 **Example** HSOLSSOM(2^5).

$S =$

		10	5	9	8	3	6	4	7
		6	9	7	10	5	4	8	3
6	9			2	7	1	10	5	8
10	5			8	1	9	2	7	6
7	10	8	1			4	9	3	2
9	8	2	7			10	3	1	4
5	4	9	2	10	3			6	1
3	6	1	10	4	9			2	5
8	3	7	6	1	4	2	5		
4	7	5	8	3	2	6	1		

$M =$

		7	8	3	4	9	10	5	6
		8	7	4	3	10	9	6	5
7	8			9	10	5	6	1	2
8	7			10	9	6	5	2	1
3	4	9	10			1	2	7	8
4	3	10	9			2	1	8	7
9	10	5	6	1	2			3	4
10	9	6	5	2	1			4	3
5	6	1	2	7	8	3	4		
6	5	2	1	8	7	4	3		

5.10 Related Designs

5.54 **Theorem** Regular SOLSSOM(n) exist if and only if there exists a resolvable spouse avoiding mixed doubles round robin tournament for n couples (see §VI.51.11).

5.55 **Theorem** If there exists a regular SOLSSOM(n), then there exists a triplewhist tournament for $4n$ players (see §VI.64.3).

5.56 **Theorem** If there exists a ($\mathbb{Z}$-cyclic) TWh(n) or if there exists a ($\mathbb{Z}$-cyclic) directed whist tournament DWh(n) on n players, then there exists a transversal SOLSSOM(n).

5.57 A k-SOLSSOM(n) is a set $\{(S_1, S_2, \ldots, S_k\}$ of self-orthogonal latin squares, together with a symmetric latin square M, for which $\{S_i, S_i^T : 1 \leq i \leq k\} \cup \{M\}$ is a set of $2k + 1$ MOLS(n).

5.58 **Theorem** [1086] For any odd prime power q, there exist $((q-3)/2)$-SOLSSOM(q). In addition, for $n \geq 1$ there is a $(2^{n-1} - 1)$-SOLSSOM(2^n).

5.59 **Theorem** [10] There exist 2-SOLSSOM(n) for all $n > 700$.

5.60 **Remark** [10] There exist 2-SOLSSOM(n) for any odd integer $n \geq 7$ except possibly for $n \in \{15, 21, 33, 35, 39, 51, 65, 87, 123, 135\}$.

See Also

§II.7	Resolvable and near-resolvable designs.
§III.1	SOLS are special types of latin squares.
§III.3	SOLS are examples of MOLS.
§VI.64	Whist tournaments.
[92]	Basic facts on SOLS.
[816]	Explicit constructions for some small SOLSSOMs.

References Cited: [10, 17, 30, 38, 92, 99, 140, 201, 206, 209, 210, 322, 580, 756, 816, 869, 1086, 1458, 2117, 2174, 2210, 2212]

6 Orthogonal Arrays of Index More Than One

Malcolm Greig
Charles J. Colbourn

6.1 Definition and Equivalent Objects

6.1 An *orthogonal array* of *size* N, with k *constraints* (or of *degree* k), s *levels* (or of *order* s), and *strength* t, denoted $\mathrm{OA}(N, k, s, t)$, is a $k \times N$ array with entries from a set of $s \geq 2$ symbols, having the property that in every $t \times N$ submatrix, every $t \times 1$ column vector appears the same number $\lambda = \frac{N}{s^t}$ times. The parameter λ is the *index* of the orthogonal array. An $\mathrm{OA}(N, k, s, t)$ is also denoted by $\mathrm{OA}_\lambda(t, k, s)$. If t is omitted, it is understood to be 2. If λ is omitted, it is understood to be 1.

6.2 **Remark** If one takes the key property that for any given $t \times N$ submatrix, every possible $t \times 1$ column vector appears the same number of times, then this property can hold even if the number of symbols used varies from row to row. Such designs are *mixed orthogonal arrays* or *asymmetric orthogonal arrays*. See also §III.7.4. If there are n_i rows with s_i symbols, the notation $\mathrm{L}_N(s_1^{n_1} s_2^{n_2} \dots)$ is used, where $k = \sum n_i$.

6.3 **Remark** In this chapter, only OAs of strength two and arbitrary index are treated.

6.4 An $(n, k; \lambda)$-*net* is a set X of λn^2 points together with a set $\mathcal{D}$ of kn subsets of X (*blocks*) each of size λn. The set of all blocks is partitioned into k parallel classes, each containing n disjoint blocks. Every two nonparallel blocks intersect in λ points.

6.5 **Remark** Alternative names for an $(n, k; \lambda)$-net are *affine resolvable 1-design* or *affine 1-design*. Here the adjective *affine* indicates that every two nonparallel blocks intersect in the same number of points.

6.6 **Theorem** An $\mathrm{OA}_\lambda(k, n)$ is equivalent to a $\mathrm{TD}_\lambda(k, n)$ and an $(n, k; \lambda)$-net (the dual structure).

6.7 An $\mathrm{OA}_\lambda(k, n)$ is *class-regular* or *regular* if some group Γ of order n acts regularly on the symbols of the array.

6.8 **Theorem** A class regular $\mathrm{OA}_\lambda(k, n)$ is resolvable and hence gives an $\mathrm{OA}_\lambda(k + 1, n)$.

6.2 Existence

6.9 **Theorem** (*Bose–Bush bound*) An $\mathrm{OA}_\lambda(k,v)$ exists only if $k \le \left\lfloor \frac{\lambda v^2-1}{v-1} \right\rfloor$. Moreover, if $\lambda - 1 \equiv b \pmod{v-1}$ and $1 < b < v-1$, then

$$k \le \left\lfloor \frac{\lambda v^2 - 1}{v-1} \right\rfloor - \left\lfloor \frac{\sqrt{1+4v(v-1-b)} - (2v-2b-1)}{2} \right\rfloor - 1.$$

6.10 **Example** For asymmetric OAs, a Bose–Bush type bound is also available. Consider a possible $\mathrm{L}_{36}(2^{12}3^{12})$, so $N = 36$ and $k = 24$. Let $R = \sum N/s_i = 360$; let $Q = \sum N/{s_i}^2 = 156$. It is necessary that $\binom{\alpha+1}{2}(N-1) - \alpha(R-k) + (R^2/N - Q)/2 - \binom{k}{2} \ge 0$ for any integral α, and, in particular, for $\alpha = \left\lfloor \frac{R-k}{N-1} \right\rfloor$. Here $35\binom{10}{2} - 9{\cdot}336 + 1722 - 276 = -3$, so the OA is not possible. An $\mathrm{L}_{36}(2^{11}3^{12})$ exists [2208].

6.11 **Theorem** A Hadamard matrix $H(4n)$ is equivalent to a $\mathrm{TD}_n(4n-1,2)$.

6.12 **Theorem** [1905] An affine resolvable 2-design with parameters 2-(v,k,λ) exists only if there are integers $n \ge 2$ and $\mu \ge 0$ for which $v = \mu n^2$, $k = \mu n$, and $\lambda = \frac{\mu n - 1}{n-1}$. Such an *affine design* is denoted $\mathrm{AD}(n,\mu)$; every two nonparallel blocks intersect in μ points. An $\mathrm{AD}(n,\mu)$ is equivalent to an $\mathrm{OA}_\mu(\ell,n)$ where $\ell = (\mu n^2 - 1)/(n-1)$.

6.13 **Remarks** Theorem 6.12 characterizes, in one sense, the upper bound in Theorem 6.9. Only two families of $\mathrm{AD}(n,\mu)$ are known:

- $\mathrm{AD}(q, q^n)$ for q a prime power, $n \ge 0$, are the affine geometries (see §VII.2.4).
- If a Hadamard matrix of order $4n$ exists, its Hadamard 3-design is an $\mathrm{AD}(2,n)$.

Shrikhande [1905] conjectures that no others exist.

6.14 An *α-parallel class* in an $\mathrm{OA}_\lambda(k,n)$ is a set of αn columns, so that each of the n symbols occurs in each row α times within these columns. An $\mathrm{OA}_\lambda(k,n)$ is *α-resolvable* if its columns can be partitioned into α-parallel classes.

6.15 **Theorem** If an α-resolvable $\mathrm{OA}_\lambda(k,n)$ exists and a β-resolvable $\mathrm{OA}_\mu(k',n)$ exists for which $\mu = \frac{\lambda}{\alpha n}$, then an $\alpha\beta n$-resolvable $\mathrm{OA}_\lambda(k+k',n)$ exists.

6.16 **Theorem** Let p be a prime and $u \ge 0$, $v \ge 1$ be integers. Let $s = p^v$ and $d = \lfloor \frac{u}{v} \rfloor$. Then an $\mathrm{OA}_{p^u}(p^u \frac{s^{d+1}-1}{s^d - s^{d-1}} + 1, s)$ exists.

6.17 **Theorem** Let q be a prime power and $n \ge 0$ be an integer. Then there exists an $\mathrm{OA}_{2q^n}(2\frac{q^{n+1}-1}{q-1} - 1, q)$.

6.18 **Theorem** [1643] If there exists an $\mathrm{OA}_\lambda(k_1,s)$ and a $(s,k_2;\mu)$-difference matrix, then there exists an $\mathrm{OA}_{\lambda\mu s}(k_1k_2+1,s)$. Moreover, if the $\mathrm{OA}_\lambda(k_1,s)$ is completely resolvable, and an $\mathrm{OA}_{\lambda\mu}(k_3,s)$ exists, then there exists an $\mathrm{OA}_{\lambda\mu s}(k_1k_2+k_3,s)$.

6.19 **Theorem** [1643] If an $\mathrm{OA}_\lambda(k_1,s)$ and an $\mathrm{OA}_\mu(k_2,s)$ both exist, then an $\mathrm{OA}_{\lambda\mu s^2}((k_1+1)(k_2+1)-1,s)$ exists.

6.20 **Theorem** [1041] A $\mathrm{TD}_\lambda(7,n)$ exists for all $\lambda \ge 2$ and $n \ge 2$.

6.21 **Theorem** [6, 21, 528] For $\lambda \ge 2$, a $\mathrm{TD}_\lambda(8,n)$ exists except when $\lambda = 2$ and $n \in \{2,3\}$, and possibly when $\lambda = 2$ and $n = 6$.

6.22 **Theorem** [21, 528] For $\lambda \ge 2$, a $\mathrm{TD}_\lambda(9,n)$ exists except when $\lambda = 2$ and $n \in \{2,3\}$, and possibly when $\lambda = 2$ and $n \in \{6,14,34,38,39,50,51,54,62\}$; $\lambda = 3$ and $n \in \{5,45,60\}$; and $\lambda = 5$ and $n \in \{6,14\}$.

6.23 **Theorem** [21, 22] A $\mathrm{TD}_\lambda(10,n)$ exists when $\lambda = 3$ and $n \notin \{5, 6, 14, 20, 35, 45, 55, 56, 60, 78, 84, 85, 102\}$ and when $\lambda = 9$ and $n \ne 35$.

6.24 Theorem [1780] For fixed positive integers k and n, there exists an integer λ_0 such that for all $\lambda \geq \lambda_0$, a $\mathrm{TD}_\lambda(k,n)$ exists.

6.3 Tables for Existence

6.25 Table Upper and lower bounds on k in $\mathrm{OA}_\lambda(k,n)$ for $1 \leq \lambda \leq 18$ and $2 \leq n \leq 50$. Entries for which the upper and lower bounds match are shown in bold face.

$n\backslash\lambda$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	**3**	**7**	**11**	**15**	**19**	**23**	**27**	**31**	**35**	**39**	**43**	**47**	**51**	**55**	**59**	**63**	**67**	**71**
3	**4**	**7**	**13**	16	22	**25**	31	34	**40**	43	49	52	58	61	67	70	76	**79**
				13	10		13	25		31	13	49	14	25	37	49	25	
4	**5**	**9**	14	**21**	25	30	37	**41**	46	53	57	62	69	73	78	**85**	89	94
			13		10	17	13		37	21	13	61	21	57	22		37	37
5	**6**	**11**	17	23	**31**	36	42	48	56	**61**	67	73	81	86	92	98	106	111
			8	21		16	18	26	21		18	26	26	21	43	81	36	91
6	**3**	13	20	27	34	43	49	56	63	70	79	85	92	99	106	115	121	128
		7	9	13	8	12	9	13	11	12	9	19	11	17	13	25	11	19
7	**8**	**15**	23	30	38	46	**57**	64	72	79	87	95	106	**113**	121	128	136	144
			10	29	12	19		29	29	19	29	50	29		36	38	29	64
8	**9**	**17**	26	34	43	52	61	**73**	81	90	98	107	116	125	137	**145**	154	162
			10	33	10	17	57		22	41	33	33	26	65	57		41	73
9	**10**	**19**	29	38	48	58	68	78	**91**	100	110	119	129	139	149	159	172	**181**
			28	37	19	55	28	73		37	37	109	50	55	55	82	73	
10	9	21	32	42	53	64	75	86	97	111	121	132	142	153	164	175	186	197
	4	10	12	10	10	20	12	11	12	12	11	28	12	12	12	19	12	30
11	**12**	**23**	35	46	58	70	81	93	105	118	**133**	144	156	167	179	191	202	214
			12	45	12	23	12	45	20	31		45	45	31	45	45	45	31
12	13	25	38	50	63	76	88	101	114	127	141	157	169	182	194	207	220	232
	7	12	14	12	12	24	12	24	14	12	31	43	12	24	14	47	24	24
13	**14**	**27**	41	54	68	81	95	109	123	137	151	165	**183**	196	210	223	237	250
			14	53	14	27	14	53	20	27	24	85		28	66	53	53	40
14	12	29	44	58	73	87	102	117	132	147	162	177	192	211	225	240	254	269
	5	8	9	14	8	27	9	28	10	15	9	27	10	27	11	55	10	42
15	16	31	47	62	78	93	109	125	141	156	172	188	205	221	241	256	272	287
	6	9	17	9	17	30	9	30	17	17	17	32	17	30	31	59	36	30
16	**17**	**33**	50	66	83	99	116	133	149	166	183	200	217	234	252	**273**	289	306
			18	65	18	33	18	129	18	33	18	65	18	33	91		34	145
17	**18**	**35**	53	70	88	105	123	141	158	176	194	212	230	248	266	285	**307**	324
			18	69	18	35	18	69	20	35	24	69	28	35	32	273		40
18	19	37	56	74	93	111	130	149	167	186	205	224	243	262	281	300	320	343
	5	18	10	18	10	35	10	18	11	19	11	38	11	19	19	19	18	35
19	**20**	**39**	59	78	98	117	137	157	176	196	216	235	255	275	295	315	336	357
			20	77	20	39	20	77	20	39	24	77	28	39	32	77	32	55
20	21	41	62	82	103	123	144	165	185	206	227	247	268	289	310	331	352	374
	6	9	9	11	9	39	9	11	11	11	9	42	11	11	13	21	11	58
21	19	43	65	86	108	129	151	172	194	216	238	259	281	303	325	347	369	391
	7	9	11	9	9	13	9	42	11	10	11	44	10	13	12	83	11	15
22	20	45	68	90	113	135	158	180	203	226	248	271	294	317	340	363	386	409
	5	9	24	12	24	44	12	24	24	24	24	44	24	24	24	24	24	44
23	**24**	**47**	71	94	118	141	165	188	212	236	259	283	307	331	354	378	402	426
			24	93	24	47	24	185	24	47	24	93	28	47	32	185	32	47

$n\backslash\lambda$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
24	25	49	74	98	123	147	172	196	221	246	270	295	320	345	369	394	419	444
	9	24	26	24	24	48	24	48	26	24	26	48	24	48	26	95	26	70
25	**26**	**51**	77	102	128	153	179	204	230	256	281	307	333	358	384	410	436	462
			26	101	126	51	51	201	101	126	51	101	126	101	126	201	101	126
26	27	53	80	106	133	159	186	212	239	266	292	319	346	372	399	426	453	480
	6	26	11	26	14	51	28	26	26	26	26	51	28	28	26	27	26	51
27	**28**	**55**	83	110	138	165	193	220	248	276	303	331	359	386	414	442	470	497
			82	109	55	82	82	217	244	82	82	109	109	82	82	217	217	244
28	29	57	86	114	143	171	200	228	257	286	314	343	372	400	429	458	486	515
	7	28	10	28	10	28	10	28	10	28	10	30	10	28	12	28	12	28
29	**30**	**59**	89	118	148	177	207	236	266	296	325	355	384	414	444	474	503	533
			30	117	30	59	30	233	30	59	30	117	30	59	32	233	32	59
30	27	61	92	122	153	183	214	244	275	306	336	367	397	428	459	490	520	551
	6	30	32	30	30	59	30	58	32	30	32	59	30	58	32	58	32	59
31	**32**	**63**	95	126	158	189	221	252	284	315	347	379	410	442	474	505	537	569
			33	125	33	63	33	249	33	63	33	125	33	63	33	249	33	63
32	**33**	**65**	98	130	163	195	228	260	293	325	358	391	423	456	489	521	554	587
			33	129	33	65	33	257	33	65	33	129	33	65	33	513	33	65
33	30	67	101	134	168	201	235	268	302	335	369	403	436	470	504	537	571	605
	7	9	12	14	17	65	17	17	17	17	17	65	17	17	17	23	17	65
34	35	69	104	138	173	207	242	276	311	345	380	415	449	484	519	553	588	623
	6	8	11	15	18	18	18	18	18	19	18	23	18	27	18	31	18	100
35	36	71	107	142	178	213	249	284	320	355	391	427	462	498	534	569	605	641
	7	9	9	11	9	12	9	15	10	18	9	18	10	18	10	21	10	18
36	37	73	110	146	183	219	256	292	329	365	402	439	475	512	549	585	622	659
	10	10	38	14	10	70	14	70	38	18	38	70	18	70	38	70	38	106
37	**38**	**75**	113	150	188	225	263	300	338	375	413	451	488	526	563	601	639	676
			38	149	38	75	38	297	38	75	38	149	38	75	38	297	38	75
38	35	77	116	154	193	231	270	308	347	385	424	463	501	540	578	617	656	694
	6	8	11	15	19	20	20	20	20	20	20	23	20	27	20	31	20	35
39	40	79	119	158	198	237	277	316	356	395	435	475	514	554	593	633	673	712
	7	8	13	13	10	14	13	14	14	14	13	25	14	14	14	25	14	27
40	41	81	122	162	203	243	284	324	365	405	446	487	527	568	608	649	690	730
	9	11	42	13	11	78	13	78	42	17	42	78	17	78	42	78	42	78
41	**42**	**83**	125	166	208	249	291	332	374	415	457	499	540	582	623	665	707	748
			42	165	42	83	42	329	42	83	42	165	42	83	42	329	42	83
42	39	85	128	170	213	255	298	340	383	425	468	511	553	596	638	681	724	766
	7	42	44	42	42	82	42	42	44	42	42	82	42	42	44	42	42	124
43	**44**	**87**	131	174	218	261	305	348	392	435	479	522	566	610	653	697	741	784
			44	173	44	87	44	345	44	87	44	173	44	87	44	345	44	87
44	45	89	134	178	223	267	312	356	401	445	490	534	579	624	668	713	758	802
	7	9	12	16	10	87	12	21	12	16	12	87	12	21	19	23	12	87
45	46	91	137	182	228	273	319	364	410	455	501	546	592	638	683	729	775	820
	8	10	8	11	10	12	14	19	13	19	11	21	12	18	28	21	14	19
46	43	93	140	186	233	279	326	372	419	465	512	558	605	652	698	745	791	838
	6	10	11	15	19	23	24	24	24	24	24	48	24	27	24	31	24	136
47	**48**	**95**	143	190	238	285	333	380	428	475	523	570	618	666	713	761	808	856
			48	189	48	95	48	377	48	95	48	189	48	95	48	377	48	95
48	49	97	146	194	243	291	340	388	437	485	534	582	631	680	728	777	825	874
	10	48	13	48	13	95	13	48	17	48	17	95	17	48	19	48	19	95
49	**50**	**99**	149	198	248	297	347	396	446	495	545	594	644	694	743	793	842	892
			50	197	50	99	344	393	99	99	197	197	99	344	344	393	99	197
50	51	101	152	202	253	303	354	404	455	505	556	606	657	708	758	809	859	910
	8	9	11	15	19	99	26	26	26	26	26	99	26	27	26	31	26	148

6.26 Table Lower bounds on k in $\mathrm{OA}_\lambda(k,n)$ for $19 \le \lambda \le 36$ and $2 \le n \le 50$. Upper and lower bounds that match are shown in bold face.

$n\backslash\lambda$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2	**75**	**79**	**83**	**87**	**91**	**95**	**99**	**103**	**107**	**111**	**115**	**119**	**123**	**127**	**131**	**135**	**139**	**143**
3	31	37	46	31	25	97	40	31	**121**	49	37	121	37	97	46	52	37	157
4	21	46	37	41	37	113	37	57	109	65	37	61	37	**169**	133	46	41	181
5	21	121	31	31	36	61	**156**	61	36	61	31	91	43	81	43	86	103	101
6	13	26	13	31	13	49	13	32	13	43	13	31	13	49	13	19	13	55
7	50	29	73	36	38	64	57	183	64	225	36	92	57	64	57	57	89	127
8	33	81	58	65	57	82	57	105	57	81	58	106	57	289	57	73	64	145
9	50	82	91	55	55	217	82	73	271	109	82	109	55	100	91	307	73	361
10	12	37	12	19	12	39	19	20	33	21	12	28	19	37	20	38	27	59
11	45	82	45	**265**	45	122	56	45	45	62	47	65	82	65	133	56	122	67
12	24	48	14	33	31	73	24	24	38	43	24	24	31	48	34	37	31	85
13	53	53	53	40	53	122	85	**365**	66	170	53	66	68	53	53	74	90	87
14	11	27	11	27	11	28	12	28	44	31	12	82	14	55	27	42	28	83
15	17	58	30	30	30	59	30	30	31	32	32	49	31	66	36	69	31	58
16	65	65	65	65	91	129	65	129	65	65	129	96	91	**545**	91	145	65	289
17	66	86	69	40	66	69	69	40	66	69	69	40	69	290	273	**613**	69	97
18	18	70	27	19	18	70	19	35	28	27	19	35	19	70	28	27	19	46
19	**381**	86	77	55	77	77	77	55	77	77	77	55	77	77	77	55	77	290
20	13	77	13	21	11	78	13	39	13	21	11	42	13	78	13	21	13	58
21	11	42	43	13	12	82	11	15	13	44	42	15	12	83	43	15	13	44
22	24	24	24	24	24	87	24	24	24	27	24	44	24	31	24	27	24	44
23	32	93	44	67	**553**	185	47	67	93	93	47	67	185	185	70	67	93	93
24	26	93	26	48	57	95	26	48	26	48	48	48	48	95	26	70	48	93
25	101	126	126	101	126	217	**651**	126	101	126	126	126	201	201	201	126	126	126
26	28	102	28	27	27	51	28	51	28	29	27	126	28	51	28	29	28	51
27	82	109	109	109	82	217	217	217	**757**	109	109	157	109	217	217	244	217	244
28	12	109	13	28	13	30	13	28	31	43	28	30	28	30	28	28	28	30
29	32	117	44	59	48	233	48	59	48	197	**871**	157	117	233	117	117	233	197
30	32	117	32	58	32	59	32	59	32	58	32	59	32	59	32	58	32	59
31	33	125	44	63	48	249	48	63	48	125	60	157	**993**	497	497	125	125	187
32	33	129	33	65	33	257	33	65	33	129	33	65	993	**1057**	70	129	129	187
33	17	23	17	23	17	65	17	23	17	23	17	65	33	31	43	23	17	65
34	18	35	18	35	18	35	18	35	18	35	18	35	18	35	18	35	18	100
35	10	29	10	18	10	19	12	18	10	21	11	19	12	26	12	18	43	21
36	38	70	38	70	38	70	38	70	38	70	38	70	38	70	38	70	57	106
37	38	149	44	75	48	297	48	75	48	149	60	75	60	297	68	75	72	361
38	20	39	20	39	20	39	20	39	20	39	20	39	20	39	20	39	20	39
39	14	27	14	14	14	27	14	14	14	25	14	27	14	27	14	25	14	40
40	42	78	42	78	42	78	42	78	42	78	42	78	42	78	42	78	42	78
41	42	165	44	83	48	329	48	83	48	165	60	83	60	329	68	83	72	165
42	42	166	44	42	44	82	42	82	44	42	44	82	42	166	44	42	44	124
43	44	173	44	87	48	345	48	87	48	173	60	87	60	345	68	87	72	173
44	16	21	24	23	19	87	19	21	24	23	21	87	19	41	24	23	24	87
45	14	31	18	19	19	26	19	19	21	21	18	31	21	178	19	19	28	26
46	24	39	24	43	24	48	24	47	24	47	24	48	24	47	24	47	24	136
47	48	189	48	95	48	377	48	95	48	189	60	95	60	377	68	95	72	189
48	19	190	26	48	26	95	26	95	26	48	26	95	26	190	26	48	26	95
49	197	197	344	344	344	393	197	197	197	344	344	344	344	393	197	197	344	344
50	26	39	26	43	26	99	26	51	26	51	26	99	26	51	26	51	27	148

See Also

§II.7	More on affine resolvable designs.
§III.3	Orthogonal arrays of index one and strength two.
§III.7	Orthogonal arrays of strength more than two.
§VI.17	Difference matrices are extensively used in the direct construction of orthogonal arrays.
§VI.21	Orthogonal arrays are used in the construction of factorial designs.
§VI.22	Mutually orthogonal frequency squares and hypercubes are constructed using OAs of higher index (Theorems 22.15 and 22.16).
§VI.39	Orthogonal arrays are types of orthogonal main effect plans.
[1074]	A new textbook on orthogonal arrays.
[1770]	An old textbook, valuable for the early results.

References Cited: [6, 21, 22, 528, 1041, 1074, 1643, 1770, 1780, 1905, 2208]

7 Orthogonal Arrays of Strength More Than Two

Charles J. Colbourn

7.1 Examples

7.1 **Remark** See §6.1 for required definitions. Only the cases when $t \geq 3$ are considered in this chapter.

7.2 **Example** An $\mathrm{OA}_1(3, 4, 3)$.

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&2&2&2&2&2&2&2&2&2\\
0&1&2&0&1&2&0&1&2&0&1&2&0&1&2&0&1&2&0&1&2&0&1&2&0&1\\
0&1&2&1&2&0&2&0&1&1&2&0&2&0&1&0&1&2&2&0&1&0&1&2&1&2\\
0&1&2&2&0&1&1&2&0&1&2&0&0&1&2&2&0&1&2&0&1&1&2&0&0&1
\end{pmatrix}$$

7.3 **Example** An $\mathrm{OA}_4(3, 16, 2)$.

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&0&0&1&1&0&0&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&1&1&1&1&0&0\\
0&1&0&1&1&0&1&0&0&1&0&1&1&0&1&0&1&0&1&0&0&1&0&1&1&0&1&0&0&1\\
0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0&1&0&0&1&0&1\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0\\
0&1&0&1&0&1&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&0&0&1&1&0&0\\
0&1&1&0&0&1&1&0&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&0&1&1&0&0&1\\
0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&1&1\\
0&1&0&1&1&0&1&0&1&0&1&0&0&1&0&1&1&0&1&0&0&1&0&1&0&1&0&1&1&0\\
0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&0&0&1&1&1&0\\
0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0&1&0&0&1&0&1&1&0&0&1&1&0&1&0
\end{pmatrix}$$

7.4 Example An $\mathrm{OA}_1(6,7,2)$.

$$\left(\begin{array}{l}
01000001111100000000001111111111000000000011111111110000001111101\\
00100001000011110000001111000000111111000011111100000111101111011\\
00010000100010001110001000111000111000111011100011101110111101 11\\
00001000010001001001100100100110100110110110011011011101111011 11\\
00000100001000100101010010010101010101101101010110111011110111 11\\
00000010000100010010110001001011001011011100101101110111101111 11\\
01111110000000000000001111111111111111111100000000000000001111110
\end{array}\right)$$

7.5 Example An $\mathrm{OA}_1(3,6,4)$.

$$\left(\begin{array}{l}
000000000000000011111111111111112222222222222222333333333333333 3\\
000011112222333300001111222233330000111122223333000011112222333 3\\
012301230123012301230123012301230123012301230123012301230123012 3\\
012310322301321010320123321023012301321001231032321023011032012 3\\
012323013210103232101032012323011032321023010123230101231032321 0\\
012332101032230123011032321001233210012323011032103223010123321 0
\end{array}\right)$$

7.2 Equivalent and Related Objects

7.6 Let $\mathcal{C}$ be a v-ary code of length n, a set of codewords that are n-tuples with entries from a fixed v-set, the *alphabet.* The *distance distribution* of $\mathcal{C}$ is the $(n+1)$-tuple of nonnegative rational numbers $A_i, i = 0, 1, \ldots, n$, where

$$A_i = (\#(x,y) \mid x,y \in \mathcal{C}, d(x,y) = i)/ \mid \mathcal{C} \mid .$$

Here $d(x,y)$ is the *Hamming distance* (the number of coordinates in which x and y differ). The *minimum distance* d of $\mathcal{C}$ is the smallest positive integer such that $A_d > 0$. The *dual distance distribution* of $\mathcal{C}$ is the $(n+1)$-tuple of rational numbers $A'_k, k = 0, 1, \ldots, n$, where A'_k is defined via the *Kravchouk transform*

$$A'_k = \tfrac{1}{|\mathcal{C}|} \textstyle\sum_{i=0}^{n} A_i K_k(i).$$

The numbers $K_k(i)$ are evaluations of the *Kravchouk polynomials*

$$K_k(X) = \textstyle\sum_{j=0}^{k} (-1)^j \binom{X}{j} \binom{n-X}{k-j} (v-1)^{k-j}.$$

The A'_k are nonnegative and $A'_0 = 1$. The *dual distance* d' of $\mathcal{C}$ is the smallest integer greater than 0 such that $A'_{d'} > 0$. See [1505] for more information.

7.7 Theorem (Delsarte [674]) $\mathcal{C}$ is an orthogonal array of strength $d' - 1$. If $v = q$ is a prime power and $\mathcal{C}$ is a linear code, then d' is the minimum distance of the dual code $\mathcal{C}^{\perp}$.

7.8 Remark $\mathrm{OA}_1(t,k,s)$ are known as *maximum distance separable (MDS) codes.*

7.3 Existence

7.9 Theorem An $\mathrm{OA}_\lambda(t,k,s)$ is an $\mathrm{OA}_{s\lambda}(t-1,k,s)$.

7.10 Remark Suppose there is an $\mathrm{OA}_\lambda(t,k,s)$. Fixing one row i and one symbol σ, then selecting all columns that contain σ in row i, and finally deleting row i, one obtains an $\mathrm{OA}_\lambda(t-1,k-1,s)$, the *derived OA*.

7.11 Theorem (*Rao bound*) An $\mathrm{OA}_\lambda(t,k,s)$ exists only if

$$\lambda s^t \geq 1 + \begin{cases} \sum_{i=1}^{t/2} \binom{k}{i} (s-1)^i & \text{if } t \text{ even,} \\ \sum_{i=1}^{(t-1)/2} \binom{k}{i} (s-1)^i + \frac{k-1}{(t-1)/2} (s-1)^{(t+1)/2} & \text{if } t \text{ odd.} \end{cases}$$

7.12 **Theorem** [1683] The Rao bound is met with equality

1. when $t = 3$, only for $\mathrm{OA}_n(3, 4n, 2)$ with n integral, and for $\mathrm{OA}_q(3, q+2, q)$ with q even;
2. when $t = 4$, only for $\mathrm{OA}_1(4, 5, 2)$, $\mathrm{OA}_3(4, 11, 3)$, and $\mathrm{OA}_\lambda(4, k, 6)$ with $\lambda = \frac{a^2(9a^2-1)}{288}$, $k = \frac{9a^2+1}{5}$, and $a \equiv 21, 69 \pmod{240}$.
3. when $t = 5$, only for $\mathrm{OA}_1(5, 6, 2)$ and $\mathrm{OA}_3(5, 12, 3)$.

7.13 **Theorem** (*Bush bound*) An $\mathrm{OA}_1(t, k, s)$ with $t > 1$ exists only if

$$k \le \begin{cases} s+t-1 & \text{if} \quad s \text{ even and } t \le s, \\ s+t-2 & \text{if} \quad s \text{ odd and } 3 \le t \le s, \\ t+1 & \text{if} \quad t \ge s. \end{cases}$$

7.14 **Theorem** (*Bose–Bush bound for* $t = 3$) An $\mathrm{OA}_\lambda(3, k, s)$ exists only if $k \le \left\lfloor \frac{\lambda s^2 - 1}{s-1} \right\rfloor + 1$. Moreover, if $\lambda - 1 \equiv b \pmod{s-1}$ and $1 \le b < s-1$, then

$$k \le \left\lfloor \frac{\lambda s^2 - 1}{s-1} \right\rfloor - \left\lfloor \frac{\sqrt{1 + 4s(s-1-b)} - (2s - 2b - 1)}{2} \right\rfloor.$$

7.15 **Table** [1074, Table 12.6(a)] General families of orthogonal arrays. q is a prime power.

t	k	v	λ	Reason
3	2^m	2	2^{m-2}	Theorem 7.17
3	4λ	2	λ	Theorem 7.21
3	$2^m + 2$	2^m	1	Theorem 7.18
3	$q^2 + 1$	q	q	Ovoid
4	$2^m - 1$	2	2^{2m-4}	BCH ($m \ge 4$)
5	$2^m + 1$	2	2^{2m-4}	BCH ($m \ge 5$)
5	2^{2m}	2	2^{4m-5}	Theorem 7.26 ($m \ge 2$)
5	$2^{2m} + 2m$	2	$2^{4(m-1)}$	X4 ($m \ge 2$)
7	2^{2m}	2	2^{6m-8}	Delsarte–Goethals ($m \ge 3$)
$2^{2m-1} - 2^{m-1} - 1$	2^{2m}	2	2^{k-4m-t}	Preparata ($m \ge 2$)
$2^{m-1} - 2^{\lfloor m/2 \rfloor} - 1$	$2^m - 1$	2	2^{k-2m-t}	BCH ($m \ge 4$)
$2^{m-1} - 1$	2^m	2	$2^{2^{m-1}-m}$	Theorem 7.17
$2^{r+1} - 1$	2^m	2	$2^{\sum_{i=0}^{r} \binom{m}{i} - t}$	Reed–Muller ($0 \le r \le m$)
$2^m - 1$	$2^m + 2$	2^m	1	Reed–Solomon
$q^{m-1} - 1$	$\frac{q^m-1}{q-1}$	q	q^{k-m-t}	Theorem 7.17
t	$t+1$	s	λ	Construction 7.16, all s
t	$q+1$	q	1	Theorem 7.18, $q \ge t$

7.16 **Construction** (Zero-Sum) For each of the s^t t-tuples over $\mathbb{Z}_s$, form a column vector of length $t+1$ by adjoining in the last row the negative of the sum of the elements in the first t rows. Use these vectors to form $(t+1) \times s^t$ array; this is an $\mathrm{OA}_1(t, t+1, s)$. See Example 7.4.

7.17 **Theorem** [1031] Using the link to Hamming codes, when q is a prime power and m is a positive integer, there is an $\mathrm{OA}_{q^{k-m-t}}(t = q^{m-1} - 1, k = \frac{q^m-1}{q-1}, q)$. When $q = 2^z$ there is an $\mathrm{OA}_{2^{z-2}}(3, 2^z, 2)$ and an $\mathrm{OA}_{2^{2^{m-1}-m}}(2^{z-1} - 1, 2^z, 2)$.

7.18 **Theorem** [401] If s is a prime power and $t < s$, then an $\mathrm{OA}_1(t, s+1, s)$ exists. Moreover, if $s \ge 4$ is a power of 2, an $\mathrm{OA}_1(3, s+2, s)$ exists. (These are essentially the Reed–Solomon codes.)

7.19 **Remark** Bush's Theorem 7.20 is a generalization of MacNeish's Theorem 3.26.

7.20 **Theorem** [400] If $\mathrm{OA}_{\lambda_i}(t, k, s_i)$ exist for $1 \le i \le m$, then an $\mathrm{OA}_{\prod_{i=1}^{m} \lambda_i}(t, k, \prod_{i=1}^{m} s_i)$ exists.

7.21 Theorem [1879] If t is even, any $\mathrm{OA}_\lambda(t,k,2)$ yields an $\mathrm{OA}_\lambda(t+1,k+1,2)$. Hence, whenever a Hadamard matrix of order $4n$ exists, so also does an $\mathrm{OA}_n(3,4n,2)$.

7.22 Theorem [255, 1643] If s and σ are powers of the same prime, then an $\mathrm{OA}_{\sigma^{t-1}}(t,\sigma s+1,s)$ exists for all $t\geq 3$ and an $\mathrm{OA}_{\sigma^{t-2}/s}(t,\sigma s,s)$ exists for all $t>s$.

7.23 Theorem [1643] If s and σ are powers of the same prime, then if an $\mathrm{OA}_\lambda(3,r,s)$ exists, so also does an $\mathrm{OA}_{\lambda s^2\sigma^2}(3,r\sigma s,s)$.

7.24 Theorem [1643] If an $\mathrm{OA}_\lambda(3,r,s)$ exists, so does an $\mathrm{OA}_{s\lambda}(3,2r,s)$.

7.25 Theorem [280] For any t, k with $2\leq t\leq k$, there exists a number $e_0=e_0(t,k)$ such that for any positive v and any prime power q there is an orthogonal array $\mathrm{OA}(t,k,v\cdot q^e)$ for all $e\geq e_0$.

7.26 Theorem [1074, §10.4] For $j\geq 3$ an odd integer, there exists an $\mathrm{OA}_{2^{2j-3}}(5,2^{j+1},2)$.

7.27 Remark The OAs from Theorem 7.26 arise from the Kerdock codes. They have the largest number of rows permitted by the Rao bound. The Rao bound is not met "with equality," however; compare Theorem 7.12.

7.4 Mixed Orthogonal Arrays

7.28 A *mixed* or (*asymmetric*) *orthogonal array* $\mathrm{OA}(N,s_1\cdots s_\ell,t)$ is an $N\times\ell$ array in which for $1\leq i\leq\ell$ the symbols in the ith column arise from an alphabet of size s_i, and for every selection of distinct columns $i_1,\ldots,i_t$, the $N\times t$ matrix obtained by restricting to these columns contains each of the possible $\prod_{j=1}^t s_{i_j}$ rows the same number of times.

7.29 Remark Exponential notation is often used. An $\mathrm{OA}(N,s_1^{u_1}\cdots s_m^{u_m},t)$ has $\sum_{i=1}^m u_m$ columns, with u_i having an alphabet of size s_i for $1\leq i\leq m$.

7.30 The ith *derived* orthogonal array is obtained from an $\mathrm{OA}(N,s_1\cdots s_\ell,t)$ by first restricting the set of rows to the N/s_i that contain a fixed symbol in the ith column, and then deleting the ith column, to form an $\mathrm{OA}(N/s_i,s_1\cdots s_{i-1}s_{i+1}\cdots s_\ell,t-1)$.

7.31 Theorem (Generalized Rao bound; see [1074]) Let $\ell\geq t\geq 1$, and suppose that an $\mathrm{OA}(N,s_1\cdots s_\ell,t)$ exists. Then if t is even, $N\geq\sum_{j=0}^{t/2}\sum_{I\subset\{1,\ldots,\ell\},|I|=j}\prod_{i\in I}(s_i-1)$. If t is odd and s_ℓ is largest among the $\{s_i\}$s, then

$$N\geq s_\ell\sum_{j=0}^{(t-1)/2}\sum_{I\subset\{1,\ldots,\ell-1\},|I|=j}\prod_{i\in I}(s_i-1).$$

7.32 Theorems (see [344])

1. **Trivial designs:** If $\prod_{i=1}^\ell s_i \mid N$ then an $\mathrm{OA}(N,s_1\cdots s_\ell,t)$ exists.
2. **Juxtaposition:** If an $\mathrm{OA}(N',s'\cdot s_2\cdots s_\ell,t)$ and an $\mathrm{OA}(N'',s''\cdot s_2\cdots s_\ell,t)$ both exist, then an $\mathrm{OA}(N'+N'',s'+s''\cdot s_2\cdots s_\ell,t)$ exists,
3. **Splitting:** If an $\mathrm{OA}(N,(\sigma\times s)\cdot s_2\cdots s_\ell,t)$ exists, then an $\mathrm{OA}(N,\sigma\cdot s\cdot s_2\cdots s_\ell,t)$ exists.
4. **Hadamard:** When a Hadamard matrix of order $m\geq 4$ exists, an $\mathrm{OA}(2m,2^m,3)$ and an $\mathrm{OA}(8m,2^{2m-4}\cdot 4^2,3)$ exist.

7.33 Remarks Mixed orthogonal arrays have been extensively studied for strength $t=2$; see [1772] and references therein for an introduction. Using Theorems 7.32, constructions from linear codes, computational direct constructions, and nonexistence arguments applying the generalized Rao bound, the parameters of $\mathrm{OA}(N,s_1\cdots s_\ell,3)$s with $N\leq 64$ have been completely determined; see Theorem 7.34.

7.34 Theorem [344] An OA$(N, s_1 \cdots s_\ell, 3)$ with $\ell > 3$ and $N \le 64$ exists if and only if $(N, s_1 \cdots s_\ell)$ is obtained by deleting zero or more columns from one of the following: $(2m, 2^m)$ for $m \equiv 0 \pmod 4$; $(2m\rho, 2^{m-1} \cdot (2\rho)^1)$ for $m \equiv 0 \pmod 4$; $(2m\rho, 2^m \cdot \rho^1)$ for $m \equiv 0 \pmod 4$; $(8m, 2^{2m-4} \cdot 4^2)$ for $m \equiv 0 \pmod 4$; $(27, 3^4)$; $(36, 2^2 \cdot 3^2)$; $(40, 2^6 \cdot 5)$; $(48, 2^2 \cdot 4 \cdot 6)$; $(48, 2^4 \cdot 3 \cdot 4)$; $(48, 2^9 \cdot 3)$; $(54, 3^3 \cdot 6)$; $(54, 2 \cdot 3^5)$; $(56, 2^7 \cdot 7)$; $(60, 2^2 \cdot 3 \cdot 5)$; $(64, 2^4 \cdot 4 \cdot 8$; $(64, 4^6)$; $(64, 2^2 \cdot 4^5)$; $(64, 2^6 \cdot 4^4)$; or $(64, 2^8 \cdot 4^3)$.

See Also

§III.1–6	MOLS and transversal designs arise in the case $t = 2$.
§V.1	Hadamard matrices correspond to certain OAs.
§VI.15	OAs are useful in derandomization of randomized algorithms.
§VI.21	Orthogonal arrays are used to construct factorial designs.
§VI.59	(t,m,s)-nets are constructed using orthogonal arrays.
§VII.1	Existence results on codes.
[258]	Chapter 15 explores the connection between OAs and codes.
[559]	A construction of OAs with a non-prime-power number of symbols, from 3-wise balanced designs.
[1074]	A textbook on orthogonal arrays. All OAs in [1074] are given at `http://support.sas.com/techsup/technote/ts723.html`.
[1770]	An old textbook, valuable for the early results.
[1971]	Chapter 10 concerns applications of OAs, and connections with coding theory.

References Cited: [255, 258, 280, 344, 400, 401, 559, 674, 1031, 1074, 1505, 1643, 1683, 1770, 1772, 1879, 1971]

Part IV

Pairwise Balanced Designs

1 PBDs and GDDs: The Basics

Ronald C. Mullin
Hans-Dietrich O. F. Gronau

1.1 PBDs and GDDs

1.1 Let K be a subset of positive integers and let λ be a positive integer. A *pairwise balanced design* (PBD(v, K, λ) or (K, λ)-PBD) of order v with block sizes from K is a pair $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a finite set (the *point set*) of cardinality v and $\mathcal{B}$ is a family of subsets (*blocks*) of $\mathcal{V}$ that satisfy (1) if $B \in \mathcal{B}$, then $|B| \in K$ and (2) every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks of $\mathcal{B}$. The integer λ is the *index* of the PBD. The notations PBD(v, K) and K-PBD of order v are often used when $\lambda = 1$.

1.2 **Example** A PBD$(10, \{3, 4\})$. The blocks are listed columnwise.

1	1	1	2	2	2	3	3	3	4	4	4
2	5	8	5	6	7	5	6	7	5	6	7
3	6	9	8	9	10	10	8	9	9	10	8
4	7	10									

1.3 Let K and G be sets of positive integers and let λ be a positive integer. *A group divisible design of index λ and order v* ((K, λ)-GDD) is a triple $(\mathcal{V}, \mathcal{G}, \mathcal{B})$, where $\mathcal{V}$ is a finite set of cardinality v, $\mathcal{G}$ is a partition of $\mathcal{V}$ into parts (*groups*) whose sizes lie in G, and $\mathcal{B}$ is a family of subsets (*blocks*) of $\mathcal{V}$ that satisfy (1) if $B \in \mathcal{B}$ then $|B| \in K$, (2) every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks or one group, but not both, and (3) $|\mathcal{G}| > 1$.

1.4 If $v = a_1 g_1 + a_2 g_2 + \ldots + a_s g_s$, and if there are a_i groups of size g_i, $i = 1, 2, \ldots, s$, then the (K, λ)-GDD is of type $g_1^{a_1} g_2^{a_2} \ldots g_s^{a_s}$. This is *exponential notation* for the group type. Alternatively, if the GDD has groups $G_1, G_2, \ldots, G_t$, then the list $T = [|G_i| : i = 1, 2, \ldots, t]$ is the *type* of the GDD when more convenient.

1.5 If $K = \{k\}$, then the (K, λ)-GDD is a (k, λ)-GDD. If $\lambda = 1$, the GDD is a K-GDD. Furthermore, a $(\{k\}, 1)$-GDD is a k-GDD.

1.6 **Remark** By convention, factors of type 0^a can be included in the exponential form of the type to accommodate null groups when needed.

1.7 **Example** A {3,4}-GDD of type $1^1 3^3$ or type [3,3,3,1] (the groups are in boldface).

1	**4**	**7**	**10**	1	2	3	1	2	3	1	2	3
2	**5**	**8**		4	5	6	5	6	4	6	4	5
3	**6**	**9**		7	8	9	9	7	8	8	9	7
				10	10	10						

1.8 **Example** A 4-GDD of type 3^9. Let $V = \mathbb{Z}_3^3$. The orbits of {000,020,111,211} and {000,102,012,110} (writing $(x, y, z) \in \mathbb{Z}_3^3$ as xyz) form the blocks. The groups are the orbit of {000,001,002}. Adding a new symbol ∞ to each group gives a (28,4,1) design.

1.9 A GDD is *uniform* if all groups have the same size, that is, if it is of type m^u for some positive integer u.

1.10 A GDD D_1 is *derivable* if it can be obtained from another GDD D_2 by replacing a group G of D_2 by the groups and blocks of a third GDD D_3 defined on the point-set of G. A GDD is *primitive* if it is not derivable.

1.11 Theorem [2211] The necessary conditions for the existence of a uniform (k,λ)-GDD of type m^u are (1) $u \geq k$, (2) $\lambda(u-1)m \equiv 0 \pmod{k-1}$, and (3) $\lambda u(u-1)m^2 \equiv 0 \pmod{k(k-1)}$.

1.12 Remarks

1. A K-GDD of order v with group sizes in a set G can be viewed as a PBD$(v, K \cup G)$ by considering the groups of the GDD to be blocks of the PBD also.
2. A K-GDD of order v with group sizes in a set G can be used to create a PBD$(v+1, K \cup \{g+1 : g \in G\})$ by adjoining a new point (say ∞) to each group to form new blocks. Conversely, a GDD can be obtained from a PBD by deleting a point.
3. A *transversal design* TD(k,n) is a k-GDD of type n^k. A GDD is a transversal design if and only if each block meets every group in exactly one point. See §III.3.
4. A BIBD$(v,k,1)$ is equivalent to a PBD$(v,\{k\})$ and a k-GDD of type 1^v. See §II.1.

1.13 Let $\mathcal{B}$ be a set of blocks in a PBD, GDD, or BIBD. A *parallel class* or *resolution class* is a collection of blocks that partition the point-set of the design.

1.14 A PBD, GDD, or BIBD is *resolvable* if the blocks of the design can be partitioned into parallel classes. In the case of a resolvable BIBD(v,k,λ), RBIBD(v,k,λ) or RB(v,k,λ) is used. A resolvable GDD is denoted by RGDD.

1.15 Theorem [2211] The necessary conditions for the existence of a uniform (k,λ)-RGDD of type m^u are (1) $u \geq k$, (2) $um \equiv 0 \pmod{k}$, and (3) $\lambda(u-1)m \equiv 0 \pmod{k-1}$.

1.16 Let K be a set of positive integers, and let k be a positive integer. PBD$(v, K \cup k^\star)$ denotes a PBD containing a block of size k. If $k \notin K$, this indicates that there is only one block of size k in the PBD. On the other hand, if $k \in K$, then there is at least one block of size k in the PBD.

1.17 Theorem Let D be a BIBD$(v,k,1)$. Let $r = (v-1)/(k-1)$ and suppose $n = v/k$ is an integer. Suppose that D contains $s \geq 1$ mutually block disjoint parallel classes, and let t be an integer. By adjoining new points, one obtains:

1. For $0 \leq t \leq s-1$, there exists a $\{k, k+1\}$-GDD of type $k^n t^1$.
2. For $0 \leq t \leq s$, there exists a PBD$(nk+t, \{k, k+1, t^\star\})$.
3. If $t = s = r$, then there exists a PBD$(nk+r, \{k+1, r^\star\})$. In this case, the operation of creating the design is the *completion* of the (resolvable) BIBD.

1.18 Example D is a resolvable PBD(9,{3}), a 3-GDD of type 3^3, and a BIBD(9,3,1). The blocks are written as columns with space between parallel classes of blocks. If {1,2,3}, {4,5,6}, {7,8,9} are taken as groups of a GDD, there are three parallel classes of the remaining blocks.

$$D = \begin{array}{cccc} 147 & 123 & 123 & 123 \\ 258 & 456 & 564 & 645 \\ 369 & 789 & 978 & 897 \end{array}$$

1.2 PBDs with Mandatory Blocks

1.19 Let K be a set of positive integers, and suppose that $k \in K$. A pairwise balanced design of order v and with block sizes from K has a *mandatory block* of size k if it contains a block of size k.

1.20 Example A PBD$(11, \{3, 5^\star\})$. (The distinguished block is in boldface.)

1	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5
2	6	8	9	6	7	10	6	7	8	6	7	9	6	7	8
3	7	11	10	8	9	11	9	11	10	10	8	11	11	10	9
4															
5															

1.21 Theorem [1062, 468] Let $N_{\geq 3} = \{n \in \mathbb{Z} : n \geq 3\}$. Then a PBD$(v, N_{\geq 3} \cup \{k^\star\})$ with $v > k$ exists if and only if $v \geq 2k + 1$ except when

1. $v = 2k + 1$ and $k \equiv 0 \pmod 2$;
2. $v = 2k + 2$ and $k \not\equiv 4 \pmod 6, k > 1$;
3. $v = 2k + 3$ and $k \equiv 0 \pmod 2, k > 6$;
4. $(v, k) \in \{(7, 2), (8, 2), (9, 2), (10, 2), (11, 4), (12, 2), (13, 2), (17, 6)\}$.

1.22 Theorem [550] Let N_{odd} denote the set of all odd positive integers. Let v and k be odd positive integers that satisfy $v \geq 2k+1$. Then there exists a PBD$(v, N_{odd} \cup \{k^\star\})$.

1.23 Remark When $v \equiv 1$ or 3 (mod 6) and $w \equiv 1$ or 3 (mod 6), Theorem 1.24 is Theorem II.2.37, the *Doyen–Wilson Theorem*.

1.24 Theorem (see [578]) There exists a PBD$(v, \{3, w^\star\})$ with $v > w$ if and only if $v \geq 2w + 1$, and (1) $v \equiv 1$ or 3 (mod 6) and either $w \equiv 1$ or 3 (mod 6) or $w = 0$, or (2) $v \equiv w \equiv 5 \pmod 6$.

1.25 Theorem [1793] There exists a PBD$(v, \{4, w^\star\})$ with $v > w$ if and only if $v \geq 3w + 1$, and (1) $v \equiv 1$ or 4 (mod 12) and $w \equiv 1$ or 4 (mod 12) or (2) $v \equiv 7$ or 10 (mod 12) and $w \equiv 7$ or 10 (mod 12).

1.26 Table Results on some specific families of PBDs with a specified hole size.

Some Families of PBDs with a Given Hole Size					
$K \cup \{k^\star\}$	Congruence Classes	Range For v	Known Exceptions	Possible Exceptions	Ref.
$3, 4, 6^\star$	0,1 (mod 3)	≥ 6	7,9,10,12,13		[975]
$4, 5, 11^\star$	2,3 (mod 4)	≥ 11	14, 15, 18, 19, 22, 23, 26, 27, 30, 31, 34	38, 42, 43, 46, 50, 54, 55, 58, 62, 66, 67, 70, 74, 78, 82, 90, 94, 98, 102, 106, 114, 118, 126, 130, 142, 154, 166, 178, 190, 202, 214, 226	[192, 1468]

1.27 Theorem [39, 195] Necessary conditions for a PBD$(v, \{5\} \cup \{w^*\})$ to exist are $v, w \equiv 1$ (mod 4), $v \geq 4w + 1$, and either $v \equiv w \pmod{20}$ or $v + w \equiv 6 \pmod{20}$. These are sufficient with a few possible exceptions. No exceptions arise when $v \equiv 1, 5, 13$ (mod 20). When $w \equiv 9 \pmod{20}$, there are at most 26 possible exceptions. All possible exceptions satisfy either $v = 4w + 13$ with $w \leq 489$ or $v \not\equiv w \pmod{20}$ with $v < 5w$ and $w \leq 129$. When $w \equiv 17 \pmod{20}$, there are at most 104 possible exceptions. All possible exceptions except $(v, w) = (197, 37), (529, 37)$ satisfy either $v = 4w + 9$ with $w \leq 1757$ or $v \not\equiv w \pmod{20}$ with $v < 5w$ and $w \leq 257$. Possible exceptions with $v < 100$ are listed here:

$w \equiv 9$ (mod 20)	$v \equiv w$ (mod 20)	$v \not\equiv w$ (mod 20)	$w \equiv 17$ (mod 20)	$v \equiv w$ (mod 20)	$v \not\equiv w$ (mod 20)
9	49		17	77	
			37	157, 197	169, 529
49	209	237	57	237	269
69	289	297, 317	77	317	369
89	369		97		429

1.28 A *mandatory representation design* MRD(v, K) is a PBD(v, K) $(V, \mathcal{B})$ in which for each $k \in K$, there is a $B \in \mathcal{B}$ with $|B| = k$ (each block size is *represented* by at least one block).

1.29 **Remark** Necessary and sufficient conditions are established for MRD$(v, \{3, k\})$ with $4 \leq k \leq 50$ [991], and for MRD$(v, \{4, k\})$ when $k \equiv 1 \pmod 3$ with ten possible exceptions [865]. For general results with $k = 3$, see [1789].

1.3 Flats and Holes

1.30 Let $D = (\mathcal{V}, \mathcal{B})$ be a PBD(v, K). When $\mathcal{F} \subset \mathcal{V}$ and $\mathcal{C} \subset \mathcal{B}$, $F = (\mathcal{F}, \mathcal{C})$ is a *flat* in D if $(\mathcal{F}, \mathcal{C})$ is also a PBD. The order of the flat is $|\mathcal{F}|$. In general, the degenerate PBDs of orders 0 and 1 are considered to be flats of all PBDs of order $v > 1$. Such flats are *trivial*.

1.31 **Example** A PBD$(7, \{2, 3\})$ that contains a flat of order 3. (The point set of the flat is {1,2,3}, the blocks of the flat are in boldface.)

1	**1**	**2**	1	1	2	2	3	3
2	**3**	**3**	4	6	4	5	4	5
			5	7	6	7	7	6

1.32 **Remark** In any PBD(v, K), any block can be considered to be a flat. Conversely the blocks of any flat of order w can be replaced by a block of size w containing these points to obtain a PBD$(v, K \cup \{w\})$.

1.33 (Breaking up blocks). Let D be a K-PBD of order v that contains a flat F of order f. Suppose that D' is a PBD(f, K'). Then by replacing the blocks of F by the blocks of D' defined on the point-set of F, a $K \cup K'$-PBD of order v is obtained. In particular, if the flat F is a block B of D, then the design D' is *obtained by breaking up the block* B.

1.34 **Remark** This operation is useful for reducing the set of block sizes of a PBD. For example, let $K' = K \setminus \{k\}$, where $k \in K$. If there exists a K'-PBD of order k and D is a K-PBD of order v, then a K'-PBD of order v can be obtained by breaking up the blocks of size k in D.

1.35 Let K be a set of positive integers and let λ be a positive integer. An *incomplete* PBD of order v and index λ with a hole of order h ($(v, h; K, \lambda)$-IPBD) is a triple $(\mathcal{V}, \mathcal{H}, \mathcal{B})$ where $\mathcal{V}$ is a set of cardinality v, $\mathcal{H}$ is a subset of $\mathcal{V}$ that contains h elements, and $\mathcal{B}$ is a family of subsets (*blocks*) of $\mathcal{V}$ that satisfy the properties:

1. If $B \in \mathcal{B}$, then $|B| \in K$;
2. Every pair of distinct elements $\{x, y\}$ from $\mathcal{V}$ with the exception of those in which both x and y lie in $\mathcal{H}$ occur in precisely λ blocks;
3. No pair of distinct elements of $\mathcal{H}$ occur in any block.

If $\lambda = 1$, the design is a $(v, h; K)$-IPBD, or simply a K-IPBD of order v with a hole of size h.

1.36 **Remark** An incomplete PBD of order v and index 1 with a hole of size h is equivalent to a PBD(v, K) from which a block of size h has been removed.

1.37 Let K be a set of positive integers, and let λ be a positive integer. An *incomplete group divisible design* with block-sizes from K and index λ ((K,λ)-IGDD) is a quadruple $(\mathcal{V}, \mathcal{G}, \mathcal{H}, \mathcal{B})$ where $\mathcal{V}$ is a finite set of cardinality v, $\mathcal{G} = (G_1, G_2, \ldots, G_s)$ is a partition of $\mathcal{V}$, $\mathcal{H} = \{H_1, H_2, \ldots, H_s\}$ is a collection of subsets of V with the property $H_i \subseteq G_i$, $i = 1, 2, \ldots, s$ (the G_i are *groups* and the H_i are *holes*), and $\mathcal{B}$ is a family of subsets of V (*blocks*) that satisfy the properties:

1. Any pair of distinct elements of $\mathcal{V}$ that occurs in a group does not occur in any block;
2. If a pair of distinct elements from V comes from distinct groups and each element occurs in the hole of its respective group, then that pair occurs in no block of $\mathcal{B}$; otherwise, it occurs in exactly λ blocks of $\mathcal{B}$.

An IGDD is of *type* $(g_1, h_1)^{a_1}(g_2, h_2)^{a_2} \ldots (g_t, h_t)^{a_t}$ if there are a_i groups of size g_i that contains a hole of size h_i, $i = 1, 2, \ldots, t$. An IGDD is a K-IGDD if $\lambda = 1$. Further, it is a k-IGDD if $K = \{k\}$.

1.38 **Example** A {3,4}-IGDD of type $(3,1)^3(1,1)^1$. (The groups are printed in boldface; the holes are overscored.)

1	**4**	**7**	$\overline{\mathbf{10}}$	1	2	1	2	3	1	2	3
2	**5**	**8**		4	5	5	6	4	6	4	5
$\overline{\mathbf{3}}$	$\overline{\mathbf{6}}$	$\overline{\mathbf{9}}$		7	8	9	7	8	8	9	7
				10	10						

1.39 **Theorem** [2211] Necessary conditions for the existence of a (k,λ)-IGDD of type $(m,h)^u$ are (1) $m \geq (k-1)h$, (2) $\lambda m(u-1) \equiv 0 \pmod{k-1}$, (3) $\lambda(m-h)(u-1) \equiv 0 \pmod{k-1}$, and (4) $\lambda u(u-1)(m^2-h^2) \equiv 0 \pmod{k(k-1)}$.

1.40 **Example** Incomplete MOLS with one hole (§III.4) provide examples of IGDD. In particular, an ITD$(k, m; h)$ (other notation: a TD$(k,m) -$ TD(k,h)) is a k-IGDD of type $(m,h)^k$.

1.41 Let K be a set of positive integers, let v, w_1, w_2, and λ be positive integers, and let w_3 be a nonnegative integer. Then a $(v; w_1, w_2; w_3; K, \lambda)$-$\diamondsuit$-IPBD *(incomplete-$\diamondsuit$-PBD)* is a quadruple $(\mathcal{V}, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{B})$ where $\mathcal{V}$ is a set of cardinality v; $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are subsets of $\mathcal{V}$ of cardinalities w_1 and w_2, respectively; $|\mathcal{Y}_1 \cap \mathcal{Y}_2| = w_3$; and $\mathcal{B}$ is a collection of subsets (*blocks*) of $\mathcal{V}$ that satisfy the properties:

1. If $B \in \mathcal{B}$, then $|B| \in K$;
2. If $\{x, y\}$ is a pair of distinct elements of $\mathcal{V}$, then $\{x, y\}$ occurs in precisely λ blocks of $\mathcal{B}$ unless $\{x, y\} \subset \mathcal{Y}_1$ or $\{x, y\} \subset \mathcal{Y}_2$, in which case the pair occurs in no block.

If $\lambda = 1$, then the design is a $(v; w_1, w_2; w_3; K)$-$\diamondsuit$-IPBD.

1.42 **Remark** Completing an RBIBD$(v - w_1, k-1, 1)$ having w_1 parallel classes, and containing an RBIBD$(w_2 - w_3, k-1, 1)$ subdesign having w_3 parallel classes where each of the w_3 parallel classes lies within one parallel class of the containing design provides one fruitful way of constructing a (completed) $(v; w_1, w_2; w_3; k, 1) -$ $\diamondsuit$-IPBD.

1.43 A *double GDD*, a K-DGDD $(\mathcal{V}, \mathcal{G}, \mathcal{H}, \mathcal{B})$ has a point set, $\mathcal{V}$, which has two partitions, $\mathcal{G}$ and $\mathcal{H}$, with the properties that any pair of points in different parts of $\mathcal{G}$ and in different parts of $\mathcal{H}$ occurs in exactly one block in the block set $\mathcal{B}$, and pairs of points in the same part of $\mathcal{G}$ or of $\mathcal{H}$ do not occur in any block. All blocks have sizes in K, and the matrix $[|G_i \cap H_j|]$ is the type of the DGDD.

1.44 Remark DGDDs were introduced by Zhu [2211] and further developed by Miao [1598]. Taking $\mathcal{G} = \mathcal{H}$ gives a GDD, and if $|\mathcal{G}| = g$ and $|\mathcal{H}| = h = g + 1$, taking $G_i \subseteq H_i$ for $1 \leq i \leq g$ and $|H_h| > 0$ gives a nontrivial IGDD.

See Also

§II.1	BIBDs are PBDs with one block size.
§III.3	TDs are special classes of GDDs.
§III.4	ITDs are special classes of IGDDs.
[1042]	A large collection of PBDs and GDDs.

References Cited: [39, 192, 195, 468, 550, 578, 865, 975, 991, 1042, 1062, 1468, 1598, 1789, 1793, 2211]

2 PBDs: Recursive Constructions

Malcolm Greig
Ronald C. Mullin

2.1 Some Constructions

2.1 Theorem (*singular direct product* [2145]) If there exists a PBD(v, K) that contains a flat of order f, and if there exists a K-GDD of type $(v - f)^m$, then there exists a PBD$(m(v - f) + f, K)$ that contains flats of orders v and f. (If $f = 0$, this is a product construction.)

2.2 Examples The construction of BIBDs.

1. A TD$(5, 21)$ is a 5-GDD of type 21^5, and a PBD$(21, \{5\})$ exists, so there exists a PBD(105,{5}). This is a (105,5,1) design.
2. A TD$(4, 21)$ is a 4-GDD of type 21^4, and a PBD$(25, \{4\})$ having a flat of size four exists, so a PBD(88,{4}) exists (an (88,4,1) design).
3. A TD$(4, 25)$ and a (25,4,1) design give a (100,4,1) design.
4. A TD$(5, 25)$ and a (25,5,1) design give a (125,5,1) design.
5. A TD$(4, 28)$ and a (28,4,1) design give a (112,4,1) design.
6. A TD$(6, 25)$ and a (31,6,1) design with flats of size 0 and 6 exist. So there are (156,6,1) and (186,6,1) designs.

2.3 Theorem (*singular direct product*, generalized from [2145]) Suppose that there exists a K-GDD of type $g_1^{a_1} g_2^{a_2} \ldots g_s^{a_s}$.

1. If for each $g_i, i = 1, 2, \ldots, s$, there exists a PBD$(g_i + f, K)$ that contains a flat of order f, then there exists a PBD$((\sum_{i=1}^{s} a_i g_i) + f, K)$ that contains flats of order $g_i + f, i = 1, 2, \ldots, s$ and a flat of order f.
2. If for some j there exists exactly one group of size g_j in the GDD (that is, $a_j = 1$), and if for all $i = 1, 2, \ldots, s$, $i \neq j$, there exists a PBD$(g_i + f, K)$ that contains a flat of order f, then there exists a PBD$((\sum_{i=1}^{s} a_i g_i) + f, K \cup \{g_j + f\})$.

2.4 Remark Theorems 2.1 and 2.3 are examples of constructions known as "filling in holes." The groups are considered as "holes" to be replaced by other objects. They require group divisible designs. The most important recursive construction for group divisible designs is Wilson's Fundamental Construction.

2.5 Theorem (*Wilson's Fundamental Construction* [2145]) Let $(V, \mathcal{G}, \mathcal{B})$ be a GDD (the *master* GDD) with groups $G_1, G_2 \ldots G_t$. Suppose there exists a function $w : V \to \mathbb{Z}^+ \cup \{0\}$ (*a weight function*) so that for each block $B = \{x_1, x_2, \ldots, x_k\} \in \mathcal{B}$ there exists a K-GDD of type $[w(x_1), w(x_2) \ldots, w(x_k)]$ (such a GDD is an *ingredient* GDD). Then there exists a K-GDD of type

$$\left[\sum_{x\in G_1} w(x), \sum_{x\in G_2} w(x), \ldots, \sum_{x\in G_t} w(x)\right].$$

2.6 Remark If the master GDD has index λ_1 and all the ingredient GDDs have index λ_2, then the constructed GDD has index $\lambda_1\lambda_2$.

2.7 Examples Wilson's Fundamental Construction for BIBDs.

1. As master GDD, start with a TD$(5, 4)$, and remove 1 or 2 points from a group to obtain a $\{4, 5\}$-GDD of type 4^4x^1 for $x \in \{2, 3\}$. Give every point weight 3, using $\{4\}$-GDDs of types 3^4 and 3^5 as ingredient GDDs. The result is a $\{4\}$-GDD of type $12^4(3x)^1$. Now duplicate each block and fill the holes with (13,4,2) and $(3x + 1,4,2)$ designs to produce both a (55,4,2) and a (58,4,2) design.
2. The master GDD is a (16,6,2) design, which is a $(\{6\}, 2)$-GDD of type 1^{16}. Give weight 5 to each point, using a $\{6\}$-GDD of type 5^6 (a TD$(6, 5)$ as the ingredient, to form a $(\{6\}, 2)$-GDD of type 5^{16}. Fill the holes using a (6,6,2) design to produce an (81,6,2) design.
3. The master GDD is an (11,6,3) design. Proceed as above, filling with (6,6,3) designs, to produce a (56,6,3) design.

2.8 Remarks The block sizes of the master GDD do not necessarily occur among the block sizes of the constructed GDD. Most recursive constructions for pairwise balanced designs employ some application or variant of Theorem 2.5, often in imaginative ways.

2.9 Examples Wilson's Fundamental Construction for BIBDs.

1. Use a (41,5,1) design as the master design, and a $\{5\}$-GDD of type 4^5 as the ingredient GDD to produce a $\{5\}$-GDD of type 4^{41}. Fill the holes using one additional point, and a (5,5,1) design to get a (165,5,1) design.
2. Start with TD$(5, 9)$ and delete four points from a group to get a $\{4, 5\}$-GDD of type 9^45^1. Use weight three on each point and ingredient $\{4\}$-GDDs of types 4^4 and 4^5 to get a $\{4\}$-GDD of type 27^415^1. Fill the holes using (28,4,1) and (16,4,1) designs to get a (124,4,1) design.

2.10 Remark In order to apply Wilson's Fundamental Construction, group divisible designs are required as both master designs and ingredients. Theorems 2.11, 2.12, 2.13, and 2.14 are used to construct group divisible designs. Often the results are treated as pairwise balanced designs.

2.11 Theorem If there exists a BIBD$(v, k, 1)$, then there exists a k-GDD of type $(k - 1)^r$, where $r = (v - 1)/(k - 1)$.

2.12 Theorem Suppose that there exists a BIBD$(v, k, 1)$ that contains u mutually disjoint parallel classes. Then there exists a $\{k, k + 1\}$-GDD of type k^nw^1 for $0 \le w \le u - 1$, where $n = v/k$. Further if $u = (v-1)/(k-1)$ (that is, if the BIBD$(v, k, 1)$ is resolvable), then there exists a $(k + 1)$-GDD of type $k^n(u - 1)^1$.

2.13 Theorem (*The grouplet construction* [19]) Suppose $(\mathcal{V}, \mathcal{B}\cup\mathcal{G})$ is a PBD$(v, \{B\cup G\}, \lambda)$, $\mathcal{G}$ forms a λ-resolution set (§IV.5.1), and $u, n \ge 1$, $w \ge 0$. If there is a (k, μ)-GDD of type $(un)^b$ for every $b \in B$, and there is a (k, μ)-GDD of type $u^{ng}w^1$ for every $g \in G$, then there is a $(k, \lambda\mu)$-GDD of type $u^{nv}w^1$.

2.2 PBDs Obtained by Truncation of TDs

2.14 Theorem (*truncation of groups of a transversal design* [1042]) Let k be an integer, $k \geq 2$. Let $K = \{k, k+1, \ldots, k+s\}$. Suppose that there exists a TD$(k+s, m)$. Let $g_1, g_2, \ldots, g_s$ be integers satisfying $0 \leq g_i \leq m$, $i = 1, 2, \ldots, s$. Then there exists a K-GDD of type $m^k g_1 g_2 \ldots g_s$.

2.15 Remark The GDD in Theorem 2.14 is obtained by deleting points from a transversal design. Because of this, it is possible to see how the blocks of the GDD relate to its groups, a necessary requirement for the application of Wilson's Fundamental Construction. An example of a typical application is given in Example 2.16.

2.16 Example An application of Wilson's Fundamental Construction. There are $\{3,4\}$-GDDs of type 3^5 and $3^5 5^1$; these are to be used as ingredient GDDs. Suppose that there exists a TD$(6, m)$. Let its groups be $G_1, G_2, \ldots, G_6$. Let t be an integer satisfying $0 \leq t \leq m$, and delete all but t points from group G_6 to obtain a master $\{5,6\}$-GDD of type $5^m t^1$. Now assign a weight of 5 to each point of the group of size t obtained from G_6, and assign a weight of 3 to all other points of the master GDD. Let $B = \{x_1, x_2, \ldots, x_5\}$ be a block of size 5 of the master GDD. It meets only the groups $G_1, G_2, \ldots G_5$. So the corresponding list of weights on the points of B is $[3,3,3,3,3]$, and there is an ingredient $\{3,4\}$-GDD of this type. Similarly, a block of size 6 of the master GDD meets all groups and, therefore, has a list of weights $[3,3,3,3,3,5]$, and again there is an ingredient $\{3,4\}$-GDD of this type. Thus, the conditions required to apply Wilson's Fundamental Construction are satisfied. It yields a $\{3,4\}$-GDD of type $(3m)^5(5t)^1$ in this case.

2.17 Theorem (*spike construction*) Let k be an integer, $k \geq 2$. Let $K = \{k, k+1, \ldots, k+s+1\}$. Suppose there exists a TD$(k+s+n, m)$ where n is a nonnegative integer. Let $g_1, g_2, \ldots, g_s$ be integers satisfying $1 \leq g_i \leq m$, $i = 1, 2, \ldots, s$. Then there exists a $K \cup \{k+s+n\}$-GDD of type $m^k g_1 g_2 \ldots g_s 1^n$.

2.18 Remarks Theorem 2.17 is similar to Theorem 2.14, except that certain points on a particular block are not deleted, resulting in the name "spike." Some of these points remain as groups of size one. Theorem 2.17 is usually applied with $s = 0$ or 1. For $s = 1$, this yields the statement: If there exists a TD$(k+1+n, m)$ where n is a nonnegative integer and if g satisfies $1 \leq g \leq m$, then there exists a $\{k, k+1, k+2, k+n+1\}$-GDD of type $m^k g^1 1^n$. For $s = 0$, if there exists a TD$(k+n, m)$, then there exists a $\{k, k+1, k+n\}$-GDD of type $m^k 1^n$.

2.19 Example The spike construction for $s = 1$. There exists a TD$(8, 9)$. Take $k = 6$. Then there exist $\{6,7,8\}$-GDDs of type $9^6 g^1 1^1$ for $1 \leq g \leq 9$.

2.20 Theorem [959] Let k be an integer, $k \geq 3$, and let $K = \{k-1, k, k+1, \ldots, k+s+1\}$. Suppose that there exists a TD$(k+s+n, m)$, where n is a positive integer. Let $g_1, g_2, \ldots, g_s$ be integers satisfying $0 \leq g_i \leq m-1$, $i = 1, 2, \ldots, s$. Then there exists a K-GDD of type $(m-1)^k g_1^1 g_2^1 \cdots g_s^1 n^1$.

2.21 Remark Theorem 2.20 is usually applied in the case $s = 0$. In this case the result states that there exists a $\{k-1, k, k+1\}$-GDD of type $(m-1)^k n^1$. Further if $k+n = m+1$, then there exists a $\{k-1, k+1\}$-GDD of type $(m-1)^k n^1$.

2.22 Theorem [959] Suppose that there exists a TD(m, m). Let k be an integer satisfying $1 \leq k \leq m-1$. Then there exists an $\{m-1, k-1, k+1\}$-GDD of type $k^{m-1}(m-k)^1$.

2.23 Theorem [959] Let k be a positive integer and let s be an integer satisfying $0 \leq s \leq k-1$. Suppose that there exists a TD$(k+n, m)$. Then there exists a $\{k-1, k, k+1, m-1, m\}$-GDD of type $k^{m-1}(n+s)^1$.

2.24 Example Application of Theorem 2.20 with $n+k=m+1$, and $s=0$. Type is the group type $(m-1)^k(m-k+1)^1$.

k	m	$\{k-1,k+1\}$	Type
5	5	$\{4,6\}$	$4^5 1^1$
	7		$6^5 3^1$
	8		$7^5 4^1$
	9		$8^5 5^1$
	11		$10^5 7^1$
6	7	$\{5,7\}$	$6^6 2^1$
	8		$7^6 3^1$
	9		$8^6 4^1$
	11		$10^6 6^1$

k	m	$\{k-1,k+1\}$	Type
7	7	$\{6,8\}$	$6^7 1^1$
	8		$7^7 2^1$
	9		$8^7 3^1$
	11		$10^7 5^1$
8	8	$\{7,9\}$	$7^8 1^1$
	9		$8^8 2^1$
	11		$10^8 4^1$
9	9	$\{8,10\}$	$8^9 1^1$
	11		$10^9 3^1$

2.25 Example Application of Theorem 2.22.

k	m	$\{m-1,k-1,k+1\}$	Group Types $k^{m-1}(m-k)^1$
5	7	$\{6,4,6\}$	$5^6 2^1$
	8	$\{7,4,6\}$	$5^7 3^1$
	9	$\{8,4,6\}$	$5^8 4^1$
	11	$\{10,4,6\}$	$5^{10} 6^1$
6	7	$\{6,5,7\}$	$6^6 1^1$
	8	$\{7,5,7\}$	$6^7 2^1$
	9	$\{8,5,7\}$	$6^8 3^1$
	11	$\{10,5,7\}$	$6^{10} 5^1$
7	8	$\{7,6,8\}$	$7^7 1^1$
	9	$\{8,6,8\}$	$7^8 2^1$
	11	$\{10,6,8\}$	$7^{10} 4^1$
8	9	$\{8,7,9\}$	$8^8 1^1$
	11	$\{10,7,9\}$	$8^{10} 3^1$

2.3 Constructions from Projective Planes and Geometries

2.26 Let A be a set of nonnegative integers, and let D be a PBD. Then a $\{w;A\}$ *arc*, (or A-arc of order w) in a PBD(v,K), say D, is a set of w points $\mathcal{S}$ of D such that if B is a block, then $|B\cap\mathcal{S}|\in A$.

2.27 Remarks Many PBDs and GDDs can be obtained by deleting judiciously chosen sets of points from other PBDs. Most frequently these are sets of points in projective or affine spaces (see §VII.2). Where the results are obtained from deletion of points from desarguesian geometries, the results are stated in terms of q for q a prime or prime power.

Suppose that a projective plane of order n contains a $\{w;A\}$ arc. Then it also contains a complementary $\{n^2+n+1-w;n+1-A\}$ arc, where $n+1-A=\{n+1-a:a\in A\}$.

2.28 Example Let π be PG$(2,n)$ where $n=2^k$. Then π contains a set $\mathcal{A}$ of $n+2$ points, no two collinear (an oval or hyperoval). $\mathcal{A}$ is a $\{0,2\}$-arc of order $n+2$ in π.

2.29 Example Let π be PG$(2,q)$ where q is odd. Then π contains a set $\mathcal{A}$ on $n+1$ points, no two collinear (an oval or conic). $\mathcal{A}$ is a $\{0,1,2\}$-arc of order $n+1$ in π.

2.30 Remark Let A be a set of positive integers, and let k be a positive integer. As in the case of PBDs, $\{w,A\cup k^\star\}$ arc is used to designate the case of an arc that has

the property that at least one block of the PBD meets the arc in exactly k points. If $k \notin A$, then there is exactly one block with this property. In the case in which the set is displayed explicitly, if the displayed set contains entries k and $k^\star$, this indicates that at least one block meets the arc in exactly k points. If the symbol $k^\star$ appears without k, there is exactly one such block.

2.31 **Theorem** [959] Let q be an odd prime power. Then

1. there exists a $\{(q+1)/2, (q-1)/2\}$-GDD of type $((q-1)/2)^q$,
2. there exists a $\{(q+1)/2, (q+3)/2\}$-GDD of type $((q+1)/2)^q$.

2.32 **Theorem** (*subfield subplanes*) Let q be a prime power. Let a and b be positive integers such that b divides a. Then $\mathrm{PG}(2, q^a)$ contains a subplane $\mathrm{PG}(2, q^b)$. (If $a = 2b$, then the subplane is a *Baer subplane*; see §VII.2.5).

2.33 **Remarks** Subfield subplanes give rise to $\{q^{2b} + q^b + 1; \{0, 1, q^b + 1\}\}$ arcs in $\mathrm{PG}(2, q^a)$ when $b \mid a$. When $a = 2b$, the arc has no lines of size zero. These Baer subplanes are the source of several constructions, including Theorems 2.34 and 2.35.

2.34 **Theorem** (Wallis, see [2105]) If q is a prime power, then there exists a q-GDD of type $(q^2 - q)^{q+1}$ that is both a frame and an RGDD. Completing the RGDD gives a $(q+1)$-GDD of type $(q^2 - q)^{q+1}(q^2)^1$.

2.35 **Theorem** (*Brouwer construction* [336]) Let q be a prime power, and let t be an integer satisfying $0 < t < q^2 - q + 1$. Then there exists a $\{t, q+t\}$-GDD of type t^{q^2+q+1}; that is, there exists a $\mathrm{PBD}(t(q^2 + q + 1), \{t, t + q\})$.

2.36 **Remark** In the PBD constructed in Theorem 2.35, the blocks of size t can be partitioned into $q^2 - q + 1 - t$ parallel classes. By adjoining new points to these classes, Theorem 2.35 extends to Theorem 2.37.

2.37 **Theorem** (*extended Brouwer construction* [336]) Let q be a prime power, and t be an integer satisfying $0 < t < q^2 - q + 1$. If u is an integer satisfying $0 \le u \le q^2 - q - t$, then there exists a $\{t, t+1, q+t\}$-GDD of type $t^{q^2+q+1}\ u^1$. Therefore, for $0 \le u \le q^2 - q + 1 - t$, there exists an incomplete PBD of order $t(q^2 + q + 1) + u$ and blocks from the set $\{t, t+1, t+q\}$ having a hole of size u. If $u = q^2 - q + 1 - t$, then no block of size t occurs in the incomplete PBD. If $u = q^2 - q - t$, then no block of size t occurs in the GDD.

2.38 **Corollary** If q is a prime power, then there exists a $\{q^2, q^2 - q\}$-GDD of type $(q^2 - q)^{q^2+q+1}$. This corresponds to the case of $t = q^2 - q$ (and $u = 0$) in Theorem 2.37.

2.39 **Example** Applications of the extended Brouwer construction of a $\{t, t+1, q+t\}$-GDD of type $t^{q^2+q+1}\ u^1$ with $u = q^2 - q - t$.

q	q^2-q	t	q^2-q-t	$\{t+1, q+t\}$	GDD Type
3	6	6	0	$\{7, 9\}$	6^{13}
3	6	5	1	$\{6, 8\}$	$5^{13}1^1$
3	6	4	2	$\{5, 7\}$	$4^{13}2^1$
3	6	3	3	$\{4, 6\}$	$3^{13}3^1$
3	6	2	4	$\{3, 5\}$	$2^{13}4^1$
3	6	1	5	$\{2, 4\}$	$1^{13}5^1$
4	12	12	0	$\{13, 16\}$	12^{21}
4	12	11	1	$\{12, 15\}$	$11^{21}1^1$
4	12	10	2	$\{11, 14\}$	$10^{21}2^1$
4	12	9	3	$\{10, 13\}$	$9^{21}3^1$
4	12	8	4	$\{9, 12\}$	$8^{21}4^1$
4	12	7	5	$\{8, 11\}$	$7^{21}5^1$

q	q^2-q	t	q^2-q-t	$\{t+1, q+t\}$	GDD Type
4	12	6	6	$\{7,10\}$	$6^{21}6^1$
4	12	5	7	$\{6,9\}$	$5^{21}7^1$
4	12	4	8	$\{5,8\}$	$4^{21}8^1$
4	12	3	9	$\{4,7\}$	$3^{21}9^1$
4	12	2	10	$\{3,6\}$	$2^{21}10^1$
4	12	1	11	$\{2,5\}$	$1^{21}11^1$
5	20	20	0	$\{21,25\}$	20^{31}
5	20	19	1	$\{20,24\}$	$19^{31}1^1$
5	20	18	2	$\{19,23\}$	$18^{31}2^1$
5	20	17	3	$\{18,22\}$	$17^{31}3^1$
5	20	16	4	$\{17,21\}$	$16^{31}4^1$
5	20	15	5	$\{16,20\}$	$15^{31}5^1$
5	20	14	6	$\{15,19\}$	$14^{31}6^1$
5	20	13	7	$\{14,18\}$	$13^{31}7^1$
5	20	12	8	$\{13,17\}$	$12^{31}8^1$
5	20	11	9	$\{12,16\}$	$11^{31}9^1$
5	20	10	10	$\{11,15\}$	$10^{31}10^1$
5	20	9	11	$\{10,14\}$	$9^{31}11^1$
5	20	8	12	$\{9,13\}$	$8^{31}12^1$
5	20	7	13	$\{8,12\}$	$7^{31}13^1$
5	20	6	14	$\{7,11\}$	$6^{31}14^1$
5	20	5	15	$\{6,10\}$	$5^{31}15^1$
5	20	4	16	$\{5,9\}$	$4^{31}16^1$
5	20	3	17	$\{4,8\}$	$3^{31}17^1$
5	20	2	18	$\{3,7\}$	$2^{31}18^1$
5	20	1	19	$\{2,6\}$	$1^{31}19^1$

2.40 **Theorem** (*Brouwer's Singer set construction* [336]) Let D be a Singer difference set for a projective plane π of order q (see §VI.18.4). Let $v = q^2+q+1$, and let $S = \{0, 1, \cdots, v-1\}$ be the representatives of $\mathbb{Z}_v$ used to represent and develop the difference set. Let u be a proper divisor of v and write $v = um$. Let $X = \{0, m, 2m, \cdots, v-m\}$, so that $|X| = u$. Then X is a $\{m; A\}$ arc in π for some A, where A contains no more than m distinct integers.

2.41 **Remarks** Theorem 2.40 has been extended by Greig [959] to multiple divisors of v. Theorem 2.42 is a specific application of Theorem 2.40.

2.42 **Theorem** (*Brouwer's 1 mod 3 construction* [336]) Let $q \equiv 1 \pmod 3$ be a prime power. Let $u = (q^2+q+1)/3$. Then there exists a PBD$(u, \{k_0, k_1, k_2\})$ where k_0, k_1, and k_2 are a solution of $k_0 + k_1 + k_2 = q+1$ and $k_0^2 + k_1^2 + k_2^2 = q+u$.

2.43 **Example** PBD$(u, \{k_0, k_1, k_2\})$ via applications of Brouwer's 1 mod 3 construction.

q	7	13	16	19	25	31	37
u	19	61	91	127	217	331	469
$\{k_0, k_1, k_2\}$	$\{1,3,4\}$	$\{3,4,7\}$	$\{3,7,7\}$	$\{4,7,9\}$	$\{7,7,12\}$	$\{7,12,13\}$	$\{9,13,16\}$

2.44 **Remark** The line flip method, in which the points of a block transverse to an arc in a projective plane or other design are replaced by the complementary set, or vice versa, is a powerful technique for creating new PBDs.

2.45 **Theorem** [959] If a projective plane of order q contains a $(v; K \cup k^\star)$ arc, and if t is an integer satisfying $0 \le t \le q+1-k$, then the plane contains a $\{v+t; K \cup (K+1) \cup (k+t)^\star\}$ arc, where $K+1 = \{k+1 : k \in K\}$.

2.46 **Theorem** [959] If a projective plane of order q contains a $\{v; K \cup k^\star\}$ arc, then the plane contains a $\{v+q+1-2k;\ (K-1)\cup(K+1)\cup(q+1-k)^\star\}$ arc, where $K+1=\{k+1 : k\in K\}$, and $K-1=\{k-1 : k\in K, k>0\}$.

2.47 **Theorem** [959] Suppose that a projective plane of order q contains a $\{0,a\}$ arc of order w. Let $s=w/a$. Then

1. (secant line flip) there exists a $\{a-1,a+1\}$-GDD of type $a^{s-1}(q-a)^1$,
2. (external line flip) there exists an $(a+1)$-GDD of type $a^s q^1$.

2.48 **Theorem** (Denniston, see [959]) There exists a $\{0,2^n\}$ arc of order $w=2^{2n+m}-2^{n+m}+2^n$ in $\mathrm{PG}(2,2^{n+m})$. The $\{0,2^n\}$ arc contains a $\{0,2^\ell\}$ Denniston arc for all $\ell\le n$.

2.49 **Corollary** [959] Let m and n be positive integers.

1. There exists a $(2^n-1,2^n+1)$-GDD of type $(2^n)^{2^m(2^n-1)}(2^{m+n}-2^n)^1$.
2. There exists a (2^n+1)-GDD of type $(2^n)^{2^{m+n}-2^m+1}(2^{m+n})^1$.

2.50 **Theorem** (*the $q-x$ construction* [959]) If there is a projective plane of order q, and if x is an integer satisfying $0\le x\le q-1$, then there exists a $\{q-x-1,q-x+1\}$-GDD of type $(q-1)^{q-x}(x+1)^1$.

2.51 **Example** Applications of the $q-x$ construction. $K=\{q-x-1,q-x+1\}$.

q	x	K	Type	q	x	K	Type	q	x	K	Type
7	1	$\{5,7\}$	$6^6 2^1$	7	2	$\{4,6\}$	$6^5 3^1$				
8	1	$\{6,8\}$	$7^7 2^1$	8	2	$\{5,7\}$	$7^6 3^1$	8	3	$\{4,6\}$	$7^5 4^1$
9	1	$\{7,9\}$	$8^8 2^1$	9	2	$\{6,8\}$	$8^7 3^1$	9	3	$\{5,7\}$	$8^6 4^1$
9	4	$\{4,6\}$	$8^5 5^1$								
11	1	$\{9,11\}$	$10^{10} 2^1$	11	2	$\{8,10\}$	$10^9 3^1$	11	3	$\{7,9\}$	$10^8 4^1$
11	4	$\{6,8\}$	$10^7 5^1$	11	5	$\{5,7\}$	$10^6 6^1$	11	6	$\{4,6\}$	$10^5 7^1$
13	1	$\{11,13\}$	$12^{12} 2^1$	13	2	$\{10,12\}$	$12^{11} 3^1$	13	3	$\{9,11\}$	$12^{10} 4^1$
13	4	$\{8,10\}$	$12^9 5^1$	13	5	$\{7,9\}$	$12^8 6^1$	13	6	$\{6,8\}$	$12^7 7^1$
13	7	$\{5,7\}$	$12^6 8^1$	13	8	$\{4,6\}$	$12^5 9^1$				
16	1	$\{14,16\}$	$15^{15} 2^1$	16	2	$\{13,15\}$	$15^{14} 3^1$	16	3	$\{12,14\}$	$15^{13} 4^1$
16	4	$\{11,13\}$	$15^{12} 5^1$	16	5	$\{10,12\}$	$15^{11} 6^1$	16	6	$\{9,11\}$	$15^{10} 7^1$
16	7	$\{8,10\}$	$15^9 8^1$	16	8	$\{7,9\}$	$15^8 9^1$	16	9	$\{6,8\}$	$15^7 10^1$
16	10	$\{5,7\}$	$15^6 11^1$	16	11	$\{4,6\}$	$15^5 12^1$				

2.52 Let p be a prime. Then a *(p,a,b)-Baer configuration* in $\pi=PG(2,p^a)$ is a set X of p^a+p^b+1 points that has the properties that, restricting the lines of π to the points of X,

1. one point of X, the *focus*, lies on $p^{a-b}+1$ lines each of size p^b+1, and
2. the remaining points each lie on one line of size p^b+1 and p^b lines each of size $p^{a-b}+1$.

2.53 **Remark** By removing the focus, a $\mathrm{TD}(p^{a-b}+1,p^b)$ is obtained. This is of itself not remarkable, because p is prime. However the embedding of the configuration into $\mathrm{PG}(2,p^a)$ (and in particular, an associated transversal design) is remarkable. This is partly due to the fact that every line of $\mathrm{PG}(2,p^a)$ meets the Baer configuration in at least one point, so the configuration is a $\{1,p^b+1,p^{a-b}+1\}$ arc in the plane.

2.54 **Theorem** (Ostrom, see [545]) The plane $\mathrm{PG}(2,p^a)$ contains a (p,a,b)-Baer configuration if p is prime and $a-b$ is a divisor of a.

2.55 Let k and x be nonnegative integers, and let $\mathcal{I} = \{i_1, i_2, \ldots, i_s\}$ be a set of integers satisfying $0 \leq i_1 < i_2 < \cdots < i_s \leq x$. Further suppose that there are integers s_i satisfying $0 \leq s_1 \leq s_2 \leq \cdots \leq s_x \leq n$. Let $(\mathcal{X}, \mathcal{G}, B)$ be a TD$(k+x, n)$ with $\mathcal{G} = \{G_1, G_2, \cdots, G_k, H_1, H_2, \cdots, H_x\}$. Then an $(x, \mathcal{I}, s_1, s_2, \ldots, s_x)$-*thwart* is a set $S = \cup_{j=1}^{x} S_j$, where $S_j \subseteq H_j$ with $|S_j| = s_j$ for $1 \leq j \leq x$, such that for every $B \in \mathcal{B}$, $|B \cap S| \in \mathcal{I}$.

2.56 Theorem [545] Let p be a prime, and let a and b be integers satisfying $a \geq b \geq 1$ and $(a-b)|a$. Then there is a TD$(p^a + 1, p^a)$

1. containing a $(p^{a-b}+1, \{1, p^{a-b}+1\}, p^b, \ldots p^b)$-thwart and
2. a $(p^{a-b}+1, \{0, p^{a-b}\}, p^a - p^b, \ldots, p^a - p^b)$-thwart.

(These arise by deleting the focus of the Baer configuration from the plane.)

2.57 Example A PBD(53,{9,8,7,5}) can be obtained from part 1 of Theorem 2.56 as follows: Take $a = 3$, $b = 2$, and $p = 2$ to obtain a TD$(9, 8)$ containing (3, {1,3}, 4,4,4)-thwart. Delete a group that does not meet the thwart to obtain a TD$(8, 8)$ containing a $(3, \{1, 3\}, 4, 4, 4)$-thwart, then delete the points of the thwart to obtain a {8,7,5}-GDD of type $8^5 4^3$. Now adjoin a new point ∞ to the groups of this GDD to obtain the PBD(53,{9,8,7,5}).

2.58 Example An application of thwarts employing Wilson's Fundamental Construction. Let D be the TD$(9, 8)$ containing a (3,{1,3},4,4,4)-thwart, and let S denote the points of the thwart. Let the groups of D be $G_i, i = 1, 2, \ldots, 9$, and let $G_1, G_2, \ldots, G_6$ be the groups that do not meet S. Let $G_i = N_i \cup T_i$, $i = 7, 8, 9$ where $T_i = G_i \cap S$, so $|T_i| = 4, i = 7, 8, 9$. For ingredient GDDs, by the table of 4-GDDs, there exist 4-GDDs of type $3^8 0^1$ and 3^9. There exists a resolvable BIBD (15,3,1) and BIBD (21,3,1), respectively. By completing the former by adjoining 7 new points, then deleting one of the old points, a $\{4, 7\}$-GDD of type $3^7 0^2$ is obtained, whereas by adjoining 9 new points to the latter, a 4-GDD of type $3^7 9^1 0^1$ is obtained. Further by deleting a point from a TD$(4, 7)$, a $\{4, 7\}$-GDD of type $3^7 6^1 0^1$ is obtained, and by adjoining a new point to the groups of a TD$(4, 7)$ then deleting another point, a $\{4, 8\}$-GDD of type $3^7 7^1 0^1$ is obtained.

Now assign weights to the points of D as follows: To each point in G_i, $i = 1, 2, \ldots, 6$, assign a weight of 3. To each point of $N_i, i = 7, 8$, also assign a weight of 3 and assign a weight of 0 to each point $T_i, i = 7, 8$. To each point of T_9 also assign a weight of 3. Let x_1, x_2, x_3, and x_4 be nonnegative integers. To x_1, x_2, x_3, and x_4 points of N_9, assign weights of 0, 3, 7, and 9, respectively.

A block of D is a *tangent* if it meets the thwart in one point, and a *transversal* if it meets the thwart in three points. Each transversal has 2 points of weight 0 and 7 points of weight 3, (that is, it has type $3^7 0^2$). If the block is a tangent meeting T_9 it is of type 3^9, otherwise it is of type $3^7 w^1 0^1$, where w is the weight of the point in which it meets N_9, that is, $w \in \{0, 6, 7, 9\}$. Because there is a {4,7,8}-GDD of each of these types, one can apply Wilson's Fundamental Construction to obtain a {4,7,8}-GDD of type $24^6 12^2 (12 + 6x_2 + 7x_3 + 9x_4)$ where $0 \leq x_2 + x_3 + x_4 \leq 4$. Because there exists a BIBD$(v, 4, 1)$ for $v \equiv 1, 4 \pmod{12}$, there exists a PBD$(v + f, \{4\})$ with a flat of order f, for $v \in \{12, 24\}$ and $f \in \{1, 4\}$. Thus, by applying the generalized singular product, one obtains PBD$(180 + 6x_2 + 7x_3 + 9x_4 + f, \{4, 7, 8, (12 + 6x_2 + 7x_3 + 9x_4 + f)^\star\})$ for any collection of x_2, x_3, x_4 satisfying $0 \leq x_2 + x_3 + x_4 \leq 4$ and $f \in \{1, 4\}$. If, in addition, $w = 12 + 6_2 + 7x_3 + 9x_4 + f$, and if there exists a PBD$(w, \{4, 7, 8\})$, then there exists a PBD$(168 + w, \{4, 7, 8\})$.

2.59 Remark A (p, a, b)-Baer configuration induces an arc in the dual plane. The corresponding PBD is noted in Theorem 2.60.

2.60 **Theorem** [545] Let p be a prime, and let a and b be integers satisfying $a \geq b \geq 1$ and $(a-b)|a$. Then PG$(2, p^a)$ contains a $\{p^a, p^a - p^{2b-a}+1\}$-GDD of type $(p^a - p^b)^{p^a+p^b}$ $(p^a - p^{a-b})^1$.

2.61 **Remark** Interesting thwarts also arise from other structures in planes such as ovals, hyperovals, and Denniston arcs. See [545, 548]. The idea of a thwart extends naturally to configurations of GDDs.

2.4 Constructions Involving Incomplete Objects

2.62 **Theorem** [1026] Let K and L be sets of positive integers and let there exist an L-IGDD of type $(g_1, h_1)^{a_1}(g_2, h_2)^{a_2} \ldots (g_s, h_s)^{a_s}$. For some positive integer n and for each $\ell \in L$, suppose that there exists a K-GDD of type n^ℓ. Then there exists a K-IGDD of type $(ng_1, nh_1)^{a_1}(ng_2, nh_2)^{a_2} \ldots (ng_s, nh_s)^{a_s}$.

2.63 **Theorem** [1026] Let $(V, \mathcal{G}, \mathcal{B})$ be a GDD (the *master* GDD) with groups $G_1, G_2 \ldots G_t$. Suppose there exists a function biweight $w = (w_1, w_2)$ with $w_i : V \to \mathbb{Z}^+ \cup \{0\}$ and $w_1(x) \geq w_2(x)$. If, for each block $B = \{x_1, x_2, \ldots, x_k\} \in \mathcal{B}$, there exists an ingredient K-IGDD of type $[(w_1(x_1), w_2(x_1)), (w_1(x_2), w_2(x_2)), \ldots, (w_1(x_k), w_2(x_k))]$, then there exists a K-IGDD of type $\left[\sum_{x\in G_1}(w_1(x), w_2(x)),\ \sum_{x\in G_2}(w_1(x), w_2(x)),\ \ldots,\ \sum_{x\in G_t}(w_1(x), w_2(x))\right]$.

2.64 **Remarks** Theorem 2.62 can be generalized to use arbitrary weights on the master IGDD. However the form given appears to be the most useful. Theorems 2.65 and 2.66 are further examples of "filling in holes." When the K-IGDD is an ITD, Theorem 2.62 is the *singular indirect product* construction. A host of variations is possible.

2.65 **Theorem** [1962] Let K be a set of positive integers and suppose that there exists a K-IGDD of type $(g_1, h_1)^{a_1}(g_2, h_2)^{a_2} \ldots (g_s, h_s)^{a_s}$. Let q be a positive integer. Suppose that for $i = 1, 2, \ldots, s$, there exists a K-IPBD of order $g_i + q$ with a hole of $h_i + q$. Then there exists a K-IPBD of order $v = (\sum_{i=1}^s a_i g_i) + q$ with a hole of order $h = (\sum_{i=1}^s a_i h_i) + q$, that is, a PBD$(v, K \cup \{h^\star\})$.

2.66 **Theorem** (*Stinson's diamond construction*) [2211] Let K be a set of positive integers. Let a and b be integers satisfying $b \geq a \geq 0$. Suppose that there exist

1. a K-IGDD of type $(t_1, u_1)(t_2, u_2), \ldots, (t_n, u_n)$,
2. a $(t_i + b; u_i + a, b; a; K) - \diamondsuit$-IPBD for $1 \leq i \leq n-1$; (§IV.1.3), and
3. a $(t_n + b, u_n + a; K)$-IPBD.

Then there exists a $(t + b, u + a; K)$-IPBD, where $t = \sum_{i=1}^n t_i$ and $u = \sum_{i=1}^n u_i$.

2.5 Designs with Higher Index

2.67 **Remarks**

1. A PBD$(v, K; \lambda_1\lambda_2)$ ($(v, h; K, \lambda_1\lambda_2)$-IPBD) is obtained from a PBD$(v, K; \lambda_1)$ ($(v, h; K, \lambda_1)$-IPBD, respectively) by replicating the blocks of the design λ_2 times.
2. A $(K, \lambda_1\lambda_2)$-GDD (or $(K, \lambda_1\lambda_2)$-IGDD) of type T is obtained from a (K, λ_1)-GDD (or (K, λ_1)-IGDD) by replicating its blocks λ_2 times.
3. In view of this, a rich source of PBDs, IPBDs, GDDs, and IGDDs of index $\lambda > 1$ is the class of equivalent objects of index 1.
4. GDDs and IGDDs of higher index are frequently obtained from transversal designs and incomplete transversal designs of general index. See §III.6.

5. The notion of filling in holes applies to GDDs and IGDDs of higher index. For example, the following BIBDs can be obtained:

GDD:	Fill the Hole with:	Resulting BIBD:
$TD_2(5,11)$	(11,5,2) design	(55,5,2) design
$TD_3(4,9)$	(9,4,3) design	(36,4,3) design
$TD_2(10,10)$	(10,10,2) design	(100,10,2) design
$TD_2(12,12)$	(12,12,2) design	(144,12,2) design
$TD_3(10,10)$	(10,10,3) design	(100,10,3) design
$TD_3(11,10)$	(11,11,3) design	(111,11,3) design
$TD_2(18,18)$	(18,18,2) design	(324,18,2) design
$TD_3(12,12)$	(12,12,3) design	(144,12,3) design
$TD_3(13,12)$	(13,13,3) design	(157,13,3) design

2.68 Remarks When $\lambda > 1$, there are opportunities for new constructions that are unavailable when $\lambda = 1$. Examples 2.69 and 2.70 give some instances used in establishing BIBD existence results for $k \in \{7, 8\}$ (see [19, 42, 1042, 1044, 2182, 2194]).

2.69 Examples Many standard direct constructions offer structure that can sometimes be exploited. If $q = (k-1)t + 1$ is a prime power, then there is a BIBD(q, k, k) given by a difference family over $\mathbb{F}_q$ consisting of the cosets of $(k-1)$st roots plus zero. Naturally, this design is k-resolvable, so completing the resolution sets by adding an infinite point to each base block gives a $(q+t, t; k+1, 1)$-IPBD. If $t > 1$, this gives a TD$(k+2, q)$, where one can truncate one group to size s, then use the trivial $(k+1, k)$-GDDs of types 1^{k+1} and 1^{k+2} as ingredients to get a $(k+1, k)$-GDD of type $q^{k+1}s^1$. Then one may fill the groups using the IPBD with t extra points to get a $(k+1, k)$-GDD of type $1^{(k+1)q}(s+t)^1$. Hence, if a BIBD$(s+t, k+1, k)$ exists, then so does a BIBD$((k+1)q + s + t, k+1, k)$.

Hanani [1042, 1044] gives difference families for $(7, \lambda)$-GDDs of type 7^q over $\mathbb{Z}_7 \times \mathbb{F}_q$. Let $B_0 = ((0,0), (1,a), (1,-a), (2,b), (2,-b), (4,c), (4,-c))$ (where the second elements of these 7 points are distinct), then the difference families have the form $B_i = (1, m^i) * B_0$ for $i = 0, 1, \ldots, (q-1)\lambda/6 - 1$. If q is odd, then suitable values of a, b, c, m can always be found for $\lambda = 3$ and 6; if $q \equiv 1 \pmod{12}$, then suitable values can usually be found for $\lambda = 1$ or 2. The same pure and mixed differences found in B_i are also found in $(-1, 1) * B_i$, so if B_i is replaced by $(-1, 1) * B_i$ when i is odd, one also gets a difference family. Now look at a pair of consecutive base blocks in this new family: developing the pair over $\mathbb{F}_q$ gives a 2-resolution set, which is then later developed over $\mathbb{Z}_7$. A 2-resolvable design results when the number of base blocks is even, so if one has a difference family with $\lambda = 2$, then there is also a family of $(\{7, 8\}, 2)$-GDDs of type $7^q s^1$.

If the point $(0,0)$ is replaced by the two points $(0,1)$ and $(0,-1)$ in B_0 above, (where the second elements of these 8 points in B_0 are distinct), then the difference family $B_i = (1, x^i) * B_0$ for $i = 0, 1, \ldots, (q-3)/2$ with x a primitive element of $\mathbb{F}_q$ gives an $(8, 4)$ GDD of type 7^q when q is an odd prime power. Because $x^i * \{a, -a\} = \mathbb{F}_q \setminus \{0\}$, developing these base blocks over $\mathbb{Z}_7$ gives a holey 4-resolution set missing the group $\mathbb{Z}_7 \times \{0\}$. Similarly, taking a and b as squares and c and d as nonsquares, developing the set $\{B_i : i \text{ odd}\}$ over $\mathbb{Z}_7$ gives a holey 2-resolution set when $q \equiv 1 \pmod 4$, so in fact there are some $(8, \alpha; 4)$-frames of type 7^q, which in turn yield α-resolvable BIBD$(7q+1, 8, 4)$s.

2.70 Examples Contracting t old points in the same group onto 1 new point in that group provides a way of generating new designs from old. If this is done for two groups in a (k, λ) GDD, the new points from different groups occur together λt^2 times. However,

if the GDD is given by a difference family over G, and the contraction is of a normal subgroup of G, then the index increases only to λt.

Using Bose's construction [302], one can take $\mathbb{F}_{7^2}$ as an extension of $\mathbb{F}_7$, set $u = 1$ and compute $D = \{\log(a\mu + 1) : a \in \mathbb{F}_7\}$, where μ is a root of the primitive equation $\mu^2 = 6\mu + 4$, to get $D = (0, 31, 28, 22, 43, 18, 29)$. Then D generates a 7-GDD of type 6^8 over $\mathbb{Z}_{48}$, which is also a frame. Reduction modulo 24 gives $D_1 = (0, 7, 4, 22, 19, 18, 5)$ which generates a $(7, 2)$-GDD of type 3^8 over $\mathbb{Z}_{24}$. Reduction modulo 16 gives $D_2 = (0, 15, 12, 6, 11, 2, 13)$ which generates a $(7, 3)$-GDD of type 2^8 over $\mathbb{Z}_{16}$. Here, both the new GDDs are also frames, but contraction does not necessarily preserve holey resolution sets in general; that depends on how these sets are structured over the blocks of the original design.

Sometimes one doesn't want to contract all groups: remove a block of PG$(2, 7)$ to get an 8-GDD of type $1^{49}8^1$ and then truncate the 8-group to get a $\{7, 8\}$-GDD of type $1^{49}3^1$. Next, give all points weight 6 in Wilson's fundamental construction and use a 7-GDD of type 6^8 or $(7, 2)$-GDDs of types 6^7 and 6^8 as ingredients to get a 7-GDD of type $6^{49}48^1$ and a $(7, 2)$-GDD of type $6^{49}18^1$. Now, contract 30 points of the 48-group in the first design onto 10 new points. Adjoining these two designs gives a $(7, 3)$-GDD of type $6^{49}28^1$. The groups can then be filled with $(v, 7, 3)$ BIBDs for $v = 7, 29$ using an extra point to get a BIBD$(323, 7, 3)$.

2.71 **Examples** Points can be contracted to form IPBDs, which are useful in pair-packing and pair-covering problems [1615]. Using 5-GDDs of types $1^{20t}m^1$ for $m = 1$, 5 and 13, one can combine two of these GDDs and contract the extra points in the larger design to get a $(5, 2)$ GDD of type $1^{20t}n^1$ for $n = 3$ when $t \geq 1$ and $n = 7$ and 9 when $t \geq 2$. These GDDs are $(20t + n, n; \{5\}, 2)$-IPBDs.

Although $(v, k; \{k\}, \lambda)$-IPBDs often arise from filling in the groups of (k, λ)-GDDs, other direct constructions for $k > 6$ seem rare. The only known examples are $(v, 7; \{7\}, 2)$-IPBDs for $v = 64$ and 106, and a $(57, 7; \{7\}, 3)$-IPBD [42].

2.72 **Theorem** Let N be the v by b incidence matrix of a balanced n-ary design (see VI.2) (so its entries are in the range 0 through $n-1$ and the blocks of the design are multisets). Assume that $NJ = rJ$, $JN = kJ$, and $NN^T = cI + \lambda J$ (this last condition is slightly weaker than, but implied by, requiring a constant replication pattern over the points). If $v\lambda = r(k-1)$ and q is a prime power with $q \geq k$, then a (k, λ)-GDD of type v^q exists.

2.73 **Remark** In Theorem 2.72, if the initial design is a ternary design, and every block containing a doubleton element contains at most one singleton element, and if all pure singleton blocks occur in identical pairs, then the index of the constructed GDD may be halved if q is odd.

2.74 **Remark** In Theorem 2.72, if the initial design is a ternary design, and every block is either pure doubleton or pure singleton, and the singleton blocks occur in identical pairs, and there is a 2-parallelism of the doubleton blocks, and there is a parallelism of the singleton blocks, then this ternary design is equivalent to an example of Baker's uniform base factorization UBF$_{\lambda/2}(k, v)$ with the singleton blocks repeated [144].

See Also

§II.1	BIBDs are PBDs with one block size.
§III.3	TDs are special classes of GDDs.
§III.4	ITDs are special classes of IGDDs.

References Cited: [19, 42, 144, 302, 336, 545, 548, 959, 1026, 1042, 1044, 1615, 1962, 2105, 2145, 2182, 2194, 2211]

3 PBD-Closure

R. Julian R. Abel
Frank E. Bennett
Malcolm Greig

3.1 Necessary Conditions

3.1 **Theorem** (Drake and Larson [749]) Let K be a set of positive integers and let m denote the smallest integer in K. Suppose that there exists a PBD(v, K) that contains blocks B_h and B_k of sizes h and k, respectively. Then

1. $v \geq (m-1)k + h - m + 1$; hence
2. $v \geq (m-1)k+1$, with equality if and only if there exists a resolvable BIBD$(k(m-2)+1, m-1, 1)$; and
3. if B_h and B_k do not intersect, then $v \geq (m-1)k + h$.

3.2 A set S of positive integers is *PBD-closed* if the existence of a PBD(v, S) implies that v belongs to S.

3.3 Let K be a set of positive integers and let $B(K) = \{v : \exists \text{PBD}(v, K)\}$. Then $B(K)$ is the PBD-*closure* of K. If $K = \{k\}$, the notation $B(k)$ is used.

3.4 Let K be a set of positive integers. Define $\alpha(K) = \gcd\{k-1 : k \in K\}$ and $\beta(K) = \gcd\{k(k-1) : k \in K\}$.

3.5 **Lemma** [2146] Necessary conditions for the existence of a PBD(v, K) are

$$v - 1 \equiv 0 \pmod{\alpha(K)}, \qquad \text{and} \qquad v(v-1) \equiv 0 \pmod{\beta(K)}.$$

3.6 **Theorem** [2146] The necessary conditions for the existence of a PBD(v, K) are asymptotically sufficient. More precisely, let K be a PBD-closed set. Then there exists a constant $v_0 = v_0(K)$ such that if $v > v_0$ and v satisfies the necessary conditions of Lemma 3.5, then there exists a PBD(v, K).

3.7 **Theorem** [2151] The necessary conditions for the existence of a PBD(v, K, λ), that $\lambda(v-1) \equiv 0 \pmod{\alpha(K)}$ and $\lambda v(v-1) \equiv 0 \pmod{\beta(K)}$, are asymptotically sufficient.

3.2 Closures

3.8 **Theorem** [2151] The asymptotic sufficiency of the necessary conditions for the existence of PBD(v, K) can be restated in terms of PBD-closed sets as follows. Let K be a PBD-closed set. Then K is *eventually periodic* with period $\beta(K)$; that is, there exists a constant $C(K)$ such that for every $k \in K$, (including $k = 1$) $\{v : v \geq C(K), v \equiv k \pmod{\beta(K)}\} \subseteq K$.

3.9 **Remark** Theorem 3.8 makes the theory of PBD-closure useful. A few examples of a certain set of objects can prove sufficient to establish the existence of an entire set of objects, as is illustrated in Example 3.10.

3.10 **Example** By breaking up blocks, the set $S = \{v : \exists \text{ a BIBD}(v, 4, 2)\}$ is PBD-closed. A necessary condition for the existence of a BIBD$(v, 4, 2)$ is $v \equiv 1 \pmod 3$. A

BIBD(4,4,2) can be obtained by taking the block {1,2,3,4} twice. (It is degenerate because $v = k$, but it is sufficient here.) A BIBD(7,4,2) is obtained by developing the set $\{0, 1, 2, 4\}$ modulo 7. Now $\gcd(7 \cdot 6, 4 \cdot 3) = 6$, so $\beta(S)|6$. Also $\{4, 7\} \subset S$. Therefore, S is eventually periodic, with period 3; so for sufficiently large $v \equiv 1 \pmod 3$, there exists a BIBD$(v, 4, 2)$, simply by the closure theorem. However, $B(\{4, 7\}) = \{v : v \equiv 1 \pmod 3, v \neq 10, 19\}$, so there exists a BIBD$(v, 4, 2)$ for all positive $v \equiv 1 \pmod 3$ with the possible exception of $v = 10$ or $v = 19$. (It is for this reason that the study of closures is important.) Because there exists a BIBD$(v, 4, 2)$ for $v = 10$ and $v = 19$, $S = \{v : v \equiv 1 \pmod 3\}$.

3.11 **Theorem** [2146] The primitive (or minimal) eventual period of a PBD-closed set is either $\beta(K)$ or $\frac{1}{2}\beta(K)$, and the latter is possible only if $\beta(K) \equiv 2 \pmod 4$.

3.12 **Remark** Every PBD-closed set $K \neq \{1\}$ is infinite.

3.13 **Examples** Examples of PBD-closed sets.

- $B(k, \lambda) = \{v : \exists$ a BIBD$(v, k, \lambda)\}$.
- $R(k) = \{r : \exists$ a BIBD$(v, k, 1)$ with replication number $r\}$.
- $R^*(k) = \{r : \exists$ a resolvable BIBD$(v, k, 1)$ with replication number $r\}$.
- $U(K, u) = \{t : \exists$ a K-GDD of type $u^t\}$, where K is a set of positive integers, and u is a fixed integer such that there exists a K-GDD of type u^k for all $k \in K$.
- $S = \{s : \exists$ a Room square of side $s\}$. (See §VI.50.)
- $S = \{s : \exists$ a self-orthogonal latin square of order $s\}$. (See §III.5.)

3.14 **Example** A set that is not PBD-closed: $RB(k) = \{v : \exists$ a resolvable BIBD$(v, k, 1)\}$.

3.15 **Theorem** [950] Let n be an integer, $n \geq 3$. Let $P_{1,n} = \{s : s \equiv 1 \pmod n, s = p^t$ for some prime p and positive integer $t\}$. Then $B(P_{1,n})$ is eventually periodic with minimum period n; that is, there exists a constant C_n such that if $v > C_n$ and $v \equiv 1 \pmod n$, then $v \in B(P_{1,n})$.

3.16 **Example** [950] The use of Theorem 3.15. A *Hering configuration* of type n and order $v = sn + 1$ is a decomposition of the complete directed graph DK_{sn+1} into a family $H = \{H_1, H_2, \ldots, H_{sn+1}\}$ of spanning directed subgraphs, each consisting of s directed n-cycles and an isolated vertex, which has the property that any pair H_i, $H_j, i \neq j$ share precisely one edge in common when viewed as undirected graphs, but that the edge is oriented in opposite directions in H_i and H_j. Let $S_n = \{v : \exists$ a Hering configuration of type n and order $v\}$. A necessary condition for $v \in S_n$ is that $v \equiv 1 \pmod n$. It is known that S_n is PBD-closed. It is also known that if $q = sn+1$ is a prime power, then there exists a Hering configuration of type n and of order q. In view of Dirichlet's theorem, which guarantees the existence of a prime $p \equiv 1 \pmod n$, and Theorem 3.15, it follows that for all fixed n and sufficiently large $v \equiv 1 \pmod n$, there exists a Hering configuration of type n and order v. In fact, as shown in Table 3.23, $B(\{4, 7\}) = \{v : v \equiv 1 \pmod 3, v \neq 10, 19\}$. Because 19 is a prime, there is a Hering configuration of type 3 and order 19. Further, it can be shown that there is no Hering configuration of type 3 and order 10. Hence, there is a Hering configuration of type 3 and order $v \equiv 1 \pmod 3$ if and only if $v \geq 4$ and $v \neq 10$. Similarly it is shown in Table 3.23 that $B(\{5, 9, 13, 17, 29, 33\}) = \{n : n \geq 5,\ n \equiv 1 \pmod 4\}$. Because $\{5, 9, 13, 17, 29\}$ is a set of prime powers and a Hering configuration of type 4 and order 33 can be constructed, there is a Hering configuration for all $v \equiv 1 \pmod 4,\ v \geq 5$.

3.17 Let K be a PBD-closed set. Let G be a set of positive integers such that $K = B(G)$. Then G is a *generating set* for K.

3.18 Let K be a PBD-closed set. An element $x \in K$ is *essential* in K if and only if $x \notin B(K\backslash\{x\})$; that is, if and only if there does not exist a PBD$(x, K\backslash\{x\})$.

3.19 **Theorem** [2146] Let E_K denote the set of all essential elements in a PBD-closed set K. Then E_K is the unique minimal generating set for K. Moreover, E_K is finite.

3.20 **Theorem** [2146] Let K be a PBD-closed set. Suppose that $G \subseteq K$. Then G is a generating set for K if and only if $E_K \subseteq G$.

3.21 **Remark** There is some confusion in the usage of these terms. Some authors refer to any generating set for a set K as a basis and speak of E_K as the minimal basis. Others speak of E_K as being the minimal generating set. Still others refer to the minimal set E_K as a basis. Here, *basis* refers to the set E_K.

3.22 **Remark** There are two approaches to PBD-closed sets. One approach is to be given a set of positive integers K and to determine $B(K)$ as accurately as possible. Alternatively one can select a PBD-closed set and determine as small a generating set as possible. Tables 3.23, 3.24, and 3.26 reflect both approaches.

3.23 **Table** Closures of subsets. In the exceptions for the closure of K, nonnegative integers smaller than $\min(K)$ are omitted, because 0 and 1 are always present and the remaining integers are always absent. Braces and commas are omitted from sets. When large sequences of exceptions occur, (a–b) means all values in the relevant residue classes from a to b (inclusive). $\mathbb{N}$ is used when the closure contains all sufficiently large integers. The precise closure of all subsets of $\{3, 4, \ldots, 10\}$ that contain the element 3 are exhibited first [975]. Because $\{7, 9\} \subset B(3)$, it is not necessary to include 7 or 9 in the list of sets whose closures are given. Similarly because $10 \in B(\{3, 4\})$, it is not necessary to include 10 when 3 and 4 are both present.

Subset	Closure	**Genuine Exceptions**
3	1 3 mod 6	–
3 4	0 1 mod 3	**6**
3 5	1 mod 2	–
3 6	0 1 mod 3	**4 10 12 22**
3 8	$\mathbb{N}$	**4 5 6 10 11 12 14 16 17 18 20 23 26 28 29 30 34 35 36 38**
3 10	0 1 mod 3	**4 6 12 16 18 22 24 34 36 42**
3 4 5	$\mathbb{N}$	**6 8**
3 4 6	0 1 mod 3	–
3 4 8	$\mathbb{N}$	**5 6 11 14 17**
3 5 6	$\mathbb{N}$	**4 8 10 12 14 20 22**
3 5 8	$\mathbb{N}$	**4 6 10 12 14 16 18 20 26 28 30 34**
3 5 10	$\mathbb{N}$	**4 6 8 12 14 16 18 20 22 24 26 32 34 36 38 42 44**
3 6 8	$\mathbb{N}$	**4 5 10 11 12 14 17 20 23**
3 6 10	0 1 mod 3	**4 12 22**
3 8 10	$\mathbb{N}$	**4 5 6 11 12 14 16 17 18 20 23 26 29 35 36**
3 4 5 6	$\mathbb{N}$	**8**
3 4 5 8	$\mathbb{N}$	**6**

3 4 6 8	$\mathbb{N}$	**5 11 14 17**
3 5 6 8	$\mathbb{N}$	**4 10 12 14 20**
3 5 6 10	$\mathbb{N}$	**4 8 12 14 20 22**
3 5 8 10	$\mathbb{N}$	**4 6 12 14 16 18 20 26**
3 6 8 10	$\mathbb{N}$	**4 5 11 12 14 17 20 23**
3 4 5 6 8	$\mathbb{N}$	–
3 5 6 8 10	$\mathbb{N}$	**4 12 14 20**

Subset	Closure	Ref(s)	**Genuine** and Possible Exceptions
4	1 4 mod 12	[1042]	–
4 5	0 1 mod 4	[225]	**8 9 12**
4 6	0 1 mod 3	[882, 1652]	**7 9 10 12 15 18 19 22 24 27** 33 34 39 45 46 51 87
4 7	1 mod 3	[335]	**10 19**
4 8	0 1 mod 4	[23, 1652]	**5 9 12 17 20 21 24 33 41 44 45** 48 53 60 65 69 77 89
4 9	0 1 4 9 mod 12	[866, 1652]	**12 21 24 48** 60 69 84 93 96
4 5 6	$\mathbb{N}$	[1426]	**7 8 9 10 11 12 14 15 18 19 23**
4 5 7	$\mathbb{N}$	[1426, 1652]	**6 8 9 10 11 12 14 15 18 19 23 26 27** 30 39 42 51 54
4 5 8	0 1 mod 4	[225]	**9 12**
4 5 9	0 1 mod 4	[225]	**8 12**
4 5 11	$\mathbb{N}$	[192]	**6 7 8 9 10 12 14 15 18 19 22 23 26 27 30 31 34** 38 42 43 46 50 54 58 62 66 67 70 74 78 82 90 94 98 102 106 114 118 126 130 142 154
4 6 7	0 1 mod 3	[1652]	**9 10 12 15 18 19 24 27** 33 45 87
4 6 8	$\mathbb{N}$	[882, 1652]	**5 7 9 10 11 12 14 15 17 18 19 20 22 23 24 26 27** 33 34 35 39 41 47 50 51 53 59 62 65 71 77 87 95 110 131 170
4 6 9	0 1 mod 3	[882, 1652]	**7 10 12 15 18 19 22 24 27** 34
4 7 8	$\mathbb{N}$	[23, 1652]	**5 6 9 10 11 12 14 15 17 18 19 20 21 23 24 26 27 30 33 35 38 39 41 42 44 45 47** 48 51 54 59 62 65 66 69 74 75 77 78 83 87 89 90 102 110 114 126 131 138 143 150 162 167 174 186
4 7 9	0 1 mod 3	[960, 1652]	**6 10 12 15 18 19 21 24 27 30 39 42 48** 51 54 60 66 69 75 78 84 87 93 96 102 111 114 138 147 150 159 174 183 195 210
4 8 9	0 1 mod 4	[866, 1652]	**5 12 17 20 21 24 41 44** 48 53 60 69 77
4 9 12	0 1 4 9 mod 12	[871]	**21 24**
4 5 6 7	$\mathbb{N}$	[1426]	**8 9 10 11 12 14 15 18 19 23**
4 5 6 8	$\mathbb{N}$	[1426]	**7 9 10 11 12 14 15 18 19 23**
4 5 6 9	$\mathbb{N}$	[1426]	**7 8 10 11 12 14 15 18 19 23**
4 5 7 8	$\mathbb{N}$	[959, 1426]	**6 9 10 11 12 14 15 18 19 23 26 27** 30 42 51

4 5 7 9	ℕ	[959, 1426]	**6 8 10 11 12 14 15 18 19 23 26 27** 30 51 54
4 5 7 11	ℕ	[192, 1652]	**6 8 9 10 12 14 15 18 19 23 26 27** 30 42 54
4 5 8 9	0 1 mod 4	[225]	**12**
4 6 7 8	ℕ	[1652]	**5 9 10 11 12 14 15 17 18 19 20 23 24 26 27** 33 35 41 65 77 131
4 6 7 9	0 1 mod 3	[882, 1652]	**10 12 15 18 19 24 27**
4 6 8 9	ℕ	[882, 1652]	**5 7 10 11 12 14 15 17 18 19 20 22 23 24 26 27** 34 35 41 47 50 53 59 62 71 77 95 131 170
4 7 8 9	ℕ	[23, 1652]	**5 6 10 11 12 14 15 17 18 19 20 21 23 24 26 27 30** 35 38 39 41 42 44 47 48 51 54 59 62 110 143 150 167 174
4 5 6 7 8	ℕ	[959]	**9 10 11 12 14 15 18 19 23**
4 5 6 7 9	ℕ	[959]	**8 10 11 12 14 15 18 19 23**
4 5 6 8 9	ℕ	[959]	**7 10 11 12 14 15 18 19 23**
4 5 7 8 9	ℕ	[1426, 1652]	**6 10 11 12 14 15 18 19 23 26 27** 30 51
4 6 7 8 9	ℕ	[1652]	**5 10 11 12 14 15 17 18 19 20 23 24 26 27** 35 41
4 5 6 7 8 9	ℕ	[959]	**10 11 12 14 15 18 19 23**
4 5 7 9 10 11	ℕ	[1426, 1652]	**6 8 12 14 15 18 19 23 26 27** 30
4 5 9 11 19 31	ℕ	[192]	**6 7 8 10 12 14 15 18 22 23 26 27 30 34** 38 42 43 46 50 54 62 66 74 78 90 98 102 114 126

5	1 5 mod 20	[1042]	–
5 6	0 1 mod 5	[196]	**10 11 15 16 20 35** 40 50 51 80
5 7	1 mod 2	[11, 196]	**9 11 13 15 17 19 23 27 29 31 33 37 39** 43 47 51 53 55 57 59 63 69 71 73 75 77 79 83 87 89 93 95 97 99 107 109 111 113 115 119 133 135 137 139 153 157 159 173 177 179 191 193 195 199 211 219 231 233 235 237 239 253 255 263 279 291 299 303 347 351 353 355 359 363 383 399 407 413 419 423 431 435 439 443 447 453 459 471 473 475 479 483 503 507 519 531 533 535 559 639
5 8	0 1 mod 4	[11, 196]	**9 12 13 16 17 20 24 28 29 32 33 37 44 49 52** 53 60 68 69 72 73 76 77 84 89 92 93 96 97 100 104 108 109 112 113 116 124 129 132 140 149 152 153 156 164 169 172 189 192 209 244 300 508 524 532 564 572 580 588 628 644 724 732 772 812
5 9	1 mod 4	[11, 196]	**13 17 29 33** 113
5 6 7	ℕ	[1473]	**(8–20) (22–24) (27–29) (32–34)** 68 69 93 94 98 99 104 108 109 114 124
5 6 8	ℕ	[196]	**7 (9–20) (22–24) (27–29) (32–35) (37–39)** 42 44 47 (50–53) 58 59 62 63 (67–69) 72 74 (77–79) (82–84) 87 89 92 94 (97–99) 103 104 107 109 112 114 118 119 122 123 124 129 139 142 149 152 154 159 169 172 174 179 182 189 194 199 202 214 219 239 242 244 247 259 262 267
5 6 9	ℕ	[11, 196]	**7 8 (10–20) (22–24) (27–29) (32–**

35) 38 39 40 42 43 44 47 48 52 58 59 62 64 67 68 72 79 80 82 83 84 87 88 92 98 99 102 103 104 107 108 112 113 118 119 122 123 124 127 128 132 138 142 147 148 152 158 162 167 172 178 179 182 188 198 199 207 208 218 219 227 238 248 288

5 7 8 | $\mathbb{N}$ [11, 196] **6 (9–20) (22–24) (26–34) (37–39)** (42–44) 46 47 (51–53) (58–60) 62 66 (68–79) (82–84) 86 87 89 90 (93–100) 102 104 106 (107–111) (114–116) 118 122 124 126 130 132 134 135 138 140 142 146 150 153 154 156 158 162 164 166 170 172 174 178 186 190 191 194 195 198 202 206 210 211 214 226 230 234 244 258 262 274 278 282 298 300 338 359 422 443 471 478 562

5 7 9 | 1 mod 2 [11, 196] **(11–19) 23 (27–33) 39** 43 51 59 71 75 83 87 95 99 107 111 113 115 119 139 179

5 8 9 | 0 1 mod 4 [11, 196] **(12–20) 24 (28–33) 44** 52 60 68 84 92 96 100 104 108 112 113 116 124 132 140 156 172 244 300

5 9 13 | 1 mod 4 [1026] **17 29 33**

5 6 7 8 | $\mathbb{N}$ [1473] **(9–20) (22–24) (27–29) (32–34)** 94 124

5 6 7 9 | $\mathbb{N}$ [1473] **8 (10–20) (22–24) (27–29) (32–34)** 68 98 99 104 108 124

5 6 8 9 | $\mathbb{N}$ [11, 196] **7 (10–20) (22–24) (27–29) (32–35) 38 39** 42 47 52 67 79 82 83 84 87 92 98 99 103 107 118 119 122 123 124 142 172 182

5 7 8 9 | $\mathbb{N}$ [1473] **6 (10–20) (22–24) (26–34) 38 39** (42–44) 46 51 52 60 (94–96) 98 99 100 102 104 (106–108) 110 111 116 138 140 142 146 150 154 156 158 162 166 170 172 174 206

5 6 7 8 9 | $\mathbb{N}$ [1473] **(10–20) (22–24) (27–29) (32–34)**

---

6 | 1 6 mod 15 Table II.3.4

6 7 8 | $\mathbb{N}$ [960, 1473] **(9–30) (32–41) 45** 46 **47** 65 (68–71) (73–75) 77 (93–95) (98–101) (122–125) (128–131) 135 (137–140) (142–150) (152–155) (159–161) (165–167) 172 173 (177–179) 184 185 233 (235–240) (242–245)

6 7 8 9 | $\mathbb{N}$ [560, 1473] **(10–30) (32–41) 45** 46 **47** (93–95) (98–101) (137–139) (142–150) (152–155) 160 161 166 167 185

---

7 | 1 7 mod 42 Tables II.3.5, II.3.6

7 8 9 | $\mathbb{N}$ [560, 1473] **(10–48) (51–55) (59–62)** (93–111) (116–118) 132 (138–168) (170–174) (180–216) (219–223) (228–230) (242–258) (261–279) (283–286) (298–300) (303–307) (311–335) (339–342)

---

8 | 1 8 mod 56 Tables II.3.8, II.3.9

8 9 | 0 1 mod 8 [11, 44] **(16–56)** (88–113) (144–225) (248–281) (304–337) (360–393) 416 417 448 (472–497) (528–560) (600–616) 624 (808–840) (888–896) 952 1064 (1384–1408) (1456–1465) (1496–1505) (1528–1624) (1664–1680)

8 9 10 | $\mathbb{N}$ [1471] **(11–56) (58–63) (66–71) (75–79)** (101–109) (111–113) (115–119) 126 127 (133–135) (155–160) 166 167 (173–231) 239 (247–249) (250–287) (290–295) (290–295) (299–343) (346–351) (355–399) (403–407) (411–423) (426–431) (435–439) (443–448) (452–455) (472–497) (499–503) (507–511) (580–582)

3.24 Table More Closures. Let $n \geq 3$ be an integer.

$$\begin{aligned} Q_{\geq n} &= \{v : v \text{ is a prime power; } v \geq n\} \\ OQ_{\geq n} &= \{v : v \text{ is a prime power; } v \geq n,\ v \text{ is odd}\} \\ Q_{1 \bmod n} &= \{v : v \text{ is a prime power, } v \equiv 1 \bmod n\} \\ Q_{0,1 \bmod n} &= \{v : v \text{ is a prime power, } v \equiv 0, 1 \bmod n\} \end{aligned}$$

(Unless n is prime power, $Q_{0,1 \bmod n}$ is identical to $Q_{1 \bmod n}$.)

Subset	Closure	Ref(s)	**Genuine** and Possible Exceptions
$OQ_{\geq 3}$	1 mod 2		–
$OQ_{\geq 5}$	1 mod 2	[11, 192]	**15 33 39** 51 75 87
$OQ_{\geq 7}$	1 mod 2	[959]	**15 21 33 35 39 45 51 55 65** 69 75 87 93 95 105 111 115 123 129 135 141 155 159 183 195 213 215 219 231 235 237 245 255 267 285 291 303 305 309 315 321 327 335 339 345 365 375 395 415 445 447 453 455 465 471 483 485 501 507 519 525 543 573 597 605 615 651 699 717 735 843 861 1047
$Q_{\geq 3}$	$\mathbb{N}$		**6**
$Q_{\geq 4}$	$\mathbb{N}$	[959, 960]	**6 10 12 14 15 18 26** 30
$Q_{\geq 5}$	$\mathbb{N}$	[208]	**6 10 12 14 15 18 20 22 24 26 28 30 33 34 38 39** 42 44 46 51 52 60
$Q_{\geq 7}$	$\mathbb{N}$	[189]	**10 12 14 15 18 20 21 22 24 26 28 30 33 34 35 36 38 39 40 42 44 45 46 48 51 52 54 55 60 62**
$Q_{\geq 8}$	$\mathbb{N}$	[11, 208, 960]	**10 12 14 15 18 20 21 22 24 26 28 30 33 34 35 36 38 39 40 42 44 45 46 48 50 51 52 54 55 56 58 60 62 63 66 68 69 70 74 75 76 77 78 82 84 85 86 87** 90 92 93 94 95 98 100 102 106 108 110 111 114 116 118 119 122 124 126 130 132 134 138 140 142 146 148 150 154 159 162 164 166 170 172 174 175 178 180 182 183 186 188 190 194 196 198 202 204 206 210 212 214 218 220 222 226 228 230 234 236 238 242 244 246 250 252 258 260 262 266 268 270 274 276 278 282 284 286 290 292 294 298 300 302 303 306 308 310 314 318 322 324 326 330 332 334 335 338 340 346 348 350 354 356 358 362 364 366 370 372 374 378 380 382 386 388 390 394 396 398 402 406 410 412 414 418 420 422 426 428 430 434 436 438 442 444 446 450 452 454 458 460 462 466 468 470 474 476 478 482 484 486 490 492 494 498 500 502 506 508 510 514 516 518 526 530 532 534 542 546 548 550 554 556 558 562 564 566 570 572 578 580 582 586 588 594 596 598 602 604 606 610 612 614 618 620 622 626 628 630 634 636 638 642 644 646 650 652 654 658 660 662 666 668 670 674 676 678 682 684 686 690 692 694 698 700 702 706 708 710 716 718 722 724 726 730 732 734 738 740 742 746 748 750 754 756 758 762 764 766 770 772 774 778 780 786 788 794 796 798 802 804 806 810 812 818 820 822 826 828 830 834 836 842 844 846 850 852 854 858 860 862 866 868 874 876 878 882 884 886 890 892 894 898 902 906 908 910 914 916 918 922 926 930 934 938 940 942 946 948 950 954 956 958 964 966 982 994 996 998 1002 1004 1006 1010 1012 1014 1018 1020 1022 1026 1030 1034 1036 1038 1042 1044 1046 1050 1052 1054 1058 1060 1062 1066 1068 1070 1074 1076 1078 1082 1084 1086 1090 1092 1094 1098 1100 1106 1108 1110 1114 1116 1118 1122 1124 1126 1130 1132 1138 1140 1146 1150 1154 1162 1186 1188 1190 1194 1206 1210 1218 1226 1234 1242 1250 1252 1258 1266 1274 1306 1314 1322 1330 1354 1378 1386 1394 1402 1410 1418 1426 1434 1442 1450 1490 1506 1514 1522 1554 1570 1578 1586 1594 1602 1610 1618 1626 1650 1658 1682 1698 1714 1722 1730 1754 1762 1786 1802
$Q_{1 \bmod 3}$	1 mod 3	[335]	**10**
$Q_{1 \bmod 4}$	1 mod 4	[1026]	**33**

$Q_{1 \bmod 5} \cup \{6\}$ | 1 mod 5 | [18, 41, 1599] **21 26 36 46** 51 56 86 116 146 221 226 286 386 411 416 441 446 471 476 501 536 566 596 626 651 686 716 746 771 776 801 806 866 896 926 986

$Q_{1 \bmod 6}$ | 1 mod 6 | [959] **55** 115 145 205 235 265 319 355 391 415 445 451 493 649 667 685 697 745 781 799 805 1315

$Q_{1 \bmod 8}$ | 1 mod 8 | [960] **33 57 65 105 129** 161 177 185 201 209 249 265 297 305 321 345 377 385 417 465 473 481 489 497 505 537 545 553 561 609 633 681 705 713 737 745 753 785 825 849 897 913 921 945 985 993 1001 1041 1057 1065 1073 1113 1121 1137 1145 1185 1209 1257 1281 1329 1401 1425 1473 1497 1529 1537 1561 1569 1577 1593 1617 1625 1633 1641 1665 1673 1689 1705 1713 1745 1761 1769 1785 1793 1809 1817 1833 1857 1905 1977 2001 2049 2073 2121 2145 2913 2937 2945 2985 3009 3057 3081 3129 3201 3393 3417 3505 3705 4857 4985 5025 5097 5145 5169 5361 6585 6657 8193 8313 8385 8673

$Q_{0,1 \bmod 7}$ | 0 1 mod 7 | [205, 960] **14 15 21 22 28 35 36 42** 70 77 78 84 85 98 99 105 106 126 133 134 140 141 147 148 154 155 161 162 168 182 183 189 190 196 238 245 246 252 253 266 267 273 274 294 315 316 322 329 364 371 378 420 574 581 588 623 630 1078 1085 1092 1106 1107 1113 1114 1120 1127 1134 1162 1169 1170 1218 1260 1372 1407

$Q_{01 \bmod 8}$ | 0 1 mod 8 | [11, 44] **10 24 33 40 48 56** 88 96 104 105 112 160 161 168 176 177 184 185 192 224 312 368 377 384 448 888 896

3.25 Theorem [11, 44] Let $Q_{015 \bmod 8}$ be the set of prime powers $\equiv 0, 1$, or 5 (mod 8). Necessary conditions for a $(v, Q_{015 \bmod 8})$-PBD to exist are $v \equiv 0, 1 \bmod 4$. These are sufficient in the following cases:

1. $v \equiv 0, 1$, or 5 mod 8 and $v \notin \{21, 24, 33, 40, 45, 48, 56, 69, 77, 85, 88, 93, 96, 160, 161, 165, 168, 176, 177, 184, 185, 192, 224, 368, 384\}$.
2. $v \equiv 4 \bmod 8$ and either $v \geq 2612$ or $v \in \{316, 404, 900, 924, 932, 1028, 1340, 1348, 1652, 1660, 1668, 1964, 2060, 2068, 2292, 2332, 2388, 2492, 2556, 2564, 2580, 2588, 2596\}$.

3.26 Table Generating sets. Here the opposite view is taken: A PBD-closed set is specified, and a generating set is presented for it. Here $K_n = \{v : v \geq n\}$, $H_{1(a)} = \{v : v \geq a,\ v \equiv 1 \pmod a\}$, and $H_{0,1(a)} = \{v : v \geq a,\ v \equiv 0, 1 \pmod a\}$. Essential elements are in bold, and elements not known to be essential are in normal typeface.

Closed Set	Generating Set	Ref.
K_3	**3 4 5 6 8**	[1042]
K_4	**4 5 6 7 8 9 10 11 12 14 15 18 19 23**	[1042, 1470]
K_5	**(5–20) 22 23 24 27 28 29 32 33 34**	[1042, 1470]
K_6	**(6–30) (32–41) (45–47)**	[1042, 1470]
K_7	**(7–48) (51–55) (59–62)**	[1470]
K_8	**(8–56) (58–63) (66–71) (75–79)**	[1470]
$H_{1(2)}$	**3 5**	[2149]
$H_{1(3)}$	**4 7 10 19**	[2149]
$H_{0,1(3)}$	**3 4 6**	[2149]
$H_{0,1(3)} \setminus \{3\}$	**4 6 7 9 10 12 15 18 19 24 27**	[1650]
$H_{0,1(3)} \setminus \{3, 4\}$	**(6–30) (33–40) 45 46** 51 **52** 69 93 94	[1651]
$H_{1(4)}$	**5 9 13 17 29 33**	[1026]
$H_{0,1(4)}$	**4 5 8 9 12**	[225]
$H_{0,1(4)} \setminus \{4, 5\}$	**(8–61) 68 69 76 77 84 85 88 92 93** 101	[19]

Closed Set	Generating Set	Ref.
$H_{1(5)}$	**6 11 16 21 26 36 41 46** 51 56 61 71 86 101 116	[18, 41, 959]
$H_{0,1(5)}$	**5 6 10 11 15 16 20 35** 40	[960, 2149]
$H_{1(6)}$	**7 13 19 25 31 37 43 55 61 67 73** 79 97 103 109 115 121 127 139 145 157 163 181 193 199 205 211 229 235 241 265 271 277 283 289 313 319 331 349 355 373 391 397 409 415 445 451 457 487 493 499 643 649 661 667 685 691 697 709 733 739 745 751 781 787 811 1315 1321 1327	[959, 967]
$H_{1(7)}$	**8 15 22 29 36 43 50 71 78 85 92 99** 106 113 127 134 141 148 155 162 169 176 183 190 197 204 211 218 225 239 246 253 260 267 274 281 295 302 309 316 323 330 337 351 358 365 372 379 386 414 421 428 442 575 582 589 596 603 610 701 708 715 722 827 834 1205 1212 1219 1226 1261 1268 1275 1282	[959]
$H_{1(8)}$	**9 17 25 33 41 49 57 65 89 97 105 113 121 129** 161 169 177 185 193 201 209 233 241 249 257 281 305 313 321 337 345 353 377 385 401 409 417 449 465 473 481 489 497 537 553 569 601 609 617 633 737 745 753 761 769 785 897 913 921 929 1049 1065 1073 1113 1121 1129 1145 1529 1537 1553 1561 1569 1577 1625 1633 1641	[960]
$H_{0,1(8)}$	**8 9 16 17 24 25 32 33 40 41 48 49 56** 88 89 96 97 104 105 112 113 160 161 168 169 176 177 184 185 192 224 312 368 377 384 448 560 888 896 944 952	[11, 44]

See Also

§II.1	Orders of BIBD(v, k, λ) form PBD-closed sets.
§II.7	Replication numbers of resolvable BIBDs with index one form PBD-closed sets.
§VI.50	The set of sides of Room squares is PBD-closed.

References Cited: [11, 18, 19, 23, 41, 44, 189, 192, 196, 205, 208, 225, 335, 560, 749, 866, 871, 882, 950, 959, 960, 967, 975, 1026, 1042, 1426, 1470, 1471, 1473, 1599, 1650, 1651, 1652, 2146, 2149, 2151]

4 Group Divisible Designs

Gennian Ge

4.1 Some Families of Group Divisible Designs

4.1 Theorem [2211] The necessary and sufficient conditions for the existence of a $(3, \lambda)$-GDD of type m^u are (1) $u \geq 3$, (2) $\lambda(u-1)m \equiv 0 \pmod 2$, and (3) $\lambda u(u-1)m^2 \equiv 0 \pmod 6$.

4.2 Theorem [555] Let g, u, and m be nonnegative integers. There exists a 3-GDD of the type $g^u m^1$ if and only if the following conditions are all satisfied:

1. if $g > 0$, then $u \geq 3$, or $u = 2$ and $m = g$, or $u = 1$ and $m = 0$, or $u = 0$;

2. $m \le g(u-1)$ or $gu = 0$;
3. $g(u-1) + m \equiv 0 \pmod 2$ or $gu = 0$;
4. $gu \equiv 0 \pmod 2$ or $m = 0$; and
5. $\frac{1}{2}g^2u(u-1) + gum \equiv 0 \pmod 3$.

4.3 **Table** All possible group-types for 3-GDDs on at most 60 points are determined [525]. Every primitive 3-GDD on at most 30 points has one of the following types. (The number of points is given in boldface.)

3: 1^3 **6:** 2^3 **7:** $3^1 1^4$ **8:** 2^4 **9:** 3^3 **10:** $4^1 2^3$
11: $5^1 1^6$ **12:** 2^6, 4^3 **13:** $3^4 1^1$ **14:** $4^3 2^1$, $6^1 2^4$ **15:** 3^5, 5^3, $7^1 1^8$
16: 4^4, $6^1 4^1 2^3$ **17:** $5^1 3^4$ **18:** $6^1 4^3$, 6^3, $8^1 2^5$ **19:** $3^6 1^1$, $5^3 3^1 1^1$, $7^1 3^4$, $9^1 1^{10}$
20: $6^1 4^3 2^1$, $6^3 2^1$, $8^1 2^6$, $8^1 4^3$ **21:** $5^3 3^2$, $7^1 3^4 1^2$, 7^3, $9^1 3^4$
22: $6^1 4^4$, $6^3 4^1$, $8^1 6^1 4^1 2^2$, $10^1 2^6$
23: $5^4 3^1$, $7^1 5^1 3^3 1^2$, $7^2 5^1 3^1 1^1$, $9^1 5^1 3^3$, $11^1 1^{12}$
24: 4^6, $6^2 4^3$, 6^4, $8^1 4^3 2^2$, $8^1 6^2 2^2$, 8^3, $10^1 4^2 2^3$
25: $7^1 5^3 3^1$, $7^2 3^3 1^2$, $7^3 3^1 1^1$, $9^1 3^5 1^1$, $9^1 5^3 1^1$, $9^1 7^1 3^3$
26: $4^6 2^1$, $6^2 4^3 2^1$, $6^4 2^1$, $8^1 6^1 4^3$, $8^1 6^3$, $8^2 6^1 2^2$, $8^3 2^1$, $10^1 6^1 4^2 2^1$, $12^1 2^7$
27: $7^1 5^3 3^1 1^2$, $7^2 3^4 1^1$, $7^3 3^2$, $9^1 5^3 3^1$, $9^1 7^1 3^3 1^2$, $9^1 7^2 1^4$, 9^3, $11^1 5^2 3^1 1^3$, $13^1 1^{14}$
28: $6^2 4^4$, $6^4 4^1$, $8^1 4^4 2^2$, $8^1 6^2 4^1 2^2$, $8^2 6^1 4^1 2^1$, $8^3 4^1$, $10^1 6^1 4^3$, $10^1 6^3$, $10^1 8^1 2^5$, $12^1 4^1 2^6$, $12^1 4^4$
29: $7^1 5^4 1^2$, $7^3 5^1 3^1$, $9^1 5^4$, $9^1 7^1 5^1 3^2 1^2$, $9^1 7^2 5^1 1^1$, $9^2 5^1 3^2$, $11^1 3^6$, $11^1 5^3 3^1$, $11^1 7^1 3^3 1^2$
30: 6^5, $8^1 6^1 4^3 2^2$, $8^1 6^3 2^2$, $8^2 4^3 2^1$, $8^2 6^2 2^1$, $8^3 6^1$, $10^1 4^5$, $10^1 6^2 4^2$, $10^1 8^1 4^2 2^2$, 10^3, $12^1 6^1 4^3$, $12^1 6^3$, $14^1 2^8$

4.4 **Theorem** [542] Let u, r, and t be positive integers. Then there exists a 3-GDD of type $u^r 1^t$ if and only if $u \equiv 1 \pmod 2$; $r + t \equiv 1 \pmod 2$; if $r = 1, t \ge u + 1$; if $r = 2, t \ge u$; and $\binom{t}{2} + rut + \binom{r}{2}u^2 \equiv 0 \pmod 3$.

4.5 **Theorem** [542] Let u and v be positive integers with $v \le u$. Then a 3-GDD of type $u^1 v^1 1^u$ exists if and only if $(u, v) \equiv (1,1), (3,1), (3,3), (3,5), (5,1)$ modulo (6,6).

4.6 **Theorem** [2211] The necessary and sufficient conditions for the existence of a $(4, \lambda)$-GDD of type m^u are (1) $u \ge 3$, (2) $\lambda(u-1)m \equiv 0 \pmod 4$, and (3) $\lambda u(u-1)m^2 \equiv 0 \pmod{12}$, with the exception of $(m, u, \lambda) \in \{(2,4,1), (6,4,1)\}$, in which case no such GDD exists.

4.7 **Theorem** The necessary conditions for a 4-GDD of type $g^u m^1$ with $g, m > 0$ and $u \ge 4$ are that $m \le g(u-1)/2, gu \equiv 0 \pmod 3, g(u-1) + m \equiv 0 \pmod 3$ and $\binom{gu+m}{2} - u\binom{g}{2} - \binom{m}{2} \equiv 0 \pmod 6$.

4.8 **Theorems** 4-GDDs with all but one group of the same size $s \in \{1, 3\}$.

1. A 4-GDD of type $1^u m^1$ exists if and only if $u \ge 2m+1$ and either $m, u+m \equiv 1$ or $4 \pmod{12}$ or $m, u+m \equiv 7$ or $10 \pmod{12}$.
2. A 4-GDD of type $3^u m^1$ exists if and only if either $u \equiv 0 \pmod 4$ and $m \equiv 0 \pmod 3, 0 \le m \le (3u-6)/2$; or $u \equiv 1 \pmod 4$ and $m \equiv 0 \pmod 6, 0 \le m \le (3u-3)/2$; or $u \equiv 3 \pmod 4$ and $m \equiv 3 \pmod 6$, $0 < m \le (3u-3)/2$.

4.9 **Theorems** 4-GDDs with all but one group of the same size $s \in \{2, 4, 5, 6, 12, 15\}$.

1. There exists a 4-GDD of type $2^u m^1$ for each $u \ge 6$, $u \equiv 0 \pmod 3$ and $m \equiv 2 \pmod 3$ with $2 \le m \le u-1$ except for $(u, m) = (6, 5)$ and possibly excepting $(u, m) \in \{(21, 17), (33, 23), (33, 29), (39, 35), (57, 44)\}$.
2. A 4-GDD of type $4^u m^1$ exists if and only if either $u = 3$ and $m = 4$, or $u \ge 6$, $u \equiv 0 \pmod 3$ and $m \equiv 1 \pmod 3$ with $1 \le m \le 2(u-1)$.

3. A 4-GDD of type $5^u m^1$ exists if and only if either $u \equiv 3 \pmod{12}$ and $m \equiv 5 \pmod 6, 5 \le m \le (5u-5)/2$; or $u \equiv 9 \pmod{12}$ and $m \equiv 2 \pmod 6$, $2 \le m \le (5u-5)/2$; or $u \equiv 0 \pmod{12}$ and $m \equiv 2 \pmod 3, 2 \le m \le (5u-8)/2$.
4. There exists a 4-GDD of type $6^u m^1$ for every $u \ge 4$ and $m \equiv 0 \pmod 3$ with $0 \le m \le 3u-3$ except for $(u,m) = (4,0)$ and except possibly for $(u,m) \in \{(7,15), (11,21), (11,24), (11,27), (13,27), (13,33), (17,39), (17,42), (19,45), (19,48), (19,51), (23,60), (23,63)\}$.
5. A 4-GDD of type $12^u m^1$ exists if and only if either $u = 3$ and $m = 12$, or $u \ge 4$ and $m \equiv 0 \pmod 3$ with $0 \le m \le 6(u-1)$.
6. A 4-GDD of type $15^u m^1$ exists if and only if either $u \equiv 0 \pmod 4$ and $m \equiv 0 \pmod 3, 0 \le m \le (15u-18)/2$; or $u \equiv 1 \pmod 4$ and $m \equiv 0 \pmod 6, 0 \le m \le (15u-15)/2$; or $u \equiv 3 \pmod 4$ and $m \equiv 3 \pmod 6$, $0 < m \le (15u-15)/2$.

4.10 Table Existence of 4-GDDs of small order [1359].

v	Group Type	Exist
4	1^4	YES
8	2^4	NO
12	3^4	YES
13	1^{13}	YES
	$1^9 4^1$	YES
14	2^7	YES
15	3^5	YES
16	1^{16}	YES
	$1^{12}4^1$	YES
	$1^8 4^2$	YES
	$1^4 4^3$	YES
	4^4	YES
17	$2^6 5^1$	NO
20	2^{10}	YES
	5^4	YES
21	$3^5 6^1$	YES
22	$1^{15}7^1$	YES
23	$2^9 5^1$	YES

v	Group Type	Exist
24	3^8	YES
	$3^4 6^2$	YES
	6^4	NO
25	1^{25}	YES
	$1^{21}4^1$	YES
	$1^{17}4^2$	YES
	$1^{13}4^3$	YES
	$1^9 4^4$	YES
	$1^5 4^5$	YES
	$1^1 4^6$	YES
26	2^{13}	YES
	$2^3 5^4$	?
	$2^9 8^1$	YES
27	3^9	YES
	$3^5 6^2$	?
	$3^1 6^4$	YES
28	1^{28}	YES
	$1^{24}4^1$	YES

v	Group Type	Exist
28	$1^{20}4^2$	YES
	$1^{16}4^3$	YES
	$1^{12}4^4$	YES
	$1^8 4^5$	YES
	$1^4 4^6$	YES
	4^7	YES
	$1^{14}7^2$	YES
	$1^{10}4^1 7^2$	YES
	$1^6 4^2 7^2$	YES
	$1^2 4^3 7^2$	YES
	7^4	YES
29	$2^{12}5^1$	YES
	$2^2 5^5$	?
	$2^8 5^1 8^1$	YES
30	$3^8 6^1$	YES
	$3^4 6^3$	YES
	6^5	YES
	$3^7 9^1$	YES

4.11 Theorem More results on 4-GDDs with all but one group of the same size.

1. Let $g \equiv 0 \pmod 6$ and $u \ge 4$. Then there exist 4-GDDs of types $g^u 0^1$ and $g^u (g(u-1)/2)^1$, except that there is no 4-GDD of type $6^4 0^1$. There is a 4-GDD of type $6^4 3^1$.
2. Let $g \equiv 3 \pmod 6$ and $u \ge 4$, $u \not\equiv 2 \pmod 4$. If $u \equiv 0 \pmod 4$ then there exist 4-GDDs of types $g^u 0^1$ and $g^u((g(u-1)-3)/2)^1$; if $u \equiv 1 \pmod 4$ then there exist 4-GDDs of types $g^u 0^1$ and $g^u(g(u-1)/2)^1$; if $u \equiv 3 \pmod 4$ then there exist 4-GDDs of types $g^u 3^1$ and $g^u(g(u-1)/2)^1$.
3. Let $g \equiv 1 \pmod 6$ and $u \equiv 0 \pmod 3$, $u \ge 9$ and $u \not\equiv 6 \pmod{12}$. If $u \equiv 0 \pmod{12}$ then there exist 4-GDDs of types $g^u 1^1$ and $g^u((g(u-1)-3)/2)^1$; if $u \equiv 3 \pmod{12}$ then there exist 4-GDDs of types $g^u 1^1$ and $g^u(g(u-1)/2)^1$; if $u \equiv 9 \pmod{12}$ then there exist 4-GDDs of types $g^u 4^1$ and $g^u(g(u-1)/2)^1$.
4. Let $g \equiv 4 \pmod 6$ and $u \equiv 0 \pmod 3$, $u \ge 6$. Then there exist 4-GDDs of types $g^u 1^1$ and $g^u(g(u-1)/2)^1$.
5. Let $g \equiv 2 \pmod 6$ and $u \equiv 0 \pmod 3$, $u \ge 6$. Then there exist 4-GDDs of types $g^u 2^1$ and $g^u(g(u-1)/2)^1$, except that there is no 4-GDD of type $2^6 5^1$.

6. Let $g \equiv 5 \pmod 6$ and $u \equiv 0 \pmod 3$, $u \geq 9$ and $u \not\equiv 6 \pmod{12}$. If $u \equiv 0 \pmod{12}$ then there exist 4-GDDs of types $g^u 2^1$ and $g^u((g(u-1)-3)/2)^1$, except possibly for type $g^{12}2^1$ when $g \in \{11, 17\}$; if $u \equiv 3 \pmod{12}$ then there exist 4-GDDs of types $g^u 5^1$ and $g^u(g(u-1)/2)^1$, except possibly for type $11^{27}5^1$; if $u \equiv 9 \pmod{12}$ then there exist 4-GDDs of types $g^u 2^1$ and $g^u(g(u-1)/2)^1$, except possibly for type $11^{21}2^1$.

4.12 Theorem There exists a 4-GDD of type $g^4 m^1$ with $m > 0$ if and only if $g \equiv m \equiv 0 \pmod 3$ and $0 < m \leq \frac{3g}{2}$.

4.13 Theorem

1. Let $g \equiv 0 \pmod 6$ and $u \equiv 0 \pmod 4$, where $u = 4$ or $u \geq 12$. Then there exists a 4-GDD of type $g^u m^1$ for every $m \equiv 0 \pmod 3$ with $0 \leq m \leq g(u-1)/2$, except possibly when $u = 12$ and either $g = 6$ or $0 < m < g$.
2. Let $g \equiv 2$ or $4 \pmod 6$ and $u \equiv 0 \pmod{12}$. Then there exists a 4-GDD of type $g^u m^1$ for every $m \equiv g \pmod 3$ with $0 < m \leq g(u-1)/2$, except possibly when $u = 12$ and $0 < m < g$.

4.14 Remark For the references to Theorems 4.7–4.13 on 4-GDDs of type $g^u m^1$, see [878] and the references therein.

4.15 Proposition There exist 4-GDDs of types
$9^5 6^1$, $3^6 9^2$, $3^7 9^2$, $3^8 6^2$, $3^8 9^4$, $3^{15} 9^2$, $6^4 12^2$, $3^8 6^1 12^1$, $3^9 6^1 12^1$, $3^{11} 6^1 15^1$, $6^4 9^1 12^1$, $6^5 12^1 15^1$, $9^4 12^1 18^1$, $6^8 18^1 24^1$, $6^8 21^1 24^1$, $6^9 12^1 27^1$, $6^6 9^1 18^1$, $6^{14} 9^1 42^1$, $12^4 15^1 24^1$, $12^5 15^1 30^1$, $12^6 15^1 36^1$, $12^8 15^1 48^1$, $12^{11} 15^1 66^1$, $12^{12} 15^1 72^1$, $12^5 21^1 30^1$, $12^6 21^1 36^1$, $12^{11} 27^1 66^1$, $18^4 30^1 36^1$, $6^{13} 24^1 39^1$, $3^{14} 9^1 21^1$, $6^{15} 24^1 45^1$, $3^{16} 9^1 24^1$, $3^{20} 9^1 30^1$, $6^{11} 12^1 33^1$, $6^{14} 18^1 42^1$, $6^{16} 18^1 48^1$, $6^{17} 12^1 51^1$, $3^{22} 21^1 33^1$, $3^{26} 9^1 39^1$, $9^{11} 39^1$, $3^{30} 21^1 45^1$, $9^9 12^1$, $9^9 30^1$, $3^{24} 21^1 36^1$, $3^{28} 9^1 42^1$ and $3^{36} 21^1 54^1$.

4.16 Theorem [881] The necessary conditions for the existence of 5-GDDs of type g^u (Theorem IV.1.11) are also sufficient, except when $g^u \in \{2^5, 2^{11}, 3^5, 6^5\}$, and possibly where

1. $g^u = 3^{45}$, 3^{65};
2. $g \equiv 2, 6, 14, 18 \pmod{20}$ and
   (a) $g = 2$ and $u \in \{15, 35, 71, 75, 95, 111, 115, 195, 215\}$;
   (b) $g = 6$ and $u \in \{15, 35, 75, 95\}$;
   (c) $g = 18$ and $u \in \{11, 15, 71, 111, 115\}$;
   (d) $g \in \{14, 22, 26, 34, 38, 46, 58, 62\}$ and $u \in \{11, 15, 71, 75, 111, 115\}$;
   (e) $g \in \{42, 54\}$ or $g = 2\alpha$ with $\alpha \equiv 1, 3, 7, 9 \pmod{10}$ and $33 \leq \alpha \leq 2443$, and $u = 15$;
3. $g \equiv 10 \pmod{20}$ and
   (a) $g = 10$ and $u \in \{5, 7, 15, 23, 27, 33, 35, 39, 47\}$;
   (b) $g = 30$ and $u \in \{9, 15\}$;
   (c) $g = 50$ and $u \in \{15, 23, 27\}$;
   (d) $g = 90$ and $u = 23$;
   (e) $g = 10\alpha$, $\alpha \equiv 1 \pmod 6$, $7 \leq \alpha \leq 319$, and $u \in \{15, 23\}$;
   (f) $g = 10\beta$, $\beta \equiv 5 \pmod 6$, $11 \leq \beta \leq 443$, and $u \in \{15, 23\}$;
   (g) $g = 10\gamma$, $\gamma \equiv 1 \pmod 6$, $325 \leq \gamma \leq 487$, and $u = 15$;
   (h) $g = 10\delta$, $\delta \equiv 5 \pmod 6$, $449 \leq \delta \leq 485$, and $u = 15$.

4.17 Theorem [39] A 5-GDD of type $g^5 m^1$ exists if $g \equiv 0 \pmod 4$, $m \equiv 0 \pmod 4$, and $m \leq 4g/3$, with the possible exceptions of $(g, m) = (12, 4)$ and $(12, 8)$.

4.18 Remark The existence of a PBD$(v, \{5, w^*\})$ is equivalent to that of a 5-GDD of types $1^{v-w} w^1$ or $4^{\frac{v-w}{4}}(w-1)^1$. See Theorem 1.27.

4.19 **Remark** There exist 5-GDDs of types $4^7 8^3$, $8^{15}4^1$, $8^{19}28^1$, $8^{23}12^1$, $12^7 4^1$, $12^{10}8^1$, $12^{10}16^1$, $12^{12}4^1$, $12^{13}8^1$, $16^7 12^1$, $12^8 8^1$, $16^8 4^1$, $12^7 4^1$, and $60^7(4a)^1$ for $0 \le a \le 19$.

4.20 **Theorem** [117] Let $\lambda \ge 2$. The necessary conditions for the existence of $(5, \lambda)$-GDDs of type g^u (Theorem IV.1.11) are also sufficient, except possibly when $\lambda = 2$, $u = 15$ and either $g = 9$ or $\gcd(g, 15) = 1$.

4.21 **Remark** The divisible (or elliptic) semiplanes in Examples VII.3.9 and 3.10 give a 7-GDD of type 3^{15}, a 12-GDD of type 3^{45}, and a 9-RGDD of type 3^{33}.

4.22 **Remark** [793] An optimal $(g+1)$-ary (v, k, d) constant weight code over $\mathbb{Z}_{g+1}$ can be constructed from a k-GDD of type g^v, $(I_v \times I_g, \{\{i\} \times I_g \mid i \in I_v\}, \mathcal{B})$, where $I_m = \{1, 2, \cdots, m\}$ and d is the minimum Hamming distance of the resulting code. For each block $\{(i_1,\ a_1), (i_2,\ a_2), \cdots, (i_k,\ a_k)\} \in \mathcal{B}$, form a codeword of length v by putting a_j in position i_j, $1 \le j \le k$, and zeros elsewhere. Then $k-1 \le d \le 2(k-2)+1$. A k-GDD of type g^v forming a code with minimum Hamming distance $2(k-2)+1$ is a *generalized Steiner system* $\mathrm{GS}(2, k, v, g)$. For the existence of generalized Steiner system and related designs, see [1197] and references therein.

4.2 GDDs with Holes

4.23 **Theorem** Let $(k-1)h = n$. A $\mathrm{TD}(k, n) - \mathrm{TD}(k, h)$ exists if and only if a $(k-1)$-GDD of type $(n-h)^k$ exists. This GDD is necessarily a frame.

4.24 **Example** By Theorem III.4.5, there is a $\mathrm{TD}(6, 10) - \mathrm{TD}(6, 2)$. Hence, there exists a 5-GDD of type 8^6. Another construction follows: The point set is $(I_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_2 \times \mathbb{Z}_4)$ where $I_2 = \{0, 1\}$. Let the groups be $g \times (\mathbb{Z}_2 \times \mathbb{Z}_4)$ for $g \in \mathbf{I}_2 \times \mathbb{Z}_3$. For blocks take

$$\begin{array}{l} \{(0,0,0,0), (0,1,0,2), (0,2,1,0), (1,0,1,1), (1,1,1,2)\}, \\ \{(0,0,0,0), (0,1,0,0), (0,2,1,1), (1,0,0,0), (1,1,0,3)\}, \\ \{(0,0,0,0), (0,1,0,1), (1,0,0,2), (1,1,0,2), (1,2,1,1)\}, \\ \{(0,0,0,0), (0,1,0,3), (1,0,1,3), (1,1,1,1), (1,2,0,3)\}, \end{array} \quad \text{all mod (-,3,2,4).}$$

4.25 **Theorem** [2211] Necessary and sufficient conditions for the existence of a $(3, \lambda)$-IGDD of type $(m, h)^u$ are $m \ge 2h$, $\lambda m(u-1) \equiv 0 \pmod 2$, $\lambda(m-h)(u-1) \equiv 0 \pmod 2$, and $\lambda u(u-1)(m^2-h^2) \equiv 0 \pmod 6$.

4.26 **Theorem** [2112] The necessary conditions for the existence of a 4-IGDD of type $(m, h)^u$ (Theorem IV.1.39) are also sufficient, except for $(u, m, h) \in \{(4, 2, 0), (4, 6, 0), (4, 6, 1)\}$ and except possibly for $(u, m, h) \in \{(14, 15, 3), (14, 21, 3), (14, 93, 27), (18, 15, 3), (18, 21, 3), (18, 93, 27)\}$.

4.27 Let X be a set of tmn points partitioned into m-subsets X_{ij}, for $0 \le i \le n-1$, and $0 \le j \le t-1$. Let $\mathcal{B}$ be a collection of subsets of X (*blocks*) that satisfies the following conditions:

1. $|b| = k$ for all blocks $b \in \mathcal{B}$,
2. let x and y be points with $x \in X_{i_1 j_1}$ and $y \in X_{i_2 j_2}$, then
   (a) if $i_1 \ne i_2$ and $j_1 \ne j_2$, then x and y are contained in exactly λ blocks together,
   (b) if $i_1 = i_2$ or $j_1 = j_2$, then x and y are together in no block.

Then $(X, \mathcal{B})$ is a *holey group divisible design* (denoted (k, λ)-HGDD(n, m^t)). The subsets $\cup_{j=0}^{t-1} X_{ij}$ where $0 \le i \le n-1$ are the *groups* and the subsets $\cup_{i=0}^{n-1} X_{ij}$, where $0 \le j \le t-1$, are the *holes*.

4.28 **Remark** HGDDs can be considered as a generalization of holey mutually orthogonal latin squares (HMOLS) (§III.4.4), since a k-HGDD(k, m^t) is equivalent to $k-2$ orthogonal HMOLS of type m^t.

4.29 **Theorem** The necessary conditions for the existence of a (k,λ)-HGDD(n, m^t) are that $t \geq k, n \geq k, \lambda(t-1)(n-1)m \equiv 0 \pmod{k-1}$, and $\lambda t(t-1)n(n-1)m^2 \equiv 0 \pmod{k(k-1)}$.

4.30 **Theorem** [2126] There exists a $(3,\lambda)$-HGDD(n, m^t) if and only if $t, n \geq 3$, $\lambda(t-1)(n-1)m \equiv 0 \pmod 2$, and $\lambda t(t-1)n(n-1)m^2 \equiv 0 \pmod 3$.

4.31 **Theorem** [2114] Let $u,\ t,\ g$ and w be nonnegative integers. The necessary and sufficient conditions for the existence of a 3-HGDD$(u,\ g^t w^1)$ are that

1. $u \geq 3,\ t = 2$ and $g = w$; or
2. $u \geq 3,\ t \geq 3,\ 0 \leq w \leq g(t-1),\ gt(u-1) \equiv 0 \pmod 2$, $(u-1)(w-g) \equiv 0 \pmod 2$, and $gtu(u-1)(g(t-1)-w) \equiv 0 \pmod 3$.

4.32 **Theorem** [884] There exists a $(4,\lambda)$-HGDD of type (n, m^t) if and only if $t, n \geq 4$ and $\lambda(t-1)(n-1)m \equiv 0 \pmod 3$ except for $(m, n, t) = (1, 4, 6), \lambda = 1$ and except possibly for $m = 3, \lambda = 1$ and $(n, t) \in \{(6, 14), (6, 15), (6, 18), (6, 23)\}$.

4.33 A *modified group divisible design* (MGDD) is a (k,λ)-HGDD$(n, 1^t)$.

4.34 **Corollary** From Theorems 4.30 and 4.32 it follows that the necessary existence conditions for MGDDs are sufficient when $k = 3$, and when $k = 4$ except for $(\lambda, n, t) = (1, 6, 4)$.

4.35 **Remark** For the existence of MGDDs with block size 5, see [8] and references therein.

4.3 Large Set of GDDs

4.36 Two k-GDDs with the same group set, say $(X, \mathcal{G}, \mathcal{A})$ and $(X, \mathcal{G}, \mathcal{B})$, are *disjoint* if $\mathcal{A} \cap \mathcal{B} = \emptyset$. A *large set* of disjoint k-GDDs is a collection $(X, \mathcal{G}_r, \mathcal{B}_r)_{r\in R}$ of k-GDDs, all having the same set of groups, such that for every k-subset B of X satisfying $|B \cap G| \leq 1$ for all $G \in \mathcal{G}$, there is exactly one $r \in R$ with $B \in \mathcal{B}_r$.

4.37 **Remark** It is not difficult to see that the maximum number of disjoint 3-GDDs of type $t^u s^1$ is $t(u-1)$ for $s \geq t$. Such a collection of disjoint 3-GDDs is denoted by $LS(t^u s^1)$ or $LS(t^{u+1})$ for $t = s$.

4.38 **Theorem** [1422] There exists an $LS(t^n)$ if and only if $n(n-1)t^2 \equiv 0 \pmod 6$ and $(n-1)t \equiv 0 \pmod 2$ and $(t, n) \neq (1, 7)$.

4.39 **Theorem** [1194] There exists an $LS(2^n 4^1)$ if and only if $n \equiv 0 \pmod 3$ with the possible exceptions of $n \in \{12, 30, 36, 48, 144\}$.

See Also

§III.3	TDs are special classes of GDDs.
§III.4	ITDs are special classes of IGDDs or HGDDs.
§IV.5	GDDs with resolvability.
[2211]	A broad survey of PBD and GDD constructions.

References Cited: [8,39,117,525,542,555,793,878,881,884,1194,1197,1359,1422,2112,2114,2126, 2211]

5 PBDs, Frames, and Resolvability

Gennian Ge
Ying Miao

5.1 Frames and Resolvability

5.1 **Remark** While the set $R(k) = \{r : \exists$ an RBIBD$(v, k, 1)$ with replication number $r\}$ is PBD-closed for fixed k, the set of replication numbers of an RBIBD(v, k, λ) is not in general PBD-closed for $\lambda \geq 2$. To overcome this difficulty, Hanani [1042] introduced resolvable frames (or briefly, frames). However, resolvable frames were explicitly defined by Stinson [1967].

5.2 Let $\mathcal{B}$ be the collection of blocks of a PBD, GDD, or BIBD of index λ. Then an *α-resolution class* (or *α-parallel class*) is a sub-collection of blocks of $\mathcal{B}$, which together contain every point of the design exactly α times.

5.3 A PBD, GDD, or BIBD of index λ is *α-resolvable* if the collection of blocks of the design can be partitioned into α-resolution classes. Furthermore, a design is *A-resolvable* if its collection of blocks $\mathcal{B}$ admits a partition into sub-collections $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_s$ where for each $i = 1, 2, \ldots, s$ there is an $\alpha_i \in A$ such that $\mathcal{B}_i$ forms an α_i-resolution class. An RGDD (*resolvable* GDD) is a 1-resolvable GDD.

5.4 **Example** A 2-resolvable BIBD$(10, 4, 6)$ with point set $\mathbb{Z}_9 \cup \{\infty\}$. 2-resolution classes are obtained by developing $[\{0,1,2,3\}, \{0,2,5,6\}, \{1,4,5,7\}, \{3,7,8,\infty\}, \{4,6,8,\infty\}]$ mod 9.

5.5 **Theorem** Let D be a PBD(v, K, λ) that is λ-resolvable. Let n denote the number of λ-resolution classes of D. Then for any $m \leq n$, there exists a PBD$(v + m, K \cup (K + 1) \cup \{m\}, \lambda)$, where $K + 1 = \{k + 1 : k \in K\}$. When $m = n$, the set of block sizes is in fact $(K + 1) \cup \{n\}$. In particular, if there exists a λ-resolvable BIBD(v, k, λ), with $v \neq k^2$, then there exists a PBD$(v + n, \{k + 1, n^\dagger\}, \lambda)$, where the symbol $n^\dagger$ indicates that there are λ identical blocks of size n in the design, and no other blocks of size n. If $v = k^2$, then one obtains a PBD$(k^2 + k + 1, \{k + 1\}, \lambda)$ (a design that has the parameters of a λ-fold copy of a (perhaps nonexistent) projective plane of order k).

5.6 Let v, k, and α be positive integers and let V be a set of cardinality v. Let any subset of size k of V be a *block*. Then an *α-partial* resolution class is a collection $\mathcal{C}$ of blocks such that every element of V occurs in either exactly α or exactly zero blocks of $\mathcal{C}$. The elements of V not occurring in the partial resolution class form the *complement* of the class.

5.7 Let k, α, and λ be positive integers. A *$(k, \alpha; \lambda)$-frame* is a triple $(V, \mathcal{G}, \mathcal{B})$ where V is a set of cardinality v, $\mathcal{G}$ is a partition of V into parts (*groups*), and $\mathcal{B}$ is a collection of blocks of size k that can be partitioned into a collection $\mathcal{P}$ of α-partial resolution classes of V that satisfies the conditions:

1. The complement of each α-partial resolution class P of $\mathcal{P}$ is a group $G \in \mathcal{G}$.
2. Each unordered pair $\{x, y\} \subseteq V$ that does not lie in some group G of $\mathcal{G}$ lies in precisely λ blocks of $\mathcal{B}$.
3. No unordered pair $\{x, y\} \subseteq V$ that lies in some group G of $\mathcal{G}$ also lies in a block of $\mathcal{B}$.

5.8 The *type* of the $(k, \alpha; \lambda)$-frame is the multiset $T = [|G| : G \in \mathcal{G}]$. If $\mathcal{G}$ contains a_1 groups of size g_1, a_2 groups of size g_2, and so on, where $v = a_1g_1 + a_2g_2 + \ldots + a_sg_s$, then the exponential notation $g_1^{a_1}g_2^{a_2}\ldots g_s^{a_s}$ is also used. By convention, factors of the type 0^a can be included in the exponential form of the type to accommodate null groups when necessary.

5.9 **Example** A $(3, 1; 1)$-frame of type 2^4 with point set $\{1, 2, 3, 4, 5, 6, 7, 8\}$.

groups	{1,5}	{2,4}	{3,6}	{7,8}
blocks	{2,6,7}	{1,6,8}	{1,4,7}	{1,2,3}
	{3,4,8}	{3,5,7}	{2,5,8}	{4,5,6}

5.10 **Remark** A $(k, \alpha; \lambda)$-frame is simply a (k, λ)-GDD with an additional property on the collection of blocks of the design.

5.11 **Theorem** Let k, α and λ be positive integers. Suppose that there exists a $(k, \alpha; \lambda)$-frame of type $g_1^{a_1}g_2^{a_2}\ldots g_s^{a_s}$, and that for $i = 1, 2, \ldots, s$, there exists an α-resolvable BIBD$(g_i + 1, k, \lambda)$. Then there exists an α-resolvable BIBD$((\sum_{i=1}^{s} a_ig_i) + 1, k, \lambda)$.

5.12 **Theorem** Let $(V, \mathcal{G}, \mathcal{B})$ be a GDD of index λ_1 (the master GDD) and let w be a mapping $V \to \mathbb{Z}^+ \cup \{0\}$. Suppose that for each $B \in \mathcal{B}$, there exists a $(k, \alpha; \lambda_2)$-frame of type $[w(x) : x \in B]$. Then there exists a $(k, \lambda_1\alpha; \lambda_1\lambda_2)$-frame of type $T = \left[\sum_{x\in G} w(x) : G \in \mathcal{G}\right]$.

5.13 **Corollary** Let $F(k, \alpha; g, \lambda) = \{u : \exists$ a $(k, \alpha; \lambda)$-frame of type $g^u\}$. Then $F(k, \alpha; g, \lambda)$ is PBD-closed. (Apply Theorem 5.12 with $\lambda_1 = 1$).

5.14 **Remark** Theorem 5.12 has been used to construct classes of α-resolvable GDD of index λ and α-resolvable BIBD(v, k, λ). However, the main application lies in the area of 1-resolvability, that is, the case of resolvable designs. Within that area, the main emphasis has been on $(k, 1; 1)$-frames, both because of the importance of the construction of RBIBD$(v, k, 1)$, and due to the fact that a $(k, 1; \lambda)$-frame can be obtained from a $(k, 1; 1)$-frame by replicating the collection of blocks λ times, maintaining the frame structure.

5.15 A (k, λ)-*frame* of type T is a $(k, 1; \lambda)$-frame of type T. A k-*frame* of type T is a $(k, 1; 1)$-frame of type T.

5.16 **Theorem** The following relationships between frames and other combinatorial objects are known.

1. A k-frame of type $(k-1)^{(v-1)/(k-1)}$ is equivalent to an RBIBD$(v, k, 1)$.
2. A $(k, k-1)$-frame of type 1^v is equivalent to an NRB$(v, k, k-1)$.
3. If there exists a $(k, k-1)$-frame of type T, then there exists a $(k+1, k+1)$-GDD of type T. Conversely if there exists a $(k+1, 1)$-GDD of type T, then there exists a $(k, k-1)$-frame of type T.
4. If there exists a TD$(k+1, kw)-$TD$(k+1, w)$, then there exists a k-frame of type $(w(k-1))^{k+1}$. Conversely, if there exists a k-frame of type t^{k+1}, then $(k-1)$ divides t; writing $t = w(k-1)$, there exists a TD$(k+1, kw) -$ TD$(k+1, w)$.
5. [31] If a complementary pair of Golay sequences exists, then a $(k, k-1)$-frame of type 2^{k+1} exists.

5.17 **Remark** Although deleting the blocks through a given point of an RBIBD(v, k, λ) does not give a frame when $\lambda > 1$, it does give a structure that can be used in Wilson's fundamental construction; for example, if an RTD$_\mu(k, n)$ and an RBIBD$((k-1)n + 1, k, \mu)$ also exist, then so does an RBIBD$((v-1)n + 1, k, \lambda\mu)$.

5.2 Frames

5.18 Theorem The necessary conditions for the existence of a (k, λ)-frame of type h^u are (1) $u \geq k+1$, (2) $h(u-1) \equiv 0 \pmod{k}$, and (3) $\lambda h \equiv 0 \pmod{k-1}$.

5.19 Theorem Let $(V, \mathcal{G}, \mathcal{B})$ be a (k, λ)-frame. Let F be a new set of points, that is, $F \cap V = \emptyset$. Suppose that for each $G \in \mathcal{G}$, there exists a (k, λ)-frame $(G \cup F, \mathcal{H}_G \cup \{F\}, \mathcal{B}_G)$. Then there exists a (k, λ)-frame $(V', \mathcal{G}', \mathcal{B}')$ where

$$V' = V \cup F, \quad \mathcal{G}' = \left(\bigcup_{G \in \mathcal{G}} \mathcal{H}_G\right) \cup \{F\}, \quad \mathcal{B}' = \mathcal{B} \bigcup \left(\bigcup_{G \in \mathcal{G}} \mathcal{B}_G\right).$$

5.20 Theorem If there exist a (k, λ_1)-frame of type g^u and an $\mathrm{RTD}_{\lambda_2}(k, m)$, then there exists a $(k, \lambda_1\lambda_2)$-frame of type $(mg)^u$.

5.21 A (k, λ) *incomplete frame* of type T is a (k, λ)-IGDD $(V, \mathcal{G}, \mathcal{H}, \mathcal{B})$ of type T such that

(1) the collection of blocks $\mathcal{B}$ can be partitioned into a collection $\mathcal{P}$ of partial resolution classes, and

(2) each $P \in \mathcal{P}$ contains either

(a) every point of $V \setminus G$ exactly once for some $G \in \mathcal{G}$ or

(b) every point of $V \setminus (G \cup \{H : H \in \mathcal{H}\})$ exactly once for some $G \in \mathcal{G}$.

5.22 Theorem [458] Suppose that there exists an $\mathrm{RTD}(u+1, t)$. If there exists a (k, λ) incomplete frame of type $(m + e_i, e_i)^u$ for any i, $1 \leq i \leq t$, then there exists a (k, λ) incomplete frame of type $(mt + e, e)^u$ with $e = \sum_{1 \leq i \leq t} e_i$. Furthermore, if there exists a (k, λ)-frame of type e^u, then there exists a (k, λ)-frame of type $(mt + e)^u$.

5.23 Remark Theorem 5.12 with $\lambda_1 = \alpha = 1$, Theorem 5.19 and Theorem 5.20 are standard frame constructions due to Stinson [1967]. Double frames were introduced to derive a general construction for frames that unifies these standard frame constructions and Theorem 5.22. See [458].

5.24 Theorem [24, 848] Let p and q be odd prime powers with $p < q$ and at least one of $p, q \equiv 3 \pmod{4}$. Then there exists a $(p, p-1)$-frame of type p^q, except possibly when $q = p + 2$, $q \equiv 7, 11, 15 \pmod{16}$, and $q \geq 27$.

5.25 Remark In [848], the existence of $(p, p-1)$-frames of type p^q for p, q both odd prime powers with $p < q$ was investigated. Extensive results were obtained although the proof for $p < q < 2p$ with $q \equiv 3 \pmod{4}$ was not correct. Since then more extensive results have been found [24]. Theorem 5.24 summarizes the most important of these.

5.26 Theorem [864] If there exists an ordered whist tournament frame of type h^n, then there exists a 4-frame of type $(3h)^n$.

5.27 Theorem [144, 848] If there exist $(k-2)/2$ SOLSSOM(n) with n odd and a basic factorization $BF_\lambda(k, m)$ (§II.7.2), then there exists a (k, λ)-frame of type m^n.

5.28 Theorem (Miao [864]) If there exist an $\mathrm{RBIBD}(2t+2, t+1, t)$ and t HSOLSSOM(h^n) with $(n-1)h \equiv 0 \pmod{2}$, then there exists a $(2t+2, 2t+1)$-frame of type $(2(t+1)h)^n$.

5.29 Theorem There exists a $(2, \lambda)$-frame of type h^u if and only if $u \geq 3$ and $h(u-1) \equiv 0 \pmod{2}$.

5.30 Theorem There exists a $(3, \lambda)$-frame of type h^u if and only if $u \geq 4$, $\lambda h \equiv 0 \pmod{2}$ and $h(u-1) \equiv 0 \pmod{3}$.

5.31 Theorem [881, 2201] There exists a 4-frame of type h^u if and only if $u \geq 5$, $h \equiv 0 \pmod{3}$ and $h(u-1) \equiv 0 \pmod{4}$, except possibly where

1. $h = 36$ and $u = 12$, and
2. $h \equiv 6 \pmod{12}$ and

(a) $h = 6$ and $u \in \{7, 23, 27, 35, 39, 47\}$;
(b) $h = 30$ or $h \in \{n : 66 \le n \le 2190\}$ and $u \in \{7, 23, 27, 39, 47\}$;
(c) $h \in \{42, 54\} \cup \{n : 2202 \le n \le 11238\}$ and $u \in \{23, 27\}$;
(d) $h = 18$ and $u \in \{15, 23, 27\}$.

5.32 Theorem [875] There exists a $(4, 3)$-frame of type h^u if and only if $u \ge 5$ and $h(u-1) \equiv 0 \pmod 4$, except possibly where $h \equiv 2 \pmod 4$ and

1. $h \in \{2\} \cup \{n : 10 \le n \le 3746\}$ and $u \in \{23, 27\}$, and
2. $h = 6$ and $u \in \{7, 23, 27, 39, 47\}$.

5.33 Theorems [883]

1. There exists a 3-frame of type $2^u m^1$ if and only if $u \equiv 0 \pmod 3$ and $m \equiv 2 \pmod 6$ with $2 \le m \le u - 1$.
2. There exists a 3-frame of type $4^u m^1$ if and only if $u \equiv 0 \pmod 3$ and $m \equiv 4 \pmod 6$ with $4 \le m \le 2u - 2$, except possibly for $(u, m) \in \{(21, 34), (33, 46), (33, 58), (39, 70)\}$.
3. There exists a 3-frame of type $6^u m^1$ if and only if either $(u, m) = (3, 6)$ or $u \ge 4$ and $m \equiv 0 \pmod 6$ with $0 \le m \le 3u - 3$, except possibly for $(u, m) \in \{(26, 54), (46, 120), (46, 126)\}$.
4. There exists a 3-frame of type $8^u m^1$ if and only if either $(u, m) = (3, 8)$ or $u \equiv 0 \pmod 4$, $u \ge 6$ and $m \equiv 2 \pmod 6$ with $2 \le m \le 4u - 4$.
5. There exists a 3-frame of type $12^u m^1$ if and only if either $(u, m) = (3, 12)$ or $u \ge 4$ and $m \equiv 0 \pmod 6$ with $0 \le m \le 6u - 6$, except possibly for $(u, m) \in \{(7, 30), (11, 42), (11, 54), (13, 54), (13, 66), (19, 102), (23, 126)\}$.

5.3 Resolvable Group Divisible Designs

5.34 Example A 3-RGDD of type 4^6 with point set $\mathbb{Z}_{10} \times \{0, 1\} \cup \{\infty_i : i = 1, 2, 3, 4\}$ and groups $\{(i, 0), (i + 5, 0), (i, 1), (i + 5, 1)\}$, $i = 0, 1, 2, 3, 4$; $\{\infty_i : i = 1, 2, 3, 4\}$. Parallel classes are obtained by developing the following $\mathrm{mod}(10, -)$:

$[\{(1, 0), (7, 0), (8, 1)\}$, $\{(3, 0), (4, 0), (6, 0)\}$, $\{(0, 0), (2, 1), \infty_1\}$, $\{(2, 0), (0, 1), \infty_2\}$,
$\{(1, 1), (7, 1), (8, 0)\}$, $\{(3, 1), (4, 1), (6, 1)\}$, $\{(5, 0), (9, 1), \infty_3\}$, $\{(9, 0), (5, 1), \infty_4\}]$.

5.35 Theorem The necessary conditions for the existence of a (k, λ)-RGDD of type h^u are (1) $u \ge k$, (2) $hu \equiv 0 \pmod k$, and (3) $\lambda h(u - 1) \equiv 0 \pmod{k - 1}$.

5.36 Theorem If there exist a (k, λ)-RGDD of type h^u and an $\mathrm{RTD}(k, m)$, then there exists a (k, λ)-RGDD of type $(mh)^u$.

5.37 Theorem Suppose that there is a (k, λ)-frame of type $T = [\ t_i : \ i = 1, 2, \ldots, n\ ]$. Suppose also that $t | t_i$ and that there exists a (k, λ)-RGDD of type $t^{1+t_i/t}$ for $i = 1, 2, \ldots, n$. Then there exists a (k, λ)-RGDD of type t^u where $u = 1 + \sum_{i=1}^{n} t_i/t$.

5.38 Theorem [1794] Suppose that there exist a (k, λ)-RGDD of type g^u, a (k, λ)-frame of type $(mg)^v$ where $u \ge m + 1$, and an $\mathrm{RTD}(k, mv)$. Then there exists a (k, λ)-RGDD of type $(mg)^{uv}$.

5.39 Theorem (Rees [1788]) Let $(V, \mathcal{G}, \mathcal{B})$ be an A-resolvable (k, λ)-GDD of type g^u in which for each $\alpha_i \in A$ there are r_i α_i-resolution classes of blocks. Suppose that there is a $\mathrm{TD}(u, h)$ admitting H as a group of automorphisms acting sharply transitively on the points of each group. Let H_j be a collection of subsets of H, there being r_i such subsets of size α_i for each $\alpha_i \in A$, and suppose that the collection $\{H_j * \delta : \delta \in H, j = 1, 2, \cdots, \sum_i r_i\}$ is resolvable on H. Then there is a (k, λ)-RGDD of type $(hg)^u$.

5.40 Theorem (Rees [1788]) If there exist an α-resolvable (k,λ)-GDD of type g^u and a TD(u,α), then there exists a (k,λ)-RGDD of type $(\alpha g)^u$.

5.41 Theorem [144, 848] If there exist $(k-2)/2$ SOLSSOM(n) with n even where the symmetric mate is unipotent and a $BF_\lambda(k,m)$ (see §II.7.2), then there exists a (k,λ)-RGDD of type m^n.

5.42 Theorem A $(2,\lambda)$-RGDD of type h^u exists if and only if hu is even.

5.43 Theorem [1788] A $(3,\lambda)$-RGDD of type h^u exists if and only if $u \geq 3$, $\lambda h(u-1)$ is even, $hu \equiv 0 \pmod 3$, and $(\lambda,h,u) \notin \{(1,2,6),(1,6,3)\} \cup \{(2j+1,2,3),(4j+2,1,6) : j \geq 0\}$.

5.44 Theorem [881] The necessary conditions for the existence of a 4-RGDD of type h^u, namely, $u \geq 4$, $hu \equiv 0 \pmod 4$ and $h(u-1) \equiv 0 \pmod 3$, are also sufficient except for $(h,u) \in \{(2,4),(2,10),(3,4),(6,4)\}$ and possibly excepting: $h = 2$ and $u \in \{34,46,52,70,82,94,100,118,130,142,178,184,202,214,238,250,334,346\}$; $h = 10$ and $u \in \{4,34,52,94\}$; $h \in [14,454] \cup \{478,502,514,526,614,626,686\}$ and $u \in \{10,70,82\}$; $h = 6$ and $u \in \{6,54,68\}$; $h = 18$ and $u \in \{18,38,62\}$; $h = 9$ and $u = 44$; $h = 12$ and $u = 27$; $h = 24$ and $u = 23$; and $h = 36$ and $u \in \{11,14,15,18,23\}$.

5.45 Theorem [868] The necessary conditions for the existence of a $(4,3)$-RGDD of type h^u, namely, $u \geq 4$ and $hu \equiv 0 \pmod 4$, are also sufficient except for $(h,u) \in \{(2,4),(2,6)\}$ and possibly excepting $(h,u) = (2,54)$.

5.46 Remark [2207] An α-resolvable $(3,\lambda)$-GDD of type h^u exists if and only if $u \geq 3$, $\lambda h(u-1) \equiv 0 \pmod 2$, $\lambda h^2 u(u-1) \equiv 0 \pmod 6$, $\alpha | \frac{\lambda h(u-1)}{2}$, $3 | \alpha hu$, and $(\alpha,\lambda,h,u) \notin \{(1,1,2,6),(1,1,6,3)\} \cup \{(1,2j+1,2,3),(1,4j+2,1,6) : j \geq 0\}$.

5.47 Remark A class-uniformly resolvable group divisible structure is a (K,λ)-GDD with its collection of blocks partitioned into (partial) resolution classes each having the same number of blocks of each size. Existence, constructions, and fundamental properties of class-uniformly resolvable group divisible structures can be found in [629, 630].

See Also

§II.7	More on frames and resolvable designs.
§III.5	SOLSSOMs can be utilized in constructions of frames and RGDDs via Theorems 5.27 and 5.41.
§VI.16	Block disjoint difference families can be utilized to construct frames, RBIBDs and RGDDs. See [1247].
§VI.64	Ordered whist tournament frames can be utilized in constructions of frames via Theorem 5.26.
[458]	Contains a general construction for double frames that can unify many known recursive constructions for frames.
[582]	Partitionable skew Room frames can be employed to construct 4-frames, and 4-frames can be used to construct HSOLSSOMs.
[848]	Survey of frames and resolvable structures. Also contains new techniques and results.

References Cited: [24, 31, 144, 458, 582, 629, 630, 848, 864, 868, 875, 881, 883, 1042, 1247, 1788, 1794, 1967, 2201, 2207]

6 Pairwise Balanced Designs as Linear Spaces

Anton Betten

6.1 Definitions and Examples

6.1 A *linear space* of order v is a PBD on v points with $\lambda = 1$ whose blocks have size at least 2. A linear space is *nontrivial* if it contains more than one block.

6.2 **Remark** It is customary to refer to elements as *points* and to blocks as *lines* when dealing with linear spaces, and theorems are often stated in this geometric language. In geometric terms, a linear space is a pair $(\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is a set of *points* and $\mathcal{B}$ is a collection of subsets of $\mathcal{P}$ (the *lines*) for which every pair of points is contained on exactly one line and every line contains at least two points.

6.3 Let L be a finite linear space. The *length of a line* is the number of points on it, and the *degree of a point* is the number of lines that pass through it.

6.4 **Remark** A linear space of order v whose lines have the same length k is a Steiner system $\mathrm{S}(2, k, v)$.

6.5 A finite linear space with $n \geq 3$ points is a *near pencil* if it contains one line consisting of $n-1$ points, and the remaining lines contain two points.

6.6 **Example** The lines of a near pencil on the 5 points $\{1, 2, 3, 4, 5\}$ are

$$\{1, 2, 3, 4\}, \{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}.$$

6.7 **Theorem** (de Bruijn and Erdős) [639] Let L be a nontrivial finite linear space with v points and b lines. Then $b \geq v$, with equality if and only if L is a finite projective plane, or L is a near-pencil.

6.8 **Remark** Every linear space is determined by its lines of size at least three. Simply add sufficiently many lines of size two to have all points connected.

6.9 If $\mathcal{B}$ is the set of lines of a linear space, $\mathcal{B}^{\#}$ denotes the set of lines of $\mathcal{B}$ that are of size at least three. $\mathcal{B}^{\#}$ is the *reduced line set*.

6.10 **Example** The near pencil of Example 6.6 has reduced line set $\mathcal{B}^{\#} = \{\{1, 2, 3, 4\}\}$.

6.11 A *proper linear space* is a linear space whose blocks have size at least 3. A *regular linear space* is a linear space such that for any k, the number of blocks of size k containing a point is constant for all points. A *proper regular linear space* is a proper linear space that is regular.

6.12 **Remark** A linear space is regular if and only if the lines of size k form a configuration for all k (see VI.7). In particular, for a regular linear space on v points with b_k lines of length k there are kb_k/v lines of length k through any point.

6.13 Let L be a finite linear space. Then L is *embeddable* in a projective plane of order n if there exists a projective plane π of order n with the property that L can be obtained by deleting points (and any resulting lines of length 0 and 1) from π.

6.2 Constructions

6.14 Let L be a finite linear space with v points and k_i blocks of size i for $2 \le k \le s$; then L has *type* $(v \mid 2^{k_2}, 3^{k_3}, \ldots, s^{k_s})$, where if $k_i = 0$, then i^{k_i} is omitted.

6.15 **Construction** If $v = ab$, then there is a regular linear space of type $(v \mid a^b, 2^c)$, where $c = \binom{v}{2} - b\binom{a}{2}$.

6.16 **Example** Because $12 = 3 \cdot 4 = 4 \cdot 3$, there are regular linear spaces of type $(12 \mid 4^3, 2^{48})$ and $(12 \mid 3^4, 2^{54})$.

6.17 **Construction** Let $2 < a < b$. An $a \times b$ *grid* is defined on the pointset $\{0, 1, \ldots, ab-1\}$ with the set $\mathcal{B}^{\#}$ of lines $\{0+ib, 1+ib, \ldots, b-1+ib\}$ and $\{0+j, b+j, 2b+j, \ldots, (a-1)b+j\}$ for $0 \le i < a$ and $0 \le j < b$. It is the reduced line set of a regular linear space of type $(ab \mid a^b, b^a, 2^c)$, with $c = \binom{ab}{2} - b\binom{a}{2} - a\binom{b}{2}$.

6.18 **Example** A 3×4 grid is a regular linear space of type $(12 \mid 4^3, 3^4, 2^{36})$.

6.19 **Construction** A configuration $v_r b_k$ (VI.7) with $k > 2$ gives rise to a regular linear space of type $(v \mid k^b, 2^a)$ where $a = \binom{v}{2} - b\binom{k}{2}$. The blocks of the configuration are just the elements of the set $\mathcal{B}^{\#}$ of the linear space. Conversely, a regular linear space with these parameters defines a configuration $v_r b_k$ where $r = bk/r$. This one-to-one correspondence induces a bijection of the corresponding isomorphism types.

6.20 **Construction** The dual of a configuration $v_r b_k$ is a configuration $b_k v_r$, with exchanged roles of v and b and of r and k. Thus, a configuration $v_r b_k$ also gives rise to a regular linear space of type $(b \mid r^v, 2^c)$, where $c = \binom{b}{2} - v\binom{r}{2}$.

6.21 An r-regular graph on v points, denoted as $\mathcal{R}(v, r)$, is a configuration $v_r b_2$.

6.22 **Construction** By Construction 6.20, an r-regular graph on n vertices gives rise to a regular linear space of type $(nr/2 \mid r^n, 2^c)$, where $c = \frac{nr}{2}(r(n-4)+2)$, and conversely. In particular, a cubic graph on n vertices (n even) corresponds to a regular linear space of type $(3n/2 \mid 3^n, 2^c)$, where $c = 3n(3n-10)/8$, and conversely.

6.23 **Remark** Let K_n denote the complete graph on n vertices (which is regular of degree $n-1$). Then Constructions 6.19 and 6.22 give regular linear spaces of type $\left(n \mid 2^{\binom{n}{2}}\right)$ and $\left(\binom{n}{2} \mid (n-1)^n, 2^c\right)$, where $c = \binom{\binom{n}{2}}{2} - n\binom{n-1}{2} = \frac{n(n-1)}{8}((n-1)(n-4)+2)$.

6.24 **Construction** Let L be a latin square of side $n > 3$ (abbreviated LS(n)) with symbol set $\{0, \ldots, n-1\}$. Define a regular linear space of type $(3n \mid n^3, 3^{n^2})$ as follows. The three lines of length n are the sets $\{1, 2, \ldots, n\}$, $\{n+1, \ldots, 2n\}$, and $\{2n+1, \ldots, 3n\}$. For any pair i, j with $1 \le i, j \le n$, define a line $\{i, n+j, 2n+1+L(i,j)\}$. Conversely, a regular linear space of type $(3n \mid n^3, 3^{n^2})$ determines a latin square of side n. The isomorphism types of linear spaces of this line type correspond in a one-to-one manner to the main classes of latin squares of side n.

6.25 **Example** The two main classes of latin squares of side 4 (from Table III.1.18) give rise to the linear spaces of type $(12 \mid 4^3, 3^{12})$ with block sets:
$\{\{1,2,3,4\}, \{5,6,7,8\}, \{9,10,11,12\}, \{1,5,9\}, \{1,6,10\}, \{1,7,11\}, \{1,8,12\}, \{2,5,10\}, \{2,6,9\}, \{2,7,12\}, \{2,8,11\}, \{3,5,11\}, \{3,6,12\}, \{3,7,9\}, \{3,8,10\}, \{4,5,12\}, \{4,6,11\}, \{4,7,10\}, \{4,8,9\}\}$ and $\{\{1,2,3,4\}, \{5,6,7,8\}, \{9,10,11,12\}, \{1,5,9\}, \{1,6,10\}, \{1,7,11\}, \{1,8,12\}, \{2,5,10\}, \{2,6,9\}, \{2,7,12\}, \{2,8,11\}, \{3,5,11\}, \{3,6,12\}, \{3,7,10\}, \{3,8,9\}, \{4,5,12\}, \{4,6,11\}, \{4,7,9\}, \{4,8,10\}\}$.

6.26 For q and n integers, $\theta_n(q) = \frac{q^{n+1}-1}{q-1} = 1 + q + q^2 + \cdots + q^n = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$ where $\begin{bmatrix} d \\ i \end{bmatrix}_q$ denotes the gaussian coefficient (see Proposition VII.2.34).

6.27 **Construction** Let $\mathcal{P}$ and $\mathcal{B}$ be the set of points and lines of $\mathrm{PG}(n,q)$. The incidence structure $(\mathcal{P},\mathcal{B})$ forms a configuration of type $v_r b_k$ where $v = \theta_n(q)$, $r = \theta_{n-1}(q)$, $b = \theta_n(q)\theta_{n-1}(q)/(q+1)$, and $k = q+1$. By Construction 6.19, this is a regular linear space of type $\left(v \mid k^b\right) = \left(\theta_n(q) \mid (q+1)^{\theta_n(q)\theta_{n-1}(q)/(q+1)}\right)$, but not every regular linear space of this type is obtained by this construction. If $q = 2$, an $\mathrm{STS}(\theta_n(2))$ results. If $q = 3$, an $\mathrm{SQS}(\theta_n(3))$ results. By Construction 6.20, the dual configuration yields a regular linear space of type $(b \mid r^v, 2^c)$, where $c = \binom{b}{2} - v\binom{r}{2}$. If $n = 2$, both constructions yield isomorphic linear spaces.

6.28 **Examples** Linear spaces from projective geometries.

$\mathrm{PG}(n,q)$	Points vs. Lines	Lines vs. Points
$\mathrm{PG}(2,2)$	$(7 \mid 3^7) \simeq \mathrm{STS}(7)$	$(7 \mid 3^7)$
$\mathrm{PG}(3,2)$	$(15 \mid 3^{35}) \simeq \mathrm{STS}(15)$	$(35 \mid 7^{15}, 2^{280})$
$\mathrm{PG}(4,2)$	$(31 \mid 3^{155}) \simeq \mathrm{STS}(31)$	$(155 \mid 15^{31}, 2^{8680})$
$\mathrm{PG}(2,3)$	$(13 \mid 4^{13}) \simeq \mathrm{SQS}(13)$	$(13 \mid 4^{13})$
$\mathrm{PG}(3,3)$	$(40 \mid 4^{130}) \simeq \mathrm{SQS}(40)$	$(130 \mid 13^{40}, 2^{5265})$
$\mathrm{PG}(2,4)$	$(21 \mid 5^{21})$	$(21 \mid 5^{21})$
$\mathrm{PG}(3,4)$	$(85 \mid 5^{357})$	$(357 \mid 21^{85}, 2^{45696})$
$\mathrm{PG}(2,5)$	$(31 \mid 6^{31})$	$(31 \mid 6^{31})$

6.29 **Remark** Construction 6.27 may be applied to arbitrary projective planes of order n, 2-$(n^2+n+1, n+1, 1)$ designs. In this case, the resulting regular linear spaces obtained from the plane and its dual always have the same parameters but may or may not be isomorphic. They are isomorphic precisely if the plane is self-dual. The smallest non self-dual projective plane has order $n = 9$ (see VII.2).

6.30 **Construction** Let $\mathcal{P}$ and $\mathcal{B}$ be the set of points and lines of $\mathrm{AG}(n,q)$. The incidence structure $(\mathcal{P},\mathcal{B})$ forms a configuration of type $v_r b_k$ where $v = q^n$, $r = \theta_{n-1}(q)$, $b = q^{n-1}\theta_{n-1}(q)$, and $k = q$. By Construction 6.19, it is a regular linear space of type $\left(v \mid k^b\right) = \left(q^n \mid q^{q^{n-1}\theta_{n-1}(q)}\right)$, but not every regular linear space of this type is obtained by this construction. If $q = 2$, a complete graph on 2^n vertices results. By Construction 6.20, the dual configuration yields a regular linear space of type $(b \mid r^v, 2^c)$, where $c = \binom{b}{2} - v\binom{r}{2}$.

6.31 **Examples** Linear spaces from affine geometries.

$\mathrm{AG}(n,q)$	Points vs. Lines	Lines vs. Points
$\mathrm{AG}(2,2)$	$(4 \mid 2^6) \simeq K_4$	$(6 \mid 3^4, 2^3)$
$\mathrm{AG}(3,2)$	$(8 \mid 2^{28}) \simeq K_8$	$(28 \mid 7^8, 2^{210})$
$\mathrm{AG}(4,2)$	$(16 \mid 2^{120}) \simeq K_{16}$	$(120 \mid 15^{16}, 2^{120})$
$\mathrm{AG}(2,3)$	$(9 \mid 3^{12})$	$(12 \mid 4^9, 2^{12})$
$\mathrm{AG}(3,3)$	$(27 \mid 3^{117})$	$(117 \mid 13^{27}, 2^{4680})$
$\mathrm{AG}(2,4)$	$(16 \mid 4^{20})$	$(20 \mid 5^{16}, 2^{30})$
$\mathrm{AG}(3,4)$	$(64 \mid 4^{336})$	$(336 \mid 21^{64}, 2^{42840})$
$\mathrm{AG}(2,5)$	$(25 \mid 5^{30})$	$(30 \mid 6^{25}, 2^{60})$

6.3 Enumeration

6.32 **Table** [227, 232] The number of nonisomorphic linear spaces of order v. $\mathrm{LIN}(v)$,

PLIN(v), RLIN(v), and PRLIN(v) denote the number of order v nonisomorphic linear spaces, proper linear spaces, regular linear spaces, and proper regular linear spaces, respectively.

v	LIN(v)	PLIN(v)	RLIN(v)	PRLIN(v)
2	1	0	1	0
3	2	0	2	0
4	3	0	2	0
5	5	0	2	0
6	10	0	4	0
7	24	1	3	1
8	69	0	4	0
9	384 [744]	1	9	1
10	5250 [911]	1	14	0
11	232929 [243, 1744]	1	33	0
12	28872973 [228]	3	839	3
13	?	7	2041	3
14	?	1	22192	0
15	?	119 [337, 1276]	≥ 245773	84
16	?	398 [1069]	≥ 3306477	25
17	?	161925 [229]	?	0
18	?	2412890 [231]	?	12
19	?	?	?	11084874886

6.33 **Table** The regular linear spaces on ≤ 19 points. $\mathcal{R}_{n,k}$ denotes k-regular graphs on n vertices, dually; $\mathcal{RP}_{n,k}$ denotes the duals of k-regular graphs with a parallel class on n vertices, dually. Dual mesh is abbreviated dm; derived is abbreviated der; and pc indicates 'with a parallel class'.

Parameters	#	Comment	Parameters	#	Comment
$(2\|1)$	1	one line			
$(3\|2)$	1	one line	$(3\|2^3)$	1	K_3
$(4\|4)$	1	one line	$(4\|2^6)$	1	K_4
$(5\|5)$	1	one line	$(5\|2^{10})$	1	K_5
$(6\|6)$	1	one line	$(6\|2^33^4)$	1	K_4 dually
$(6\|2^93^2)$	1	2 disjoint 3-lines	$(6\|2^{15})$	1	K_6
$(7\|7)$	1	one line	$(7\|3^7)$	1	PG$(2,2)$ or 7_3
$(7\|2^21)$	1	K_7			
$(8\|8)$	1	one line	$(8\|2^43^8)$	1	der AG$(2,3)$ or 8_3
$(8\|2^{16}4^2)$	1	2 disjoint 4-lines	$(8\|2^{28})$	1	K_8
$(9\|9)$	1	one line	$(9\|3^{12})$	1	AG$(2,3)$
$(9\|2^93^9)$	3	9_3	$(9\|2^{18}3^6)$	2	$\mathcal{R}_{6,3}$ or der LS(4)
$(9\|2^{27}3^3)$	1	3 disjoint 3-lines	$(9\|2^{36})$	1	K_9
$(10\|10)$	1	one line	$(10\|2^{15}4^5)$	1	K_5 dually
$(10\|2^{15}3^{10})$	10	10_3 [244]	$(10\|2^{25}5^2)$	1	2 disjoint 5-lines
$(10\|2^{45})$	1	K_{10}			
$(11\|11)$	1	one line	$(11\|2^{22}3^{11})$	31	11_3
$(11\|2^{55})$	1	K_{11}			
$(12\|12)$	1	one line	$(12\|3^44^9)$	1	der PG$(2,3)$
$(12\|3^{16}4^3)$	2	LS(4)	$(12\|2^63^84^6)$	1	
$(12\|2^63^{20})$	5	der STS(13)	$(12\|2^{12}4^9)$	1	AG$(2,3)$, dually
$(12\|2^{12}3^{12}4^3)$	4	12_3 pc; der LS(5)	$(12\|2^{18}3^44^6)$	1	
$(12\|2^{18}3^{16})$	574	12_416_3	$(12\|2^{24}3^84^3)$	8	$\mathcal{RP}_{8,3}$
$(12\|2^{30}4^6)$	1	$\mathcal{R}_{6,4}$	$(12\|2^{30}3^{12})$	229	12_3
$(12\|2^{36}6^2)$	1	2 disjoint 6-lines	$(12\|2^{36}3^44^3)$	1	3×4 grid
$(12\|2^{42}3^8)$	6	$\mathcal{R}_{8,3}$	$(12\|2^{48}4^3)$	1	3 disjoint 4-lines
$(12\|2^{54}3^4)$	1	4 disjoint 3-lines	$(12\|2^{66})$	1	K_{12}
$(13\|13)$	1	one line	$(13\|4^{13})$	1	PG$(2,4)$ or 13_4
$(13\|3^{26})$	2	STS(13)	$(13\|2^{39}3^{13})$	2036	13_3[979]
$(13\|2^{78})$	1	K_{13}			

Parameters	#	Comment	Parameters	#	Comment
$(14\|14)$	1	one line	$(14\|2^7 4^{14})$	1	14_4 [230]
$(14\|2^7 3^{28})$	787	der STS(15)	$(14\|2^{49} 7^2)$	1	2 disjoint 7-lines
$(14\|2^{49} 4^7)$	2		$(14\|2^{49} 3^{14})$	21399	14_3
$(14\|2^{91})$	1	K_{14}			
$(15\|15)$	1	one line	$(15\|3^5 4^{15})$	1	der AG$(2,4)$
$(15\|3^{15} 5^6)$	1	$\binom{15}{2}$+15 parallel classes 2+2+2 (dually)	$(15\|3^{25} 5^3)$	2	LS(5)
$(15\|3^{35})$	80	STS(15)	$(15\|2^{15} 4^{15})$	4	15_4 [230]
$(15\|2^{15} 3^{10} 5^6)$	1		$(15\|2^{15} 3^{20} 5^3)$	40	15_3 pc; der LS(6)
$(15\|2^{15} 3^{30})$	10177328	$15_6 30_3$	$(15\|2^{30} 3^5 5^6)$	1	
$(15\|2^{30} 3^{15} 5^3)$	251		$(15\|2^{30} 3^{25})$	≥ 1	$15_5 25_3$
$(15\|2^{45} 5^6)$	1	K_6 dually	$(15\|2^{45} 3^{10} 5^3)$	23	
$(15\|2^{45} 3^{20})$	≥ 1	$15_4 20_3$	$(15\|2^{60} 3^5 5^3)$	1	3×5 grid
$(15\|2^{60} 3^{15})$	245342	15_3	$(15\|2^{75} 5^3)$	1	3 disjoint 5-lines
$(15\|2^{75} 3^{10})$	21	$\mathcal{R}_{10,3}$	$(15\|2^{90} 3^5)$	1	5 disjoint 3-lines
$(15\|2^{105})$	1	K_{15}			
$(16\|16)$	1	one line	$(16\|4^{20})$	1	AG$(2,4)$
$(16\|3^{16} 4^{12})$	1		$(16\|3^{32} 4^4)$	23	see [828]
$(16\|2^{24} 4^{16})$	19	16_4 [230]	$(16\|2^{24} 3^{16} 4^8)$	300880	
$(16\|2^{24} 3^{32})$	≥ 1	$16_6 32_3$	$(16\|2^{48} 4^{12})$	574	$16_3 12_4$
$(16\|2^{48} 3^{16} 4^4)$	88	16_3 pc	$(16\|2^{64} 8^2 2)$	1	2 disjoint 8-lines
$(16\|2^{72} 4^8)$	6	$\mathcal{R}_{8,4}$	$(16\|2^{72} 3^{16})$	3004881	16_3 [233]
$(16\|2^{96} 4^4)$	1	4 disjoint 4-lines	$(16\|2^{120})$	1	K_{16}
$(17\|17)$	1	one line	$(17\|2^{34} 4^{17})$	1972	17_4 [230]
$(17\|2^{34} 3^{34})$	≥ 1		$(17\|2^{85} 3^{17})$	38904499	17_3 [233]
$(17\|2^{136})$	1	K_{17}			
$(18\|18)$	1	one line	$(18\|3^{36} 6^3)$	12	dm$(36,6,3)$ [242]
$(18\|2^9 3^{12} 4^{18})$	77		$(18\|2^9 3^{30} 4^9)$	≥ 1	
$(18\|2^9 3^{48})$	210611385743	der STS(19); see Table VI.7.18	$(18\|2^{18} 3^{30} 6^3)$	4260	dm$(30,5,3)$
$(18\|2^{27} 3^6 4^{18})$	≥ 1		$(18\|2^{27} 3^{24} 4^9)$	≥ 1	
$(18\|2^{27} 3^{42})$	≥ 1		$(18\|2^{36} 3^{24} 6^3)$	≥ 1	dm$(24,4,3)$
$(18\|2^{45} 4^{18})$	971171	18_4 [230]	$(18\|2^{45} 3^{18} 4^9)$	≥ 1	
$(18\|2^{45} 3^{36})$	≥ 1		$(18\|2^{54} 3^{18} 6^3)$	568	dm$(18,3,3)$
$(18\|2^{63} 3^{12} 4^9)$	≥ 1		$(18\|2^{63} 3^{30})$	≥ 1	
$(18\|2^{72} 3^{12} 6^3)$	157	dm$(12,2,3)$	$(18\|2^{81} 9^2)$	1	
$(18\|2^{81} 3^6 4^9)$	150373		$(18\|2^{81} 3^{24})$	≥ 1	
$(18\|2^{90} 3^6 6^3)$	1	3×6 grid	$(18\|2^{99} 4^9)$	16	$\mathcal{R}_{9,4}$
$(18\|2^{99} 3^{18})$	530425205	18_3 [233]	$(18\|2^{108} 6^3)$	1	3 disjoint 6-lines
$(18\|2^{117} 3^{12})$	94	$\mathcal{R}_{12,3}$	$(18\|2^{135} 3^6)$	1	6 disjoint 3-lines
$(18\|2^{153})$	1	K_{18}			
$(19\|19)$	1	one line	$(19\|3^{19} 4^{19})$	56	
$(19\|3^{57})$	11084874829	STS(19) [1268]	$(19\|2^{57} 4^{19})$	≥ 1	19_4
$(19\|2^{57} 3^{38})$	≥ 1		$(19\|2^{114} 3^{19})$	≥ 1	19_3
$(19\|2^{171})$	1	K_{19}			

See Also

§II.1	BIBDs of index one give linear spaces.
§VI.7	Regular linear spaces give configurations for each block size.
§VII.2	Linear spaces are simple finite geometries.
[164]	A text dedicated to finite linear spaces.
[1597]	Treats the question of embeddability in projective spaces.

References Cited: [164, 227, 228, 229, 230, 231, 232, 233, 242, 243, 244, 337, 639, 744, 828, 911, 979, 1069, 1268, 1276, 1597, 1744]

Part V

Hadamard Matrices and Related Designs

1 Hadamard Matrices and Hadamard Designs

Robert Craigen
Hadi Kharaghani

1.1 Definitions and Examples

1.1 An $n \times n$ (± 1)-matrix H is a *Hadamard matrix* if $HH^T = nI$ (that is, its rows are pairwise orthogonal). H(n) denotes a Hadamard matrix of order n.

1.2 **Examples** H(n) for $n \in \{2, 4, 8\}$. ("$-$" represents -1 in arrays in this entire part).

$$A = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{pmatrix}$$

1.3 Two Hadamard matrices are *equivalent* if one can be transformed into the other by a series of row or column permutations or negations. A Hadamard matrix is *normalized* if all entries in its first row and first column are 1.

1.4 **Remark** Every Hadamard matrix is equivalent to a normalized one. This $H(4)$ is equivalent to the normalized Hadamard matrix B in Examples 1.2.

$$\begin{pmatrix} 1 & - & 1 & 1 \\ 1 & - & - & - \\ - & - & 1 & - \\ 1 & 1 & 1 & - \end{pmatrix}$$

1.5 A *Hadamard design* is a symmetric $(4n-1, 2n-1, n-1)$ block design. A *Hadamard 3-design* (see §II.6) is a 3-$(4n, 2n, 2n-1)$. The *core* of a normalized Hadamard matrix is the submatrix obtained by deleting its first row and column.

1.6 **Proposition** The core of a normalized $H(4n)$, $n > 1$, is the (± 1)-incidence matrix of a Hadamard design. Conversely, given the (± 1)-incidence matrix of a Hadamard design, a Hadamard matrix is obtained by adding a row and a column of all $+1$s.

1.7 **Construction** A Hadamard 3-design can be constructed from a normalized H$(4n)$. Write $H'(4n)$ for the $4n \times (4n-1)$ submatrix by deleting the first column of $H(4n)$. The augmented matrix $(H(4n)|-H'(4n))$ is the (± 1)-incidence matrix of the Hadamard 3-design. Conversely, the derived design of a Hadamard 3-design is a Hadamard design.

1.2 Special Types of Hadamard Matrices

1.8 A Hadamard matrix H is *skew-type* if $H = A + I$, where $A^T = -A$ and I is the identity matrix. H is *graphical* if it is symmetric and has constant diagonal.

1.9 **Remark** $A + I$ is a skew-type Hadamard matrix if and only if A is a skew conference matrix (see §V.2).

1.10 A Hadamard matrix H is *regular* if its row and column sums are constant. A *Menon design* is a symmetric $(4u^2, 2u^2 \pm u, u^2 \pm u)$ block design.

1.11 **Examples** P is a skew-type H(12); Q is a graphical H(16):

$$P = \begin{pmatrix}
1&-&-&-&-&-&-&-&-&-&-&-\\
1&1&1&-&1&1&1&-&-&-&1&-\\
1&-&1&1&-&1&1&1&-&-&-&1\\
1&1&-&1&1&-&1&1&1&-&-&-\\
1&-&1&-&1&1&-&1&1&1&-&-\\
1&-&-&1&-&1&1&-&1&1&1&-\\
1&-&-&-&1&-&1&1&-&1&1&1\\
1&1&-&-&-&1&-&1&1&-&1&1\\
1&1&1&-&-&-&1&-&1&1&-&1\\
1&1&1&1&-&-&-&1&-&1&1&-\\
1&-&1&1&1&-&-&-&1&-&1&1\\
1&1&-&1&1&1&-&-&-&1&-&1
\end{pmatrix}
\qquad
Q = \begin{pmatrix}
1&1&1&1&1&-&-&1&1&-&1&-&1&1&-&-\\
1&1&1&1&-&1&1&-&-&1&-&1&1&1&-&-\\
1&1&1&1&-&1&1&-&1&-&1&-&-&-&1&1\\
1&1&1&1&1&-&-&1&-&1&-&1&-&-&1&1\\
1&-&-&1&1&1&1&1&1&1&-&-&1&-&1&-\\
-&1&1&-&1&1&1&1&1&1&-&-&-&1&-&1\\
-&1&1&-&1&1&1&1&-&-&1&1&1&-&1&-\\
1&-&-&1&1&1&1&1&-&-&1&1&-&1&-&1\\
1&-&1&-&1&1&-&-&1&1&1&1&1&-&-&1\\
-&1&-&1&1&-&-&1&1&1&1&1&-&-&1&-\\
1&-&1&-&-&-&1&1&1&1&1&1&-&1&1&-\\
-&1&-&1&-&-&1&1&1&1&1&1&1&-&-&1\\
1&1&-&-&1&-&1&-&1&-&-&1&1&1&1&1\\
1&1&-&-&-&1&-&1&1&-&1&1&1&1&1&1\\
-&-&1&1&1&-&1&-&-&1&-&1&1&1&1&1\\
-&-&1&1&-&1&-&1&1&-&-&1&1&1&1&1
\end{pmatrix}.$$

1.12 **Proposition** There is a Menon design on n points if and only if there is a regular $H(n)$. If H is a regular $H(n)$, where $n = 4u^2$, then one of H, $-H$ is the incidence matrix of a Menon design with parameters $(4u^2, 2u^2 + u, u^2 + u)$ and the other is the incidence matrix of its dual, which has parameters $(4u^2, 2u^2 - u, u^2 - u)$.

1.13 A Hadamard matrix of order n^2 is *Bush-type* if it is partitioned into n^2 blocks of size $n \times n$, all row and column sums of every nondiagonal block are 0, and for diagonal blocks, these sums are equal to n.

1.14 **Construction** From a normalized H(n) with rows $h_1, h_2, \ldots, h_n$, a graphical Bush-type Hadamard matrix of order n^2 is obtained by arranging blocks $h_1^T h_1, h_2^T h_2, \ldots, h_n^T h_n$ in an $n \times n$ symmetric latin square with constant diagonal (which is where $h_1^T h_1$ goes).

1.15 **Remark** Bush-type Hadamard matrices are regular. The matrix Q in Examples 1.11 is a Bush-type matrix obtained by Construction 1.14 from B in Examples 1.2.

1.16 **Example** Circulant Hadamard matrices are also regular. The only known nontrivial circulant Hadamard matrix is the H(4) generated by first row $(-, 1, 1, 1)$.

1.3 Necessary Conditions

1.17 **Theorem** If there is an H(n), then $n = 1$, 2, or $4k$, where k is a positive integer.

1.18 **Theorem** If there is a regular or graphical H(n), then n is a square.

1.19 **Remarks** Theorem 1.17 follows for $n \geq 3$, by considering any three rows. The first case of Theorem 1.18 follows from Proposition 1.12, the second case because the eigenvalues must be $\pm\sqrt{n}$.

1.4 Some Conjectures

1.20 **Conjecture** (Hadamard [1003]) H(n) exists if and only if $n = 1$, 2, or $4k$.

1.21 **Conjecture** (Seberry) A skew-type H(n) exists if and only if $n = 1$, 2, or $4k$.

1.22 Conjecture (Ryser) If $n > 4$, then there is no circulant H(n).

1.23 Conjecture For any order $4k^2$, there exists

1. a regular Hadamard matrix,
2. a graphical Hadamard matrix,
3. a regular Hadamard matrix equivalent to a graphical Hadamard matrix,
4. a regular graphical Hadamard matrix, and
5. a Bush-type Hadamard matrix.

1.24 Conjecture (Wallis, Lin) If an H(n) exists, then so do

1. a symmetric H(n) and
2. a skew-type H(n) equivalent to a symmetric H(n).

1.25 Remarks Conjecture 1.20 is confirmed for $n < 668$; Conjecture 1.21 for $n < 188$; Conjecture 1.22 for $n < 548964900 (= 4 \cdot 11715^2)$ [1430]; Conjecture 1.23 for $k < 47$ (case 1), $k < 45$ (cases 2–4), $k < 7$ (case 5); case 1 of Conjecture 1.24 for $n < 92$, and case 2 for $n < 36$. There is a regular H(36) that is not equivalent to a graphical one; there is an H(28) that is skew-type but not equivalent to a symmetric one and an H(28) that is symmetric but not equivalent to a skew-type one. There exists an H(24) that is equivalent to its transpose, but not to a symmetric matrix.

1.5 Existence

1.26 If $M = (m_{ij})$ is an $a \times b$ matrix and $N = (n_{ij})$ is a $c \times d$ matrix, then the *Kronecker product* $M \otimes N$ is the $ac \times bd$ matrix given by

$$M \otimes N = \begin{bmatrix} m_{11}N & m_{12}N & \cdots & m_{1b}N \\ m_{21}N & m_{22}N & \cdots & m_{2b}N \\ \vdots & & & \vdots \\ m_{a1}N & m_{a2}N & \cdots & m_{ab}N \end{bmatrix}$$

1.27 Proposition [1997] If H is an H(m) and K is an H(n), then $H \otimes K$ is an H(mn).

1.28 Remarks In Examples 1.2, $C = A \otimes B$. Observe that H(n) implies H($2^t n$) for all $t \in \mathbb{Z}^+$. For this reason the key question of existence for Hadamard matrices is considered to be the minimum value of t, for each odd $p \geq 1$, such that H($2^t p$) exists.

1.29 Theorem [65, 615] Given H(n) for $n = 4a, 4b, 4c, 4d$, there exists an H($8ab$) and an H($16abcd$).

1.30 Remark The first part of Theorem 1.29 does not imply the second part. It is stronger than Proposition 1.27.

1.31 Theorem Suppose there is a conference matrix (see §V.2.1) of order n, and $k \in \mathbb{Z}^+$.

1. If $n \equiv 0 \pmod 4$, then there is an H($n(n-1)^k$);
2. If $n \equiv 0 \pmod 4$ and k is odd, there is a skew-type H($(n-1)^k + 1$);
3. If $n \equiv 2 \pmod 4$, then there is an H($2n(n-1)^k$);
4. If $n \equiv 2 \pmod 4$ or k is even, then there is a graphical H($2((n-1)^k + 1)$).

1.32 Remark Parts 2 and 4 of Theorem 1.31 give H($q+1$) or H($2(q+1)$) when q is a prime power $\equiv 3$ or $1 \pmod 4$, respectively. In Example 1.2, B is obtained from a conference matrix of order 3 in this fashion.

1.33 **Examples** The *Williamson* and *Goethals–Seidel* arrays:

$$W = \begin{pmatrix} A & -B & -C & -D \\ B & A & -D & C \\ C & D & A & -B \\ D & -C & B & A \end{pmatrix}, \quad G = \begin{pmatrix} A & -BR & -CR & -DR \\ BR & A & -D^TR & C^TR \\ CR & D^TR & A & -B^TR \\ DR & -C^TR & B^TR & A \end{pmatrix}.$$

1.34 A matrix is *type I* or *type II* (relative to group G) if it has the same form as the division table of G or, respectively, the multiplication table of G. (Elsewhere type I/II matrices are known as *group developed*, *group-invariant*, *group matrices* and various other things.) When used together, all type I/II matrices are relative to the same group G.

1.35 **Examples** Circulant matrices are type I, and back-circulant matrices are type II, relative to a cyclic group. If the group is abelian, then all type I matrices commute with each other and are amicable to type II matrices. If A is type I and R is type II, then AR is type II:

$$A = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \qquad R = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}; \quad AR = \begin{pmatrix} c & b & a \\ b & a & c \\ a & c & b \end{pmatrix}$$

circulant (type I) back circulant (type II)

1.36 $n \times n$ (± 1)-matrices A, B, C, D such that $AA^T + BB^T + CC^T + DD^T = 4nI$ are

1. *Williamson matrices* if they are symmetric and circulant,
2. *Williamson-type matrices* if they are pairwise amicable (see §2.1), or
3. *Goethals–Seidel type matrices* if they are type I.

1.37 **Construction** Replacing variables of W (from Examples 1.33) with Williamson matrices A, B, C, D of order n gives an H$(4n)$.

1.38 **Remark** Williamson matrices are known for all orders $n \leq 63$, except when $n \in \{35, 47, 53\}$, for which orders the array does not exist, and $n = 59$, which is unresolved. Williamson matrices are both Williamson-type and Goethals–Seidel type.

1.39 **Examples** The first rows of Williamson matrices A, B, C, D of orders $n = 5, 7, \ldots, 19$.

5
1 − − − −
1 − − − −
1 1 − − 1
1 − 1 1 −

7
1 − − − − − −
1 1 − − − − 1
1 − 1 − − 1 −
1 − − 1 1 − −

9
1 1 − − − − − − 1
1 − 1 − − − − 1 −
1 − − 1 − − 1 − −
1 − − − 1 1 − − −

11
1 − 1 1 − − − − 1 1 −
1 1 − 1 1 − − 1 1 − 1
1 1 − 1 − 1 1 − 1 − 1
1 1 − − − − − − − − 1

13
1 − 1 − − 1 1 1 1 − − 1 −
1 − − − 1 1 1 1 1 − − −
1 1 − 1 − − 1 1 − − 1 − 1
1 − − − − 1 − − 1 − − − −

15
1 1 − 1 1 − 1 − − 1 − 1 1 − 1
1 1 − 1 1 1 1 − − 1 1 1 1 − 1
1 1 − 1 1 − − − − − − 1 1 − 1
1 − 1 − − − 1 1 1 1 − − − 1 −

17
1 − 1 1 − 1 1 1 − − 1 1 1 − 1 1 −
1 − − 1 − 1 1 1 1 1 1 1 1 − 1 − −
1 1 − 1 − − − 1 − − 1 − − − 1 − 1
1 − − − 1 1 1 − − − − 1 1 1 − − −

19
1 1 − − 1 − 1 1 1 1 1 1 1 1 − 1 − − 1
1 − 1 − − − 1 1 1 1 1 1 1 1 − − − 1 −
1 1 − 1 1 − − 1 − 1 1 − 1 − − 1 1 − 1
1 1 − − 1 1 1 − 1 − − 1 − 1 1 1 − − 1

1.40 **Construction** Replacing variables of an OD$(4n; n, n, n, n)$ (see §V.2) with Williamson-type matrices A, B, C, D of order m gives an H$(4mn)$.

1.41 **Construction** [919] Replacing variables of G (from Examples 1.33) with Goethals–Seidel type matrices A, B, C, D, and R with any type II monomial matrix, gives an H($4n$). If $A = I + S$, $S^T = -S$, then the H($4n$) is skew-type.

1.42 **Remark** Turyn type sequences (see §V.8.4) of lengths 56, 56, 56, 55 would give Goethals–Seidel type matrices of order 167 and so H(668), the first unresolved order. This may be the currently most promising approach to this order, see [1287].

1.43 **Theorem** Let n be an odd positive integer whose binary expansion has N nonzero digits. There exists a Hadamard matrix of order $2^t n$ when:

1. $n \equiv 1 \pmod 4$ and $t \geq 2N$; or
2. $n \equiv 3 \pmod 4$ and $t \geq 2N - 1$; or
3. $t \geq 6 \left\lfloor \frac{\log_2 \frac{n-1}{2}}{16} \right\rfloor + 2$.

1.44 **Theorem** [1906] If there is a BIBD$(u(2u-1), 4u^2-1, 2u+1, u, 1)$, then there is a regular graphical Hadamard matrix of order u^2.

1.45 **Theorem** [2172] If q is a prime power, $q \not\equiv 7 \pmod 8$, then there exists a regular H($4q^2$).

1.46 **Theorem** [1660] If $q \in \mathbb{Z}^+$ is odd, then there exists a graphical Bush-type H($4q^4$).

1.47 **Remark** A Bush-type $H(4q^2)$ with odd nonsquare q is known only for $q = 3$ and 5.

1.48 **Theorem** If $n+1$ and $n-1$ are both odd prime powers, then there exists a symmetric regular H(n^2).

1.49 **Table** The number of equivalence classes of Hadamard matrices of order n, $4 \leq n \leq 40$.

n	4	8	12	16	20	24	28	32	36	40
#	1	1	1	5	3	60	487	> 3600000	> 15000000	> 366000000000

1.50 **Table** $n < 300$ for which Williamson-type matrices of order n are not known.

47, 59, 65, 67, 77, 103, 105, 107, 111, 119, 133, 143, 151, 155, 151, 155, 161, 163, 167, 171, 179, 183, 185, 191, 203, 207, 209, 215, 219, 221, 223, 227, 237, 245, 247, 249, 251, 253, 259, 267, 273, 275, 283, 287, 291, 299

1.51 **Table** Odd $n < 500$ for which a skew-type Hadamard matrix of order $4n$ is not known (t in brackets, when provided, indicates that one of order $2^t n$ is known).

47(4), 63(3), 89(4), 97(9), 101(10), 107(10), 109(9), 119(4), 145(5), 149(4), 153(3), 167(4), 177(12), 179(8), 191, 193(3), 201(3), 205(3), 209(4), 213(4), 223(3), 225(4), 229(3), 233(4), 235(3), 239(4), 245(4), 247(6), 249(4), 251(6), 253(4), 257(4), 259(5), 261(3), 265(4), 269(8), 275(4), 277(5), 283(11), 285(3), 287(4), 289(3), 295(5), 299(4), 301(3), 303(3), 305(4), 309(3), 311(26), 317(6), 319(3), 325(5), 329(6), 331(3), 335(7), 337(18), 341(4), 343(6), 345(4), 347(18), 349(3), 353(4), 359(4), 361(3), 369(4), 373(7), 377(6), 385(3), 389(15), 391(4), 397(5), 401(10), 403(5), 409(3), 413(4), 419(4), 423(4), 429(3), 433(3), 435(4), 441(3), 443(6), 445(3), 449, 451(3), 455(4), 457(9), 459(3), 461(17), 465(3), 469(3), 473(5), 475(4), 479(12), 481(3), 485(4), 487(5), 489(3), 491(46), 493(3)

1.52 **Table** Odd $n < 200$ for which a symmetric Hadamard matrix of order $4n$ is not known (t in brackets, when provided, indicates that one of order $2^t n$ is known).

23(4), 29(4), 39(3), 43(3), 47(4), 59(12), 65(3), 67(5), 73(7), 81(3), 89(4), 93(3), 101(10), 103(3), 107(10), 109(9), 113(8), 119(3), 127(25), 133(3), 149(4), 151(5), 153(3), 163(3), 167(4), 179(8), 183(3), 189(3), 191, 193(3)

1.53 **Table** Values of t such that a Hadamard matrix of order $2^t n$ is known, for odd $n < 9999$ (n is obtained by adding the three indices of the entry). "." indicates $t = 2$.

	000	100	200	300	400	500	600	700	800	900
00	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . 3 .
10	. . . . .	. . . . .	. . . . .	3	 3	. . 3 . .	. . . . .	 4	. . . . .	. . . 3 3
20	. . . . .	. . . . .	. 3 . . .	. . . . .	. . . . .	. 3 . . .	. . . . .	3	. 3 . . .	. . . . .
30	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . 3 .	3	. . . 5 .	. . . 3 .	4 . . .
40	. . . . .	. . . . .	. . . . .	. . . 3 .	. 3 . . .	. . . . .	. 3 . 3 .	. . . . .	. . . . .	. . . 3 .
50	. . . . .	. . . . .	3	 3	. . . . .	. . . . .	 4	3	 3	. . 3 . .
60	. . . . .	. . . 3 .	. . . . .	. . . . .	. . . . .	. . . . .	. . . 3	. . . . .	. 3 . . .	. . . . .
70	. . . . .	 3	. . . . .	. . . . .	 3	3 3 . . .	. . . . .	. . . . .	. . . . .	5 . . . .
80	. . . . .	. . . . .	. 3 . . .	. . . . .	. . . 3 .	. . . . .	. . . . .	. . . 3 3	. 3 . . .	. . . . .
90	. . . . .	3	. . . . .	. . . . .	3	. . . 5 .	. . . . .	. . . . .	. . . . .	3 . . . .

	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900
00	. . . . .	. 3 . . .	. . . . .	. 3 . . .	. . . . .	 3	. . . . .	. 3 . . .	. . . . .	. . . 3 .
10	 3	. . 3 . .	. . . . .	. . 3 . 4	. . . . .	. . . . .	 3	. 3 . . 3	. . . . .	. . 3 . .
20	. . . . .	. 3 . . .	. 6 . . .	. . . 3 .	. 3 . 3 .	. . . 3 .	. . . . .	. . . . .	. . . . .	 3
30	3 . . . 3	. 3 . . .	. . . . .	. . . . .	. . . 4 8	. . . . .	. . . . .	. . . . .	3	. . . . .
40	. . . . .	. . . . .	. . . . .	. . . . .	3 . . 7 .	. 3 . . .	. . . . .	. . . . .	3 . . 3 .	 4
50	3	. . . . .	. . 3 3 4	 3	6	 4	. . . . .	. . . . .	. . . . .	. . . 3 .
60	. 3 . . .	 4	. . . . .	. . . 3 .	. . . . .	. . . 6 .	3 3 . 3 .	. . . . .	. . . . .	. 3 . . 4
70	. . . . .	. . . . .	. . . . .	. . . . .	3 3 . . .	5 . . . 5	. . . . .	. . . . .	3 . . . 3	 4
80	. . . 3 .	. . . 3 .	. 3 . . .	. . . . .	. 3 . 3 .	. 3 . . 3	 3	. 6 . 3 .	. 3 . . .	4 . . 7 .
90	. . . . .	. . . . .	3	. . . 3 .	 7	. . . . .	 3	. 3 4 . .	. 3 . . .	. . . . .

	2000	2100	2200	2300	2400	2500	2600	2700	2800	2900
00	. . . . .	. . . . .	. 3 . 4 .	. . . . .	. . . . .	. 3 . . .	. . . . .	. . . . .	. 3 . . .	. 4 . . .
10	. . . . .	 3	. . 4 . .	. . 3 . .	. . 3 . .	. 4 3 . .	. . . . .	3	. . 3 . 3	. 3 . . .
20	. . . 3 .	. . . . .	. . . 3 .	. . . 4 .	. . 4 . . 4	. . . . .	 3	. . . . .	. 3 . . .	3 . . 3 .
30	 5	. . . . .	. . . . .	. . 3 . 4	. . . . .	3	. . . . .	3 3 . . .	. . . . .	 6
40	. . . . .	. 3 . . .	. . . . .	. . . 3 .	. . . . .	. 6 3 . .	. . . 3 .	. . . . .	3 3 . . .	. . . . .
50	. . . . .	. . 3 . 3	5	. . . . .	. . . 3 .	. . . . .	. . . 3 .	. . . . .	. . 4 . .	3 . . . .
60	. 3 . . .	. . . . .	. . . . .	. . . 3 .	. . . . .	. . . . .	3	. . . 3 .	. . 3 . .	. 3 . . .
70	. . . . .	4	. . . . .	4	. . . . .	3 . . . 3	7 . . 4 .	. 3 . . .	 7	3 4 . . .
80	. 3 . 3 .	. . . . .	. . . 6 .	. 3 . . .	 3	 4	. 7 . 8 .	. . . . .	. . . 5 .	. . . 3 .
90	. . 3 . 3	. . . . .	. 6 . . .	 8	. . . . .	3	 7	. . . . .	. 3 . . 4	. . 6 . 8

	3000	3100	3200	3300	3400	3500	3600	3700	3800	3900
00	. . . . .	4 . . 3 .	. 3 . . .	. . . 6 4	4 . . . 3	. . . . .	. . . . .	. . . . .	. 3 . . .	. . . 6 .
10	. 3 . 3 .	. . . 4 7	. . 3 . .	. . . . .	 3	3	. . . . .	. . 3 . 6	. . . 4 .	 3
20	. 3 . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. 3 . . 4	. . . . .	. 3 . . .	. 6 . . .
30	. . . . .	. . . . .	. . . . .	. . . . .	. . . 4 .	. 4 . . 6	5 . . . 3	. . . . .	3	3 . . . .
40	. . . . .	 3	. . . 3 .	. 3 . 3 .	. . . . .	. . . 8 .	. 3 . . .	 3	. . . 3 3	3 3 3 . 4
50	. . . . .	. . . . .	 3	. . . 7	. 3 . . .	 3	 4	. . 3 . .	3	. 3 . 4 .
60	. . . . .	. 3 . 4 .	. 4 . . 3	. . . . .	. 3 . 3 .	. . . . .	. . 3 . 6	. . . 4 .	. . . . .	. . . . .
70	 3	. 4 3 . .	6 3 . . 3	7	. 3 . . .	6	. . . 4 .	 3	. 3 . . .	. . . . .
80	. 3 . . .	 3	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .
90	. 6 . 3 .	. 3 . . .	. . 5 . 4	. . . . .	. . . 3 .	. . 3 . .	3	4 . . 3 .	. . . . .	. . . . .

	4000	4100	4200	4300	4400	4500	4600	4700	4800	4900
00	. . . 3 .	3 . . . 3	. . . . .	. . . 3 .	. . . . .	 3	. 3 . . 3	. 3 . . .	. . . . .	. 3 . . .
10	3 . . . 4	. . 4 . .	. 3 . . .	3 3 . 5 .	. 4 . . .	. . . . .	. . . . .	. 4 . . .	4	 8
20	. . . . .	. . . 6 .	. 3 . 3 .	. . . 8 .	 3	. 3 . 3 .	. . . . .	. . . 3 .	3	3 . . . .
30	. . . . .	. . . 8 .	. . . 4 .	. . . . .	. . 3 . 3	. . 4 . .	. 3 . . .	. . . . .	. . . . .	3 . . . .
40	. 4 . . .	. 3 . . .	. . . . .	 8	 3	3 . . 3 .	. 3 . . .	3 . . 3 .	3	. 3 . . .
50	. 3 . . .	. . . . .	 8	. 6 . . .	8 3 . . .	. . . . .	 3	6 . . 3 5	. . 3 . 3	. . . . .
60	3 3 . . .	. . . . .	. . 3 4 .	. 8 . . .	4	. . . . .	. 3 . 4 .	. . 3 . 4	. . . . .	. . . . .
70	. . 3 3 8	. . . . .	3	 3	 3	3 3 . . .	. . . 4 8	. . 4 . .	. 4 . . .	. . . . .
80	. 3 . . .	3	. 3 3 . .	. 3 . . 3	. . . . .	. 4 3 . 3	3	3 7 . 6 .	. . . . .	3 3 . . 4
90	. . . 3 8	. 6 . . .	. . 4 . .	3	. . 3 . 3	. . . . .	8	. 8 . . 8	. . . . .	 8

	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9

	5000	5100	5200	5300	5400	5500	5600	5700	5800	5900
00	4 . . 3 .	. . . 3 3	3 . . 3 .	 8	3 . . 5 .	 3	. 3 . . .	 3	. . . . .	. 4 . . 4
10	. . . 3 .	 8	3	. . 4 4 .	3	. . 3 . 8	. 4 4 . 3	8	. . . . .	. 3 3 . 3
20	 3	 4	3	. 8 . . .	. . . . .	. . . 8 .	. 3 . . .	3	. . 3 8 .	4 8 . 8 .
30	. 4 . . 8	3 . . . 4	3	. . . . .	. 4 . 8 .	. 3 . . 4	 8	. . . . .	. . . . .	3 . 4 . 8
40	. . . . .	. . . 4 .	. . . . .	. . . 3 5	8 . . . 3	3 . 3 . 4	. . . 8 .	. . . . .	. . . 5 .	. . . . .
50	3 3 . . 3	. . 8 . .	 3	8 . . 4 3	 3	. . . . .	3	. . 3 . 4	. 3 . . .	. . . . .
60	. . 3 . .	. . 3 . .	6 . . . 4	4 3 . . .	3	. 8 . 3 .	. . . 3 .	4 . . 3 .	. . . 3 .	8 . 3 . 3
70	. . . . .	6 6 . . .	3 8 . . 4	3 . . . 3	3	. . . . .	 4	. 3 . . 8	. . 3 . 4	 3
80	. . . . .	. . . . .	. 3 . 4 .	. 3 . . .	. 8 . . .	. . . . .	. 8 . . .	. . . 4 3	. . . . .	. . . 3 3
90	. . 3 . 8	4 . 4 . 3	. . . . .	. . . . .	. . . . .	6 . . 3 .	. . . . .	3 3 . . .	 4	. . . 3 3

	6000	6100	6200	6300	6400	6500	6600	6700	6800	6900
00	7 . . 3 7	. 3 . . .	. 8 . . 8	. . . . .	. . . . .	 5	. . 8 8 .	. . . 8 .	6 . 8 . .	3 . 4 8 .
10	. 7 . . .	. . 8 4 .	. . . . .	. . . 8 .	 4	8 3 4 . .	. . . 4 3 .	. . . 5 8	. 3 . . 4	8 5 . . .
20	. . . . .	 3	. . . . .	. 6 . . .	 3	. 3 . . .	. 4 . . 8	. . . . .	. 3 . 8 .	. . . . .
30	3	6	. . . . .	3 8 . . .	. 8 . . .	5 . 8 . 4	. . . . .	6	. . . . .	6 . . . .
40	5 8 . 6 .	. . . . .	. . . 3 .	8 8 . . .	. . . . .	. . . . .	. . . . .	. 8 . . .	. . . . .	. 8 . 6 .
50	 4	. . 4 5 4	. . . . .	8 . . . 8	. . . 5 .	. . . . .	7 6 . . 4	. . 4 . 8	. . . . .	. 8 . . 8
60	. . 4 8 .	. 3 . . .	3 4 . . 8	. . . 8 3	. . 3 . .	. . . . .	. . . 8 .	. . . . .	. 3 . . .	. . . . .
70	4 . . 4 .	 5	. . 8 . .	. . . 4 .	. . . . .	. . 4 . .	 5	 4	. . . . .	. . . . .
80	. . . . .	5	8 3 . . .	. 8 . . .	. . . . .	. 4 . . .	. . 3 . .	. . . . .	6 3 . . .	7 3 8 . 8
90	. . . . .	. 7 . . .	. . . 8 8	. . . . .	3 8 4 . .	. . 5 . 8	. 7 . . .	8 . 4 . .	. 8 . . 8	. . 4 . .

	7000	7100	7200	7300	7400	7500	7600	7700	7800	7900
00	 3	. . . . .	. . 3 3 .	. . 3 4 .	 3	. . 3 . .	. 8 . . .	. 8 . . 3	. . . . .	. . . . .
10	 4	. 5 4 4 .	. . . . .	 3	. 3 4 . .	. 3 . . .	. 3 3 . .	. . . 8 .	. . . . .	. 3 4 . 4
20	. 3 . 3 .	. 3 . 3 .	. 3 . . .	. 3 3 . .	. 4 . 3 .	. . . . .	. . . 3 3	4 3 . 3 3	. 3 . . 8	. . . 8 .
30	. . . 3 3	. 4 4 . .	. 3 8 . .	8 . . . 3	 3	. . . . .	3 3 . 3 .	. . . . .	. . 7 . .	. . . . .
40	. 3 3 . .	 3	. 3 . 6 3	. . . . .	4 3 . . .	. . 3 . .	. 8 . 3 .	. . . . .	 3	 8
50	. . . . .	. 3 . . 3	3 . 7 . .	. . 4 . .	. . . . .	. . 3 . 4	3	. . . . .	. 6 5 . .	. 3 . . .
60	. . . 4 .	. . 3 4 .	. . . . .	. . . . .	. . . . .	. . . . .	. 3 . . .	. . 3 4 .	4 3 . . .	. 3 . . .
70	. 4 . . 8	 3	. 4 . 3 .	. 3 . . .	3	3 7 . . .	. . . . .	 3	3 . . 4 .	. . . . .
80	3	. 3 . 8 .	. . . . .	. . . 3 .	. . . . .	. 4 . . .	. . . . .	. . . . .	. . . . .	4 3 . . 3
90	3 3 . . .	. . . 4 .	. . . . .	. . . . .	. 3 8 . 4	. 4 . . .	. . . 4 7	. . 5 . .	. . 6 . .	. . . . .

	8000	8100	8200	8300	8400	8500	8600	8700	8800	8900
00	. 3 . . .	. . . . .	. 4 . 4 .	. . 3 . 4	 3	. 3 . . 3	. . . . .	. . . 5 .	. 3 . . 3	 3
10	. . . . .	. . . . .	. 4 . . 8	3 . 4 . .	4 4 . 4 8	. . . . .	3 . 3 3 .	 5	 8	. 4 7 3 .
20	. . . . .	 6	. . . . .	. . . 3 .	. 3 . . .	 4	. 8 . 6 .	. . . . .	. . . . .	. 8 . . .
30	. 3 . . 8	5 . . . 3	8 . . 8 .	. . 4 . 3	. . . . .	. . . . .	. 3 . 4 3 3	3	. 3 . . .	. . 3 . 3
40	. . . . .	. 4 . . .	 3	. . 3 . .	. 3 . 4 .	 3	. . . . .	. 3 . 3 .	. 3 . . .	. . 3 . .
50	. . . 3 8	. . 3 . .	4 . . 4 3	 4	. . . . .	3	. 3 3 4 .	3	4 . . . 3	. . . . .
60	8 . . 3 .	. . . . .	4 3 . 3 .	. 8 . 3 .	. . 3 3 .	7 3 . . .	. . 3 . .	. . . . .	8 . . 4 .	. . . . .
70	 3	3 3 . . 8	 4	. . . . .	. . . 3 .	. 6 . 3 .	. . . . .	. 3 . . 5	3 . . . 3	. . . 4 .
80	. . . 8 .	. . 4 . 3 3	. . . . .	. . . . .	. . 3 . 3	 3	. . . . .	4 4 . . .	. . . 8 4	. . . . .
90	. . . . .	. . . 3 3	8 . . . 3	. . . . .	. . 4 . 3	. . . . .	 8	. . . . .	4 . . . 3	. . . 8 8

	9000	9100	9200	9300	9400	9500	9600	9700	9800	9900
00	. . 3 . .	4 3 . 3 .	. 8 3 . .	3 . . 3 .	. 3 . 3 .	. . . . .	 3	. . . 4 .	. 3 . . .	. . . . .
10	6 . . . 4	3	3	. . . . .	 8	7 . 3 . .	3 . . 4 .	 8	3 . 3 . .	. . . . .
20	. . . . .	4 3 . . .	. . . 3 .	. 6 3 . 4	. . . 3 .	. . . 3 3	. 8 . 3 .	. . . . .	. . . 3 .	. 3 . . .
30	. . . 4 .	. . . . .	. . 4 . 8	. . . . .	3	. 8 . . 4	. . . . .	. . . . .	. . . 3 8	. . 4 4 3
40	. . . . .	 3	 4	. . . 5 .	. . 3 . 4	. . . 8 3	4 8 . . .	4	. . . . .	. 3 . . .
50	3 4 3 . 8	. . 4 . .	. 4 . . .	. . 4 . 3	. . . . .	6 3 . 3 .	 3	. 3 . 3 3	3 3 . . .	. 3 . . 3
60	. . 3 . 3	. . . 3 3	. . . . .	. . 3 . .	. . 3 4 .	. 3 . 4 .	. . 3 . .	. . . 3 .	. . 3 . .	3 . 3 8 .
70	3	. . . . .	. 3 . . .	. . . . .	 8	. 3 . . .	3	. . . . .	3	. . . 4 3
80	. 3 . 3 .	. . . 3 .	 3	. 3 . . .	. . 3 . 4	. . . 8 4	. . . . .	. . . 3 .	3 3 3 8 .	 4
90	. 3 . 3 .	. . . . .	. . . . .	5	. 4 . . .	. . . . .	. . . . .	. . . . .	. . 3 . .	3 . . . .
	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9	1 3 5 7 9

See Also

§II.6	Hadamard matrices are equivalent to Hadamard designs. Regular Hadamard matrices are equivalent to Menon designs. Bush-type Hadamard matrices are used to construct twin symmetric designs and siamese twin symmetric designs.
§III.6	Hadamard matrices are equivalent to certain orthogonal arrays and transversal designs of higher index; see Theorem III.6.11.
§V.2	Orthogonal designs provide some of the most important constructions for Hadamard matrices.
§V.3	Hadamard matrices realize the maximum determinant among $(1, -1)$-matrices of order n.
§V.5	Generalized Hadamard matrices.
§VI.18.6	Some difference sets correspond to Hadamard matrices.
§VII.1	A Hadamard matrix of order n gives an optimal error-correcting code of length n.
§VII.11	Regular Hadamard matrices are used to construct strongly regular graphs; Bush type are used to construct twin strongly regular graphs, twin siamese strongly regular graphs and doubly regular graphs.
§VII.13	Hadamard matrices are used to construct regular two-graphs (Remark VII.13.50).
[616]	Concise survey examining topics connected to Hadamard matrices.
[891]	Constructing Hadamard matrices from orthogonal designs.
[1271]	Contains the Hadamard matrices up to order 28 in electronic form.
[1866]	More detailed information about Williamson and Williamson-type matrices, skew Hadamard matrices, and so on.
[1660, 2172]	Important constructions of Hadamard matrices.
[1850]	Powerful new results about the nonexistence of circulant Hadamard matrices.
[780]	A survey of modular Hadamard matrices.
[656, 658]	New constructions and concept of cocyclic Hadamard matrices.

References Cited: [65, 615, 616, 656, 658, 780, 891, 919, 1003, 1271, 1287, 1430, 1660, 1850, 1866, 1906, 1997, 2172]

2 Orthogonal Designs

Robert Craigen
Hadi Kharaghani

2.1 Definitions

2.1 Let n and w be positive integers. A *weighing matrix* W, of *weight* w and *order* n, is an $n \times n$ $(0, \pm 1)$-matrix satisfying $WW^T = wI$. Such a matrix is denoted by $W(n, w)$. ($w = 0$ is generally not permitted.)

2.2 Remark The term weighing matrix comes from the fact that these matrices arise as solutions in certain weighing experiments.

2.3 Examples A is a $W(4,3)$; B is a $W(6,5)$; C is a circulant $W(7,4)$; D is a $W(10,9)$; E is a $W(12,10)$. Every signed permutation matrix is a $W(n,1)$; a Hadamard matrix $H(n)$ (see §V.1) is the same as a $W(n,n)$.

$$A = \begin{pmatrix} 0 & - & - & - \\ 1 & 0 & 1 & - \\ 1 & - & 0 & 1 \\ 1 & 1 & - & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} - & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & - & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & - & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & - & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & - & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & - & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & - \end{pmatrix},$$

$$D = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - \\ 1 & 0 & 1 & 1 & 1 & - & - & - & 1 & 1 \\ 1 & 1 & 0 & 1 & - & 1 & - & 1 & - & 1 \\ 1 & 1 & 1 & 0 & - & - & 1 & 1 & 1 & - \\ 1 & 1 & - & - & 0 & 1 & 1 & - & 1 & 1 \\ 1 & - & 1 & - & 1 & 0 & 1 & 1 & - & 1 \\ 1 & - & - & 1 & 1 & 1 & 0 & 1 & 1 & - \\ - & - & 1 & 1 & - & 1 & 1 & 0 & 1 & 1 \\ - & 1 & - & 1 & 1 & - & 1 & 1 & 0 & 1 \\ - & 1 & 1 & - & 1 & 1 & - & 1 & 1 & 0 \end{pmatrix}, \qquad E = \begin{pmatrix} 0 & 1 & 1 & 1 & - & 1 & 0 & - & 1 & 1 & - & - \\ 1 & 0 & 1 & 1 & 1 & - & - & 0 & - & 1 & 1 & - \\ - & 1 & 0 & 1 & 1 & 1 & - & - & 0 & - & 1 & 1 \\ 1 & - & 1 & 0 & 1 & 1 & 1 & - & - & 0 & - & 1 \\ 1 & 1 & - & 1 & 0 & 1 & 1 & 1 & - & - & 0 & - \\ 1 & 1 & 1 & - & 1 & 0 & - & 1 & 1 & - & - & 0 \\ 0 & - & - & 1 & 1 & - & 0 & - & 1 & - & - & - \\ - & 0 & - & - & 1 & 1 & - & 0 & - & 1 & - & - \\ 1 & - & 0 & - & - & 1 & - & - & 0 & - & 1 & - \\ 1 & 1 & - & 0 & - & - & - & - & - & 0 & - & 1 \\ - & 1 & 1 & - & 0 & - & 1 & - & - & - & 0 & - \\ - & - & 1 & 1 & - & 0 & - & 1 & - & - & - & 0 \end{pmatrix}$$

2.4 Two $n \times n$ matrices X and Y are *disjoint* if there is no position in which they are both nonzero. They are *amicable* if $XY^T = YX^T$ or *antiamicable* if $XY^T = -YX^T$. A *circulant matrix*, $A = [a_{ij}]$, is an $n \times n$ matrix such that, for all $1 \le i, j \le n$, $a_{ij} = a_{j-i+1}$ (index reduced modulo n). A matrix is *regular* if its row and column sums are equal.

2.5 Examples Matrices A, B, D, and E in Example 2.3 are disjoint from the identity matrix. C is circulant. C and D are regular. H_1 below, being symmetric, is amicable to I_2, but it is antiamicable to H_2.

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \quad H_2 = \begin{pmatrix} - & 1 \\ 1 & 1 \end{pmatrix}.$$

2.6 A *conference matrix* of order n is a $W(n, n-1)$.

2.7 Examples A, B, and D in Examples 2.3 are conference matrices of orders 4, 6, and 10, respectively. More examples and information on conference matrices is in §V.6.1.

2.8 An *orthogonal design* of *order* n and *type* $(s_1, \ldots, s_u)$ (or with *parameters* $s_1, \ldots, s_u$), is a matrix of the form $D = x_1W_1 + x_2W_2 + \cdots + x_uW_u$, where $x_1, \ldots, x_u$ are distinct commuting indeterminates, $W_i = W(n, s_i)$, $i = 1, \ldots, u$, and W_i and W_j are disjoint and antiamicable, for all $1 \le i < j \le u$. Such a design is denoted $\mathrm{OD}(n; s_1, s_2, \ldots, s_u)$. It is *full* if $\sum_{i=1}^{u} s_i = n$ (equivalently, if it has no zeros).

2.9 Remarks

1. D has s_i entries $\pm x_i$ in each row.
2. $DD^T = sI_n$, where $s = s_1x_1^2 + \cdots + s_ux_u^2$.
3. D^T is also an $\mathrm{OD}(n; s_1, \ldots, s_t)$.
4. A one parameter orthogonal design is essentially the same as a weighing matrix. More generally, replacing each of the variables of an $\mathrm{OD}(n; s_1, \ldots, s_u)$ with $0, \pm 1$ gives a $W(n, w)$ where w is the sum of the s_is such that x_i is replaced by ± 1.

2.10 **Examples** The Williamson array (see §V.1.5) is an OD(4; 1, 1, 1, 1). Below, D_1 and D_2 are OD(2; 1, 1); D_3 and D_4 are OD(4; 1, 1, 1); and D_5 is an OD(4; 1)

$$D_1 = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad D_2 = \begin{pmatrix} x & y \\ y & -x \end{pmatrix}$$

$$D_3 = \begin{pmatrix} 0 & a & b & c \\ -a & 0 & c & -b \\ -b & -c & 0 & a \\ -c & b & -a & 0 \end{pmatrix} \quad D_4 = \begin{pmatrix} 0 & x & y & z \\ -x & 0 & -z & y \\ -y & z & 0 & -x \\ -z & -y & x & 0 \end{pmatrix} \quad D_5 = \begin{pmatrix} d & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & d \end{pmatrix}$$

2.2 Necessary Conditions

2.11 **Theorem** Suppose $W(n, w)$ exists.

1. If $n > 1$ is odd, then w is a perfect square and $n \geq w + \sqrt{w} + 1$ (equivalently, (1) $w \leq n - \frac{1+\sqrt{4n-3}}{2}$ or (2) $(n-w)^2 - (n-w) + 1 \geq n$). The case of equality, $W(k^2 + k + 1, k^2)$, implies the existence of a projective plane (see §VII.2.1) of order k.
2. If $n \equiv 2 \pmod 4$, then w is a sum of two squares; and if $n > 2$, then $w < n$.

2.12 A matrix A is *skew* if $A^T = -A$.

2.13 **Theorem** Suppose that there is a skew $W(n, w)$. Then $n \equiv 0 \pmod 2$; if $n \equiv 2 \pmod 4$, then w is a square, and $w < n - 1$ unless $n = 2$; and if $n \equiv 4 \pmod 8$, then w is a sum of 3 squares. If, further, $w = n - 2$, then it is a sum of 2 squares.

2.14 **Theorem** If W is a regular $W(n, w)$ with row sum k, then $w = k^2$.

2.15 The *Radon function* ρ is defined by $\rho(n) := 8q + 2^r$ when $n = 2^k \cdot p$, where $p \in \mathbb{Z}^+$ is odd, $k = 4q + r$, and $0 \leq r < 4$.

2.16 **Remark** For odd p, $\rho(2^k p)$ depends only on k. The first few values of $\rho(2^k)$:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\rho(2^k)$	1	2	4	8	9	10	12	16	17	18	20	24	25	26	28	32	33

2.17 **Theorem** If there exists an OD$(n; a_1, \ldots, a_s)$, then $s \leq \rho(n)$.

2.18 **Remark** Theorem 2.17 gives a necessary, but not sufficient, condition for existence.

2.19 **Theorem** [891, 1286] There is an OD$(n; 1, 1, 1, 1, 1, n-5)$ if and only if $n \leq 40$.

2.20 Let p be a prime and let $a = p^\alpha u$ and $b = p^\beta v$ where $(p, u) = (p, v) = 1$. The *Hilbert norm residue*, $(a, b)_p$, can be computed as

$$(a, b)_p = \begin{cases} (-1^{\alpha\beta(p-1)/2}) \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha & \text{if } p \neq 2 \\ -1^{(u-1)(v-1)/4 + \alpha(v^2-1)/8 + \beta(u^2-1)/8} & \text{if } p = 2 \end{cases}$$

where $\left(\frac{u}{p}\right)$ is the Legendre symbol (see §VII.8.2).

2.21 **Theorem** (see [891]) For odd values of n, and all primes p:

1. if there is an OD$(2n; a, b)$, then each of a, b and $a + b$ is a sum of two squares and $a + b < 2n$ unless $n = 1$;
2. if there is an OD$(4n; a, b)$, then $(-1, ab)_p (a, b)_p = 1$;
3. if there is an OD$(4n; a, b, c)$, then $(-1, abc)_p (a, b)_p (a, c)_p (b, c)_p = 1$;
4. if there is an OD$(4n; a, b, c, d)$, then $a + b + c + d \neq 4n - 1$, $abcd$ is a square, and $(a, b)_p (a, c)_p (a, d)_p (b, c)_p (b, d)_p (c, d)_p = 1$.

2.22 Remarks

1. For $n = 1, 3, 5$, and 7 the necessary condition given by Part 1 of Theorem 2.21 is sufficient for the existence of an OD$(2n; a, b)$. There is no OD$(18; 1, 16)$ and no OD$(26; 5, 20)$.
2. Compare Part 1 of Theorem 2.21 with Theorem 2.83.
3. For large $\rho(n)$, the closer s is to $\rho(n)$, the less likely an OD$(n; a_1, \ldots, a_s)$ is to exist, even if the algebraic conditions are satisfied. But when $s < \min(6, \rho(n))$, it is very likely that such a design exists. For example, all 3-parameter designs exist for orders 2^t, $t \geq 0$, and for $n \in \{24, 40, 48\}$, while Theorem 2.19 shows that some 6 parameter designs do not exist in cases satisfying Theorem 2.17.
4. Further algebraic and number theoretic conditions on the parameters of orthogonal designs are given in [891].

2.3 Amicable Orthogonal Designs and Product Designs

2.23 Orthogonal designs $A = \sum_{i=1}^{s} x_i A_i$ (an OD$(n; a_1, \ldots, a_s)$) and $B = \sum_{j=1}^{t} y_j B_j$ (an OD$(n; b_1, \ldots, b_t)$) are *amicable* if A_i is amicable to B_j for all i, j. The pair $(A; B)$ is denoted AOD$(n; (a_1, \ldots, a_s); (b_1, \ldots, b_t))$. (Internal parentheses may be omitted.) A and B are *antiamicable* if A_i and B_j are antiamicable for all i, j.

2.24 Examples D_1 and D_2 in Example 2.10 form an $AOD(2; (1, 1); (1, 1))$; D_3 and D_4 form an $AOD(4; (1, 1, 1); (1, 1, 1))$; D_5 is antiamicable to both D_3 and D_4

2.25 Construction If $X = \sum_{i=1}^{t} x_i P_i$ is an orthogonal design of order m and $A_1, \ldots, A_t$ are pairwise amicable orthogonal designs of order n, then $\sum P_i \otimes A_i$ is an orthogonal design of order mn (its parameters may be inferred from those of X and the A_is). In particular, if $(A; B)$ is an AOD$(n; (a_1, \ldots, a_s); (b_1, \ldots, b_t))$, then $\begin{pmatrix} A & -B \\ B & A \end{pmatrix}$ is an OD$(2n; a_1, \ldots, a_s, b_1, \ldots, b_t)$.

2.26 Example Refer to Examples 2.10. Write $D_3 = aP_1 + bP_2 + cP_3$. Let $A_1 = D_1$; let A_2 be the OD$(2; 2)$s obtained by replacing both variables of D_2 with w; and let A_3 be similarly obtained with variable z. Construction 2.25 gives an OD$(8; 1, 1, 2, 2)$:

$$P_1 \otimes A_1 + P_2 \otimes A_2 + P_3 \otimes A_3 = \begin{pmatrix} 0 & 0 & a & b & z & z & w & w \\ 0 & 0 & -b & a & z & -z & w & -w \\ -a & -b & 0 & 0 & w & w & -z & -z \\ b & -a & 0 & 0 & w & -w & -z & z \\ -z & -z & -w & -w & 0 & 0 & a & b \\ -z & z & -w & w & 0 & 0 & -b & a \\ -w & -w & z & z & -a & -b & 0 & 0 \\ -w & w & z & -z & b & -a & 0 & 0 \end{pmatrix}.$$

2.27 Construction Suppose H is a Hadamard matrix of order $2t$. In Examples 2.10, let $D_1 = aA_1 + bA_2$ and $D_2 = cB_1 + dB_2$, an AOD$(n; (1, 1); (1, 1))$. Let $P_1 = (A_1 \otimes I_t)H$, $P_2 = (A_2 \otimes I_t)H$, $Q_1 = (B_1 \otimes I_t)H$ and $Q_2 = (B_2 \otimes I_t)H$. Then $A = \frac{1}{2}(x_1(P_1 + P_2) + x_2(P_1 - P_2))$ and $B = \frac{1}{2}(y_1(Q_1 + Q_2) + y_2(Q_1 - Q_2))$ form an AOD$(2t; (t, t); (t, t))$. Construction 2.25 now gives OD$(4t; t, t, t, t)$.

2.28 Theorem [2165] If there is an AOD$(n; (a_1, \ldots, a_s); (b_1, \ldots, b_t))$ and $n = 2^p q$, q odd, then $s + t \leq 2(p + 1)$.

2.29 **Construction** If $A\ (= xA_1 + C)$ and B form an AOD$(n; (a_1, \ldots, a_s); (b_1, \ldots, b_t))$, then
$$\begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} \otimes A_1 + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes C \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes B + \begin{pmatrix} x_3 & 0 \\ 0 & -x_3 \end{pmatrix} \otimes A_1$$
form an AOD$(2n; (a_1, a_1, a_2, \ldots, a_s); (a_1, b_1, \ldots, b_t))$.

2.30 **Example** The AOD$(2^p; (1, \ldots, 1); (1, \ldots, 1))$ obtained by iterating Construction 2.29, starting with AOD$(1; (1); (1))$, achieves equality in Theorem 2.28 for all p.

2.31 A *product design* of *order* n and *type* $(a_1, \ldots, a_s; b_1, \ldots, b_t; c_1, \ldots, c_u)$ is a triple $(A; B; C)$, where

1. A, B, C are orthogonal designs of order n and types $(a_1, \ldots, a_s)$, $(b_1, \ldots, b_t)$, $(c_1, \ldots, c_u)$, respectively;
2. A and B are amicable; and
3. $A + C$ and $B + C$ are orthogonal designs.

2.32 **Example** In Examples 2.10, $(D_3; D_4; D_5)$ is a product design of order 4 and type $(1, 1, 1; 1, 1, 1; 1)$.

2.33 **Theorem** If there is an AOD$(n; (u_1, \ldots, u_k); (v_1, v_2))$, then there is a product design of order $2n$ and type $(v_1, u_1, \ldots, u_k; v_1, v_1, v_2; v_2)$.

2.34 **Example** An AOD$(4; (1, 1, 2); (1, 3))$:
$$X = \begin{pmatrix} a & b & c & c \\ -b & a & c & -c \\ c & c & -a & -b \\ c & -c & b & -a \end{pmatrix}, \quad Y = \begin{pmatrix} d & e & e & e \\ e & -d & e & -e \\ -e & -e & e & d \\ -e & e & d & -e \end{pmatrix}.$$
Product designs of order 8 and types $(1, 1, 1, 2; 1, 1, 3; 3)$ and $(1, 1, 2, 3; 1, 3, 3; 1)$ are then given by Theorem 2.33.

2.35 **Construction** [1808] Suppose $(A; x_1B_1 + x_2B_2; C)$ is a product design of order n and type $(a_1, \ldots, a_s; b_1, b_2; c_1, \ldots, c_t)$. Then
$$\left(\begin{pmatrix} wB_1 & A \\ A & -wB_1 \end{pmatrix}; \begin{pmatrix} xB_1 & xB_1 + zB_2 \\ -xB_1 + zB_2 & xB_1 \end{pmatrix}; \begin{pmatrix} vB_2 + C & C \\ -C & -vB_2 + C \end{pmatrix} \right)$$
is a product design of order $2n$ and type $(b_1, a_1, \ldots, a_s; 2b_1, b_2; b_2, 2c_1, 2c_2, \ldots, 2c_t)$.

2.36 **Construction** If $(A; B; C)$ is a product design of type $(a_1, \ldots, a_s; b_1, \ldots, b_t; c_1, \ldots, c_u)$ and order n, then $\begin{pmatrix} A + C & B + C \\ B - C & -A + C \end{pmatrix}$ is an OD$(2n; a_1, \ldots, a_s, b_1, \ldots, b_t, 2c_1, \ldots, 2c_u)$.

2.37 **Example** Equating two variables of D_4 in Example 2.32 gives a product design of order 4 and type $(1, 1, 1; 1, 2; 1)$. Iterating Construction 2.35 and applying Construction 2.36 give the full orthogonal designs in the following result.

2.38 **Theorem** [1808] For $k \geq 3$, there exists an OD$(2^k; 1, 1, 1, 1, 2, 2, 4, 4, \ldots, 2^{k-2}, 2^{k-2})$.

2.39 **Remark** When $k \equiv 1$ or $2 \pmod 4$, the design obtained in Theorem 2.38 has the maximum number of parameters. No full orthogonal designs of order $2^k p$ having $\rho(2^k)$ parameters, with p odd and $k > 4$ congruent to 0 or $3 \pmod 4$, are known.

2.40 **Corollary** If $a, b, c > 0$, $n > 2$ and $a + b + c = 2^n$, then an OD$(2^n; a, b, c)$ exists.

2.41 **Construction** Suppose that $(x_1P + x_2Q; R)$ is an AOD$(m; (d, e); (q_1, \ldots, q_u))$ and that $(A; B; xC)$ is a product design of order n and type $(a_1, \ldots, a_s; b_1, \ldots, b_t; c)$. Then $P \otimes A + Q \otimes B + R \otimes C$ is an OD$(mn; da_1, \ldots, da_s, eb_1, \ldots, eb_t, cq_1, \ldots, cq_u)$.

2.42 Example From H(2t), Construction 2.27 gives AOD(2t; (t, t); (t, t)) and Example 2.32 gives a product design of order 4 and type (1, 1, 1; 1, 1, 1; 1). From Construction 2.41 one obtains an OD(8t; t, t, t, t, t, t, t, t). [891]).

2.43 A *Plotkin array* P_t is an OD$(8t; t, t, t, t, t, t, t, t)$.

2.4 T-Matrix Constructions

2.44 A matrix is *monomial* each row and column has exactly one nonzero entry.

2.45 Disjoint $(0, \pm 1)$-matrices A, B, C, D of order t are *T-matrices* if

1. the elements of $S = \{A, B, C, D, A^T, B^T, C^T, D^T\}$ commute pairwise;
2. there exists a $t \times t$ monomial matrix R such that XR is amicable to Y for all $X, Y \in S$; and
3. $AA^T + BB^T + CC^T + DD^T = tI$.

2.46 Remarks

1. Conditions 1 and 2 are satisfied by any type I matrices A, B, C, D (see §V.1.5). For circulants, R can be any back-circulant monomial matrix.
2. Type I matrices are the most common (but not the only) kind of T-matrices.
3. T-matrices give powerful recursive constructions for *Baumert–Hall arrays* (that is, OD$(4t; t, t, t, t)$s).

2.47 Construction If A, B, C, D are T-matrices of order $4t$, then the Goethals–Seidel array (see §V.1.33), using A', B', C', D' in place of A, B, C, D, is an OD$(4t; t, t, t, t)$, where

$$A' = aA + bB + cC + dD, \quad B' = -bA + aB + dC - cD$$
$$C' = -cA - dB + aC + bD, \quad D' = -dA + cB - bC + aD\ .$$

2.48 An orthogonal design OD$(4k; a_1, \ldots, a_s)$ is a *Baumert–Hall–Welch array (BHW-array)* of order $4k$, if it can be partitioned into 16 $k \times k$ type I matrices.

2.49 Theorem [1866] Suppose there is a BHW-array OD$(4k; a_1, \ldots, a_s)$. If there are T-matrices of order t, then there is an OD$(4kt; ta_1, \ldots, ta_s)$.

2.50 Remark There are BHW-arrays of order $4k$ for all even $k \leq 36$, $k = 5$, $k = 9$, and $k = 134$. There is none of order 12.

2.51 Remark T-matrices are known for all orders $t \leq 200$ with the exception of $t = 73$, 79, 83, 89, 97, 103, 109, 113, 127, 131, 133, 135, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 183, 191, 193, 197, and 199.

2.52 Four mutually disjoint complementary ternary sequences (see §V.8) a, b, c, d of length and weight t are *T-sequences*.

2.53 Construction T-sequences give the first rows of circulant T-matrices. There are circulant T-matrices that do not correspond to T-sequences in this way.

2.54 Examples $(1, 1, -, 0, 0, 0, 0)$, $(0, 0, 0, 1, 0, 1, 0)$, $(0, 0, 0, 0, 1, 0, 0)$, $(0, 0, 0, 0, 0, 0, 0)$ are T-sequences of length 7; Constructions 2.53 and 2.47 give OD(28; 7, 7, 7, 7). Base sequences (see §8) a, b, c, d of lengths m, m, n, n give T-sequence of length $m + n$: $(\frac{a+b}{2}, 0_n)$, $(\frac{a-b}{2}, 0_n)$, $(0_m, \frac{c+d}{2})$, $(0_m, \frac{c-d}{2})$. (Here "(x, y)" denotes concatenation of sequences x and y.) Base sequences $a = (1, 1, -, 1), b = (1, 1, -, 1), c = (1, 1, 1, -, 1), d = (1, 1, 1, -, -)$ give T-sequences of length 9 (which give, in turn, OD(36; 9, 9, 9, 9)):

$(1, 1, -, 1, 0, 0, 0, 0, 0)$, $(0, 0, 0, 0, 0, 0, 0, 0, 0)$, $(0, 0, 0, 0, 1, 1, 1, -, 0)$, $(0, 0, 0, 0, 0, 0, 0, 0, 1)$.

2.55 An ordered list of T-matrices A, B, C, D is *weakly amicable* if
$$A(B^T + C^T) + D(B^T - C^T) = (B + C)A^T + (B - C)D^T.$$

2.56 **Example** Circulants A, B, C, D with first rows $(1,0,0), (0,1,0), (0,0,1), (0,0,0)$, respectively, are weakly amicable T-matrices of order 3.

2.57 A 4-tuple of matrices (A, B, C, D) of order n with entries $0, \pm x_1, \pm x_2, \ldots, \pm x_k$, where $x_1, \ldots, x_k$ are distinct variables, have *type* $(s_1, s_2, \ldots, s_k)$ if
$$AA^T + BB^T + CC^T + DD^T = (s_1 x_1^2 + s_2 x_2^2 + \cdots + s_k x_k^2) I_n.$$
Suppose that (A, B, C, D) is a 4-tuple of type I matrices of order n and type (s_1, s_2, s_3, s_4), (E, F, G, H) is a second 4-tuple of type I matrices of order n and type (t_1, t_2, t_3, t_4), and
$$AE^T - EA^T + \epsilon_1(BF^T - FB^T) + \epsilon_2(CG^T - GC^T) + \epsilon_3(DH^T - HD^T) = 0,$$
with $\epsilon_i \in \{\pm 1\}$, $i = 1, 2, 3$. The ordered list $(A, B, C, D; E, F, G, H)$ is a *special amicable set* of order n and *type* $(s_1, s_2, s_3, s_4; t_1, t_2, t_3, t_4)$. Without loss of generality, one can assume that $\epsilon_i = 1$ for $i = 1, 2, 3$.

2.58 **Remark** From a given special amicable set of type I matrices $(A, B, C, D; E, F, G, H)$ of order n, one gets four matrices with circulant blocks
$$\begin{pmatrix} A & E \\ -E & A \end{pmatrix}, \begin{pmatrix} B & F \\ -F & B \end{pmatrix}, \begin{pmatrix} C & G \\ -G & C \end{pmatrix}, \begin{pmatrix} D & H \\ -H & D \end{pmatrix}.$$
Substituting these matrices in the Goethals–Seidel array (from Examples 1.33) yields the *K-array* (see [1284]), an 8×8 analog of the Goethals–Seidel array:
$$K = \begin{pmatrix} A & E & FR & BR & GR & CR & HR & DR \\ -E & A & BR & -FR & CR & -GR & DR & -HR \\ -FR & -BR & A & E & -H^tR & D^tR & G^tR & -C^tR \\ -BR & FR & -E & A & D^tR & H^tR & -C^tR & -G^tR \\ -GR & -CR & H^tR & -D^tR & A & E & -F^tR & B^tR \\ -CR & GR & -D^tR & -H^tR & -E & A & B^tR & F^tR \\ -HR & -DR & -G^tR & C^tR & F^tR & -B^tR & A & E \\ -DR & HR & C^tR & G^tR & -B^tR & -F^tR & -E & A \end{pmatrix}$$

2.59 **Theorem** [1125] If there is a special amicable set of circulant matrices of order n and type $(s_1, s_2, s_3, s_4; t_1, t_2, t_3, t_4)$, then there exist

1. OD$(8n; s_1, s_2, s_3, s_4, t_1, t_2, t_3, t_4)$;
2. OD$(4(p+1)n; s_1, s_2, s_3, s_4, pt_1, pt_2, pt_3, pt_4)$ for every prime power $p \equiv 3 \pmod 4$;
3. AOD$(8n; (s_1, s_2, s_3, s_4); (t_1, t_2, t_3, t_4))$; and
4. AOD$(8n; (2s_1, 2s_2, 2s_3, 2s_4); (2t_1, 2t_2, 2t_3, 2t_4))$.

2.60 **Example** Let $(A, B, C, D, E, F, G, H) = ((a, d, -d), (c, d, d), (c, -d, b), (c, -b, -d), (g, h, h), (e, h, -h), (g, -h, f), (g, -f, -h))$. Then a special amicable set of matrices of type $(1, 2, 3, 6; 1, 2, 3, 6)$ is given by $(A, B, C, D; E, F, G, H)$. Theorem 2.59 gives OD$(24; 1, 1, 2, 2, 3, 3, 6, 6)$; OD$(12(p+1); 1, 2, 3, 6, p, 2p, 3p, 6p)$ for prime powers $p \equiv 3 \pmod 4$; AOD$(24; (1, 2, 3, 6); (1, 2, 3, 6))$; and AOD$(24; (2, 4, 6, 12); (2, 4, 6, 12))$.

2.61 **Theorem** If there is a weakly amicable set of circulant T-matrices of order n, then there is a special amicable set of eight circulant matrices of type $(n, n, n, n; n, n, n, n)$ and order n.

2.62 **Theorem** If there are weakly amicable T-matrices of order n and $p = 1$ or any prime power congruent to 3 mod 4, then there is an OD$(4n(p+1); n, n, n, n, np, np, np, np)$.

2.63 **Corollary** If there are weakly amicable T-matrices of order n, then there exists a Plotkin array, OD$(8n; n, n, n, n, n, n, n, n)$.

2.64 **Remark** [1126] Weakly amicable T-matrices exist for all orders $n \le 21$.

2.65 **Examples** In this and the following two examples, $\mathbf{x}$ represents $-x$. The Plotkin array P_1 is obtained from the K-array of Remark 2.58.

The Baumert–Hall array H is constructed by substituting circulant matrices A, B, C, and D with first rows (a,b,c), $(d,-a,b)$, $(-c,d,a)$, and $(-b,c,d)$, respectively, in the Goethals–Seidel array of Example 1.33.

$$\begin{pmatrix}
a & b & d & c & f & e & g & h \\
\mathbf{b} & a & c & \mathbf{d} & e & \mathbf{f} & h & \mathbf{g} \\
\mathbf{d} & \mathbf{c} & a & b & \mathbf{g} & h & f & \mathbf{e} \\
\mathbf{c} & d & \mathbf{b} & a & h & g & \mathbf{e} & \mathbf{f} \\
\mathbf{f} & \mathbf{e} & g & \mathbf{h} & a & b & \mathbf{d} & c \\
\mathbf{e} & f & \mathbf{h} & \mathbf{g} & \mathbf{b} & a & c & d \\
\mathbf{g} & \mathbf{h} & \mathbf{f} & e & d & \mathbf{c} & a & b \\
\mathbf{h} & g & e & f & \mathbf{c} & \mathbf{d} & \mathbf{b} & a
\end{pmatrix}$$

P_1: Plotkin OD(8;1,1,1,1,1,1,1,1)

$$\begin{pmatrix}
a & b & c & b & \mathbf{a} & d & a & d & \mathbf{c} & d & c & \mathbf{b} \\
c & a & b & \mathbf{a} & d & b & d & \mathbf{c} & a & c & \mathbf{b} & d \\
b & c & a & d & b & \mathbf{a} & \mathbf{c} & a & d & \mathbf{b} & d & c \\
\mathbf{b} & a & \mathbf{d} & a & b & c & c & d & \mathbf{b} & \mathbf{d} & \mathbf{a} & c \\
a & \mathbf{d} & \mathbf{b} & c & a & b & d & \mathbf{b} & c & \mathbf{a} & c & \mathbf{d} \\
\mathbf{d} & \mathbf{b} & a & b & c & a & \mathbf{b} & c & d & c & \mathbf{d} & \mathbf{a} \\
\mathbf{a} & \mathbf{d} & c & \mathbf{c} & \mathbf{d} & b & a & b & c & \mathbf{a} & b & d \\
\mathbf{d} & c & \mathbf{a} & \mathbf{d} & b & \mathbf{c} & c & a & b & b & d & \mathbf{a} \\
c & \mathbf{a} & \mathbf{d} & b & \mathbf{c} & \mathbf{d} & b & c & a & d & \mathbf{a} & b \\
\mathbf{d} & \mathbf{c} & b & d & a & \mathbf{c} & a & \mathbf{b} & \mathbf{d} & a & b & c \\
\mathbf{c} & b & \mathbf{d} & a & \mathbf{c} & d & \mathbf{b} & \mathbf{d} & a & c & a & b \\
b & \mathbf{d} & \mathbf{c} & \mathbf{c} & d & a & \mathbf{d} & a & \mathbf{b} & b & c & a
\end{pmatrix}$$

H: an OD(12;3,3,3,3)

2.66 **Example** The Plotkin array P_5 is obtained from the K-array by substituting the special amicable set of circulant matrices E, A, F, B, C, G, H, D by

$(a,f,f,c,-c)$, $(g,h,h,e,-e)$, $(-f,a,a,b,-b)$, $(-d,e,e,-h,h)$, $(c,b,b,-a,a)$, $(e,d,d,-g,g)$, $(-b,c,c,-f,f)$, and $(-h,g,g,d,-d)$, respectively.

$$\begin{pmatrix}
g & h & h & e & \mathbf{e} & a & f & f & c & \mathbf{c} & \mathbf{b} & b & a & a & \mathbf{f} & h & \mathbf{h} & e & e & \mathbf{d} & g & \mathbf{g} & d & d & e & a & \mathbf{a} & b & b & c & f & \mathbf{f} & c & c & \mathbf{b} & \mathbf{d} & d & g & g & \mathbf{h} \\
\mathbf{e} & g & h & h & e & \mathbf{c} & a & f & f & c & b & a & a & \mathbf{f} & \mathbf{b} & \mathbf{h} & e & e & \mathbf{d} & h & \mathbf{g} & d & d & e & g & \mathbf{a} & b & b & c & a & \mathbf{f} & c & c & \mathbf{b} & f & d & g & g & \mathbf{h} & \mathbf{d} \\
e & \mathbf{e} & g & h & h & c & \mathbf{c} & a & f & f & a & a & \mathbf{f} & \mathbf{b} & b & e & e & \mathbf{d} & h & \mathbf{h} & d & d & e & g & \mathbf{g} & b & b & c & a & \mathbf{a} & c & c & \mathbf{b} & f & \mathbf{f} & g & g & \mathbf{h} & \mathbf{d} & d \\
h & e & \mathbf{e} & g & h & f & c & \mathbf{c} & a & f & a & \mathbf{f} & \mathbf{b} & b & a & e & \mathbf{d} & h & \mathbf{h} & e & d & e & g & \mathbf{g} & d & b & c & a & \mathbf{a} & b & c & \mathbf{b} & f & \mathbf{f} & c & g & \mathbf{h} & \mathbf{d} & d & g \\
h & h & e & \mathbf{e} & g & f & f & c & \mathbf{c} & a & \mathbf{f} & \mathbf{b} & b & a & a & \mathbf{d} & h & \mathbf{h} & e & e & e & g & \mathbf{g} & d & d & c & a & \mathbf{a} & b & b & \mathbf{b} & f & \mathbf{f} & c & c & \mathbf{h} & \mathbf{d} & d & g & g \\
a & f & f & c & \mathbf{c} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & \mathbf{h} & h & \mathbf{e} & \mathbf{e} & d & \mathbf{b} & b & a & a & \mathbf{f} & \mathbf{a} & a & \mathbf{b} & \mathbf{b} & \mathbf{c} & g & \mathbf{g} & d & d & e & d & \mathbf{d} & \mathbf{g} & \mathbf{g} & h & f & \mathbf{f} & c & c & \mathbf{b} \\
\mathbf{c} & a & f & f & c & e & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & h & \mathbf{e} & \mathbf{e} & d & \mathbf{h} & b & a & a & \mathbf{f} & \mathbf{b} & a & \mathbf{b} & \mathbf{b} & \mathbf{c} & \mathbf{a} & \mathbf{g} & d & d & e & g & \mathbf{d} & \mathbf{g} & \mathbf{g} & h & d & \mathbf{f} & c & c & \mathbf{b} & f \\
c & \mathbf{c} & a & f & f & \mathbf{e} & e & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & \mathbf{e} & d & \mathbf{h} & h & a & a & \mathbf{f} & \mathbf{b} & b & \mathbf{b} & \mathbf{b} & \mathbf{c} & \mathbf{a} & a & d & d & e & g & \mathbf{g} & \mathbf{g} & \mathbf{g} & h & d & \mathbf{d} & c & c & \mathbf{b} & \mathbf{f} & \mathbf{f} \\
f & c & \mathbf{c} & a & f & \mathbf{h} & \mathbf{e} & e & \mathbf{g} & \mathbf{h} & \mathbf{e} & d & \mathbf{h} & h & \mathbf{e} & a & \mathbf{f} & \mathbf{b} & b & a & \mathbf{b} & \mathbf{c} & \mathbf{a} & a & \mathbf{b} & d & e & g & \mathbf{g} & d & \mathbf{g} & h & d & \mathbf{d} & \mathbf{g} & c & \mathbf{b} & f & \mathbf{f} & c \\
f & f & c & \mathbf{c} & a & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & \mathbf{g} & d & \mathbf{h} & e & \mathbf{e} & \mathbf{f} & \mathbf{b} & b & a & a & \mathbf{c} & \mathbf{a} & a & \mathbf{b} & \mathbf{b} & e & g & \mathbf{g} & d & d & h & d & \mathbf{d} & \mathbf{g} & \mathbf{g} & \mathbf{b} & f & \mathbf{f} & c & c \\
b & \mathbf{b} & \mathbf{a} & \mathbf{a} & f & \mathbf{h} & h & \mathbf{e} & \mathbf{e} & d & g & h & h & e & \mathbf{e} & a & f & f & c & \mathbf{c} & \mathbf{c} & c & \mathbf{f} & f & \mathbf{b} & \mathbf{g} & \mathbf{g} & \mathbf{d} & d & h & \mathbf{d} & \mathbf{d} & g & \mathbf{g} & \mathbf{e} & b & b & \mathbf{a} & a & c \\
\mathbf{b} & \mathbf{a} & \mathbf{a} & f & b & h & \mathbf{e} & \mathbf{e} & d & \mathbf{h} & \mathbf{e} & g & h & h & e & \mathbf{c} & a & f & f & c & c & \mathbf{f} & f & \mathbf{b} & c & \mathbf{g} & \mathbf{d} & d & h & \mathbf{g} & \mathbf{d} & g & \mathbf{g} & \mathbf{e} & \mathbf{d} & b & a & a & c & b \\
\mathbf{a} & \mathbf{a} & f & b & \mathbf{b} & \mathbf{e} & \mathbf{e} & d & \mathbf{h} & h & e & \mathbf{e} & g & h & h & c & \mathbf{c} & a & f & f & f & f & \mathbf{b} & c & c & \mathbf{d} & d & h & \mathbf{g} & \mathbf{g} & g & \mathbf{g} & \mathbf{e} & \mathbf{d} & \mathbf{d} & \mathbf{a} & a & c & b & b \\
\mathbf{a} & f & b & \mathbf{b} & \mathbf{a} & \mathbf{e} & d & \mathbf{h} & h & \mathbf{e} & h & e & \mathbf{e} & g & h & f & c & c & \mathbf{a} & f & f & \mathbf{b} & c & c & \mathbf{f} & d & h & \mathbf{g} & \mathbf{g} & \mathbf{d} & \mathbf{g} & \mathbf{e} & \mathbf{d} & \mathbf{d} & g & a & c & b & b & \mathbf{a} \\
f & b & \mathbf{b} & \mathbf{a} & \mathbf{a} & d & \mathbf{h} & h & \mathbf{e} & \mathbf{e} & h & h & e & \mathbf{e} & g & f & f & c & \mathbf{c} & \mathbf{a} & b & \mathbf{c} & c & \mathbf{f} & f & h & \mathbf{g} & \mathbf{g} & \mathbf{d} & d & \mathbf{e} & \mathbf{d} & \mathbf{d} & g & \mathbf{g} & c & b & b & \mathbf{a} & a \\
h & \mathbf{h} & e & e & \mathbf{d} & b & \mathbf{b} & \mathbf{a} & \mathbf{a} & f & a & f & f & c & \mathbf{c} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & g & g & d & \mathbf{d} & \mathbf{h} & c & c & \mathbf{f} & f & \mathbf{b} & \mathbf{b} & \mathbf{b} & a & \mathbf{a} & \mathbf{c} & \mathbf{d} & \mathbf{d} & g & \mathbf{g} & \mathbf{e} \\
\mathbf{h} & e & e & \mathbf{d} & h & \mathbf{b} & \mathbf{a} & \mathbf{a} & f & a & f & f & c & \mathbf{c} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & g & g & d & \mathbf{d} & \mathbf{h} & c & c & \mathbf{f} & f & \mathbf{b} & \mathbf{b} & \mathbf{b} & a & \mathbf{a} & \mathbf{c} & \mathbf{b} & \mathbf{d} & g & \mathbf{g} & \mathbf{e} & \mathbf{d} \\
e & e & \mathbf{d} & h & \mathbf{h} & \mathbf{a} & \mathbf{a} & f & b & \mathbf{b} & c & \mathbf{c} & a & f & \mathbf{f} & \mathbf{e} & \mathbf{e} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{d} & \mathbf{d} & \mathbf{h} & g & g & \mathbf{f} & f & \mathbf{b} & c & c & a & \mathbf{a} & \mathbf{c} & \mathbf{b} & \mathbf{b} & g & \mathbf{g} & \mathbf{e} & \mathbf{d} & \mathbf{d} \\
e & \mathbf{d} & h & \mathbf{h} & e & \mathbf{a} & f & b & \mathbf{b} & \mathbf{a} & f & c & \mathbf{c} & a & \mathbf{f} & \mathbf{h} & \mathbf{e} & e & \mathbf{g} & \mathbf{h} & \mathbf{d} & \mathbf{h} & g & g & d & f & \mathbf{b} & c & c & \mathbf{f} & \mathbf{a} & \mathbf{c} & \mathbf{b} & \mathbf{b} & a & \mathbf{g} & \mathbf{e} & \mathbf{d} & \mathbf{d} & g \\
\mathbf{d} & h & \mathbf{h} & e & e & f & b & \mathbf{b} & \mathbf{a} & \mathbf{a} & f & f & c & \mathbf{c} & a & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & \mathbf{g} & \mathbf{h} & g & g & d & \mathbf{d} & \mathbf{b} & c & c & \mathbf{f} & f & \mathbf{c} & \mathbf{b} & \mathbf{b} & a & \mathbf{a} & \mathbf{e} & \mathbf{d} & \mathbf{d} & g & \mathbf{g} \\
\mathbf{g} & g & \mathbf{d} & \mathbf{d} & \mathbf{e} & \mathbf{a} & a & \mathbf{b} & \mathbf{b} & \mathbf{c} & \mathbf{c} & \mathbf{c} & f & \mathbf{f} & b & g & g & d & \mathbf{d} & \mathbf{h} & g & h & h & e & \mathbf{e} & a & f & f & c & \mathbf{c} & a & a & b & \mathbf{b} & \mathbf{f} & \mathbf{e} & \mathbf{e} & h & \mathbf{h} & d \\
g & \mathbf{d} & \mathbf{d} & \mathbf{e} & \mathbf{g} & a & \mathbf{b} & \mathbf{b} & \mathbf{c} & \mathbf{a} & \mathbf{c} & f & \mathbf{f} & b & \mathbf{c} & \mathbf{g} & d & \mathbf{d} & \mathbf{h} & g & \mathbf{e} & g & h & h & e & \mathbf{c} & a & f & f & c & a & b & \mathbf{b} & \mathbf{f} & a & \mathbf{e} & h & \mathbf{h} & d & \mathbf{e} \\
\mathbf{d} & \mathbf{d} & \mathbf{e} & \mathbf{g} & g & \mathbf{b} & \mathbf{b} & \mathbf{c} & \mathbf{a} & a & f & \mathbf{f} & b & \mathbf{c} & \mathbf{c} & \mathbf{d} & \mathbf{d} & \mathbf{h} & g & \mathbf{e} & g & h & h & e & \mathbf{c} & a & f & f & c & \mathbf{a} & b & \mathbf{b} & \mathbf{f} & a & \mathbf{e} & h & \mathbf{h} & d & \mathbf{e} & \mathbf{e} \\
\mathbf{d} & \mathbf{e} & \mathbf{g} & g & \mathbf{d} & \mathbf{b} & \mathbf{c} & \mathbf{a} & a & \mathbf{b} & \mathbf{f} & b & \mathbf{c} & \mathbf{c} & \mathbf{d} & \mathbf{d} & \mathbf{h} & g & g & d & h & e & e & g & h & f & c & \mathbf{c} & a & f & \mathbf{b} & \mathbf{f} & a & \mathbf{e} & h & \mathbf{h} & \mathbf{d} & e & e \\
\mathbf{e} & \mathbf{g} & g & \mathbf{d} & \mathbf{d} & \mathbf{c} & \mathbf{a} & a & \mathbf{b} & \mathbf{b} & \mathbf{b} & c & \mathbf{c} & \mathbf{c} & f & \mathbf{f} & \mathbf{h} & g & g & d & \mathbf{d} & \mathbf{h} & h & e & \mathbf{e} & g & g & f & f & c & \mathbf{c} & a & \mathbf{f} & \mathbf{b} & \mathbf{b} & a & \mathbf{g} & \mathbf{e} & \mathbf{d} & \mathbf{d} & g \\
a & \mathbf{a} & b & b & c & \mathbf{g} & g & \mathbf{d} & \mathbf{d} & \mathbf{e} & \mathbf{g} & \mathbf{g} & \mathbf{d} & d & h & \mathbf{c} & \mathbf{c} & f & \mathbf{f} & b & a & f & f & c & \mathbf{c} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & e & e & \mathbf{h} & h & \mathbf{d} & a & a & b & \mathbf{b} & \mathbf{f} \\
\mathbf{a} & b & b & c & a & g & \mathbf{d} & \mathbf{d} & \mathbf{e} & \mathbf{g} & \mathbf{g} & \mathbf{d} & d & h & \mathbf{g} & \mathbf{c} & f & \mathbf{f} & b & \mathbf{c} & \mathbf{c} & a & f & f & c & \mathbf{e} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & \mathbf{h} & h & \mathbf{d} & e & a & b & \mathbf{b} & f & a \\
b & b & c & a & \mathbf{a} & \mathbf{d} & \mathbf{d} & \mathbf{e} & \mathbf{g} & \mathbf{g} & \mathbf{d} & d & h & \mathbf{g} & \mathbf{g} & \mathbf{f} & \mathbf{f} & b & \mathbf{c} & \mathbf{c} & \mathbf{c} & c & \mathbf{c} & a & f & f & \mathbf{e} & \mathbf{e} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{h} & \mathbf{h} & \mathbf{d} & e & e & b & \mathbf{b} & \mathbf{f} & a & a \\
b & c & a & \mathbf{a} & b & \mathbf{d} & \mathbf{e} & \mathbf{g} & \mathbf{g} & \mathbf{d} & d & h & \mathbf{g} & \mathbf{g} & \mathbf{d} & \mathbf{f} & b & \mathbf{c} & \mathbf{c} & f & f & c & \mathbf{c} & a & f & \mathbf{h} & \mathbf{e} & \mathbf{e} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{d} & e & e & \mathbf{h} & \mathbf{b} & \mathbf{f} & a & a & b \\
c & a & \mathbf{a} & b & b & \mathbf{e} & \mathbf{g} & \mathbf{g} & \mathbf{d} & \mathbf{d} & h & \mathbf{g} & \mathbf{g} & \mathbf{d} & d & b & \mathbf{c} & \mathbf{c} & f & \mathbf{f} & f & f & c & \mathbf{c} & a & \mathbf{h} & \mathbf{h} & \mathbf{e} & \mathbf{e} & \mathbf{g} & \mathbf{d} & e & e & \mathbf{h} & h & \mathbf{f} & a & a & b & \mathbf{b} \\
\mathbf{f} & f & \mathbf{c} & \mathbf{c} & b & d & \mathbf{d} & \mathbf{g} & \mathbf{g} & h & d & \mathbf{d} & \mathbf{g} & \mathbf{g} & e & \mathbf{b} & \mathbf{b} & a & \mathbf{a} & \mathbf{c} & \mathbf{a} & \mathbf{a} & \mathbf{b} & b & f & e & e & \mathbf{h} & \mathbf{h} & \mathbf{d} & g & h & h & e & \mathbf{e} & a & f & f & c & \mathbf{c} \\
f & \mathbf{c} & \mathbf{c} & b & \mathbf{f} & \mathbf{d} & \mathbf{d} & \mathbf{g} & \mathbf{g} & h & d & \mathbf{d} & \mathbf{g} & \mathbf{g} & e & d & \mathbf{b} & \mathbf{a} & \mathbf{a} & \mathbf{c} & \mathbf{b} & \mathbf{a} & \mathbf{b} & b & f & \mathbf{a} & e & \mathbf{h} & \mathbf{h} & \mathbf{d} & e & \mathbf{e} & \mathbf{g} & h & h & e & \mathbf{c} & a & f & f & c \\
\mathbf{c} & \mathbf{c} & b & \mathbf{f} & f & \mathbf{g} & \mathbf{g} & \mathbf{h} & d & \mathbf{d} & \mathbf{g} & g & e & d & d & \mathbf{a} & \mathbf{a} & \mathbf{c} & \mathbf{b} & \mathbf{b} & \mathbf{b} & b & f & \mathbf{a} & \mathbf{a} & \mathbf{h} & \mathbf{h} & \mathbf{d} & e & e & e & e & g & h & h & c & c & a & f & f \\
\mathbf{c} & b & \mathbf{f} & f & \mathbf{c} & \mathbf{g} & h & d & \mathbf{d} & \mathbf{g} & g & e & d & d & \mathbf{g} & \mathbf{a} & \mathbf{c} & \mathbf{b} & \mathbf{b} & \mathbf{b} & b & f & \mathbf{a} & \mathbf{a} & \mathbf{b} & h & \mathbf{d} & e & e & \mathbf{h} & h & e & \mathbf{e} & g & h & f & c & c & a & f \\
b & \mathbf{f} & f & \mathbf{c} & \mathbf{c} & h & d & \mathbf{d} & \mathbf{g} & \mathbf{g} & e & d & \mathbf{d} & \mathbf{g} & g & \mathbf{c} & \mathbf{b} & \mathbf{b} & a & a & f & \mathbf{a} & \mathbf{a} & \mathbf{b} & b & \mathbf{d} & e & e & \mathbf{h} & h & h & h & e & \mathbf{e} & g & f & f & c & \mathbf{c} & a \\
\mathbf{d} & d & g & g & \mathbf{h} & \mathbf{f} & f & \mathbf{c} & \mathbf{c} & b & b & b & \mathbf{a} & a & c & d & d & \mathbf{g} & \mathbf{g} & e & \mathbf{e} & \mathbf{e} & h & \mathbf{h} & d & \mathbf{a} & \mathbf{a} & \mathbf{b} & b & f & a & f & f & c & \mathbf{c} & \mathbf{g} & \mathbf{h} & \mathbf{h} & \mathbf{e} & e \\
d & g & g & \mathbf{h} & \mathbf{d} & f & \mathbf{c} & \mathbf{c} & b & \mathbf{f} & b & \mathbf{a} & a & c & b & d & \mathbf{g} & \mathbf{g} & e & d & \mathbf{e} & \mathbf{e} & h & \mathbf{h} & d & \mathbf{e} & \mathbf{a} & \mathbf{b} & b & f & \mathbf{a} & \mathbf{c} & a & f & f & c & e & \mathbf{g} & \mathbf{h} & \mathbf{h} & e \\
g & g & \mathbf{h} & \mathbf{d} & d & \mathbf{c} & \mathbf{c} & b & \mathbf{f} & f & \mathbf{a} & a & c & b & \mathbf{b} & \mathbf{g} & g & e & d & d & \mathbf{h} & \mathbf{h} & d & \mathbf{e} & \mathbf{e} & \mathbf{b} & b & f & \mathbf{a} & \mathbf{a} & c & \mathbf{c} & a & f & f & e & \mathbf{e} & \mathbf{g} & \mathbf{h} & \mathbf{h} \\
g & \mathbf{h} & \mathbf{d} & d & g & \mathbf{c} & b & \mathbf{f} & f & \mathbf{c} & a & c & b & b & \mathbf{a} & g & e & d & d & \mathbf{g} & \mathbf{h} & d & \mathbf{e} & \mathbf{e} & h & b & f & \mathbf{a} & \mathbf{a} & \mathbf{b} & f & c & \mathbf{c} & a & f & \mathbf{h} & \mathbf{e} & \mathbf{e} & \mathbf{g} & \mathbf{h} \\
\mathbf{h} & \mathbf{d} & d & g & g & b & \mathbf{f} & f & \mathbf{c} & \mathbf{c} & c & b & b & \mathbf{a} & a & e & d & d & \mathbf{g} & \mathbf{g} & d & \mathbf{e} & \mathbf{e} & h & \mathbf{h} & f & \mathbf{a} & \mathbf{a} & \mathbf{b} & b & f & f & c & \mathbf{c} & a & \mathbf{h} & \mathbf{h} & \mathbf{e} & e & \mathbf{g}
\end{pmatrix}$$

P_5: Plotkin OD(40;5,5,5,5,5,5,5,5)

2.67 **Examples** Substituting E, A, F, B, G, C, D, H, the special amicable set of circulant matrices with first rows (a,b,c), (e,f,g), $(-b,a,d)$, $(-g,-h,e)$, $(-c,-d,a)$, $(-f,e,h)$, $(-d,c,-b)$, $(-h,g,-f)$, respectively, in the K-array, the Plotkin P_3 is constructed.

The OD(24; 1, 1, 2, 2, 3, 3, 6, 6) is from Example 2.60 with D and H switched.

$$\begin{pmatrix}
e&f&g&a&b&c&d&a&\mathbf{b}&e&\mathbf{h}&\mathbf{g}&a&\mathbf{d}&\mathbf{c}&h&e&\mathbf{f}&\mathbf{f}&g&\mathbf{h}&\mathbf{b}&c&\mathbf{d}\\
g&e&f&c&a&b&a&\mathbf{b}&d&\mathbf{h}&\mathbf{g}&e&\mathbf{d}&\mathbf{c}&a&e&f&h&g&\mathbf{h}&\mathbf{f}&c&\mathbf{d}&\mathbf{b}\\
f&g&e&b&c&a&\mathbf{b}&d&a&\mathbf{g}&e&\mathbf{h}&\mathbf{c}&a&\mathbf{d}&\mathbf{f}&h&e&\mathbf{h}&\mathbf{f}&g&\mathbf{d}&\mathbf{b}&c\\
a&b&c&\mathbf{e}&\mathbf{f}&\mathbf{g}&\mathbf{e}&h&g&d&a&\mathbf{b}&\mathbf{h}&\mathbf{e}&f&a&\mathbf{d}&\mathbf{c}&b&\mathbf{c}&d&f&g&\mathbf{h}\\
c&a&b&\mathbf{g}&\mathbf{e}&\mathbf{f}&h&g&\mathbf{e}&a&\mathbf{b}&\mathbf{d}&\mathbf{e}&f&\mathbf{h}&\mathbf{d}&\mathbf{c}&a&\mathbf{c}&d&b&g&\mathbf{h}&\mathbf{f}\\
b&c&a&\mathbf{f}&\mathbf{g}&\mathbf{e}&g&\mathbf{e}&h&\mathbf{b}&d&a&f&\mathbf{h}&\mathbf{e}&\mathbf{c}&a&\mathbf{d}&\mathbf{d}&b&\mathbf{c}&\mathbf{h}&\mathbf{f}&g\\
\mathbf{d}&\mathbf{a}&b&\mathbf{e}&h&g&e&f&g&a&b&c&g&\mathbf{f}&\mathbf{h}&\mathbf{c}&b&d&d&\mathbf{a}&c&e&h&\mathbf{f}\\
\mathbf{a}&b&\mathbf{d}&h&g&\mathbf{e}&g&e&f&c&a&b&\mathbf{f}&\mathbf{h}&g&b&d&\mathbf{c}&\mathbf{a}&c&d&h&\mathbf{f}&e\\
b&\mathbf{d}&\mathbf{a}&g&\mathbf{e}&h&f&g&e&b&c&a&\mathbf{h}&\mathbf{g}&\mathbf{f}&d&\mathbf{c}&b&\mathbf{c}&d&\mathbf{a}&\mathbf{f}&e&h\\
e&\mathbf{h}&\mathbf{g}&\mathbf{d}&\mathbf{a}&b&a&b&\mathbf{c}&\mathbf{e}&\mathbf{f}&\mathbf{g}&c&\mathbf{b}&\mathbf{d}&g&\mathbf{f}&\mathbf{h}&\mathbf{e}&\mathbf{h}&f&d&\mathbf{a}&c\\
\mathbf{h}&\mathbf{g}&e&\mathbf{a}&b&\mathbf{d}&c&a&b&\mathbf{g}&\mathbf{e}&\mathbf{f}&\mathbf{b}&\mathbf{d}&c&\mathbf{f}&\mathbf{h}&g&\mathbf{h}&f&\mathbf{e}&\mathbf{a}&c&d\\
\mathbf{g}&e&\mathbf{h}&b&\mathbf{d}&\mathbf{a}&b&c&a&\mathbf{f}&\mathbf{g}&\mathbf{e}&\mathbf{d}&\mathbf{c}&b&\mathbf{h}&\mathbf{g}&\mathbf{f}&f&\mathbf{e}&\mathbf{h}&c&d&\mathbf{a}\\
\mathbf{a}&d&c&\mathbf{h}&\mathbf{e}&f&\mathbf{g}&f&h&\mathbf{c}&\mathbf{b}&\mathbf{d}&e&f&g&a&b&c&a&d&\mathbf{b}&\mathbf{h}&e&g\\
d&c&\mathbf{a}&\mathbf{e}&f&\mathbf{h}&f&\mathbf{h}&\mathbf{g}&\mathbf{b}&\mathbf{d}&c&g&e&f&c&a&b&d&\mathbf{b}&a&\mathbf{e}&g&\mathbf{h}\\
c&\mathbf{a}&d&f&\mathbf{h}&\mathbf{e}&\mathbf{h}&\mathbf{g}&\mathbf{f}&\mathbf{d}&\mathbf{c}&\mathbf{b}&f&g&e&b&c&a&\mathbf{b}&a&d&g&\mathbf{h}&\mathbf{e}\\
h&e&\mathbf{f}&\mathbf{a}&d&c&\mathbf{c}&\mathbf{b}&\mathbf{d}&\mathbf{g}&f&\mathbf{h}&a&\mathbf{b}&\mathbf{c}&\mathbf{e}&\mathbf{f}&\mathbf{g}&\mathbf{h}&\mathbf{e}&\mathbf{g}&a&d&\mathbf{b}\\
e&\mathbf{f}&h&d&c&\mathbf{a}&\mathbf{b}&\mathbf{d}&\mathbf{c}&\mathbf{f}&\mathbf{h}&\mathbf{g}&c&\mathbf{a}&\mathbf{b}&\mathbf{g}&\mathbf{e}&\mathbf{f}&\mathbf{e}&\mathbf{g}&\mathbf{h}&\mathbf{d}&\mathbf{b}&a\\
\mathbf{f}&h&e&c&\mathbf{a}&\mathbf{d}&\mathbf{d}&\mathbf{c}&\mathbf{b}&\mathbf{h}&\mathbf{g}&\mathbf{f}&\mathbf{b}&\mathbf{c}&\mathbf{a}&\mathbf{f}&\mathbf{e}&\mathbf{g}&\mathbf{e}&\mathbf{h}&c&\mathbf{b}&a&d\\
f&\mathbf{g}&\mathbf{h}&\mathbf{b}&\mathbf{c}&d&\mathbf{d}&\mathbf{a}&\mathbf{c}&\mathbf{e}&\mathbf{h}&\mathbf{f}&\mathbf{a}&\mathbf{d}&\mathbf{b}&\mathbf{h}&\mathbf{e}&\mathbf{g}&e&f&g&a&b&c\\
\mathbf{g}&\mathbf{h}&\mathbf{f}&\mathbf{c}&d&\mathbf{b}&\mathbf{a}&\mathbf{c}&\mathbf{d}&\mathbf{h}&\mathbf{f}&\mathbf{e}&\mathbf{d}&\mathbf{b}&\mathbf{a}&\mathbf{e}&\mathbf{g}&\mathbf{h}&g&e&f&c&a&b\\
h&f&\mathbf{g}&d&\mathbf{b}&\mathbf{c}&\mathbf{c}&\mathbf{d}&\mathbf{a}&\mathbf{f}&\mathbf{e}&\mathbf{h}&\mathbf{b}&\mathbf{a}&\mathbf{d}&\mathbf{g}&\mathbf{h}&e&f&g&e&b&c&a\\
\mathbf{b}&\mathbf{c}&\mathbf{d}&\mathbf{f}&\mathbf{g}&\mathbf{h}&\mathbf{e}&\mathbf{h}&\mathbf{f}&\mathbf{d}&\mathbf{a}&\mathbf{c}&\mathbf{h}&\mathbf{e}&\mathbf{g}&\mathbf{a}&\mathbf{d}&\mathbf{b}&a&b&c&\mathbf{e}&\mathbf{f}&\mathbf{g}\\
c&\mathbf{d}&\mathbf{b}&\mathbf{g}&h&f&h&\mathbf{f}&e&a&\mathbf{c}&\mathbf{d}&\mathbf{e}&g&h&\mathbf{d}&\mathbf{b}&a&\mathbf{c}&a&b&\mathbf{g}&\mathbf{e}&\mathbf{f}\\
\mathbf{d}&\mathbf{b}&c&h&f&\mathbf{g}&\mathbf{f}&e&h&\mathbf{c}&\mathbf{d}&\mathbf{a}&g&h&\mathbf{f}&\mathbf{e}&\mathbf{h}&\mathbf{c}&\mathbf{d}&\mathbf{a}&g&\mathbf{h}&\mathbf{f}&e&a
\end{pmatrix}$$

P_3: Plotkin OD(24;3,3,3,3,3,3,3,3)

$$\begin{pmatrix}
a&\mathbf{d}&\mathbf{d}&g&h&h&\mathbf{h}&e&d&d&c&f&\mathbf{h}&g&b&\mathbf{d}&c&\mathbf{d}&\mathbf{b}&c&\mathbf{h}&\mathbf{f}&g\\
\mathbf{d}&a&d&h&g&h&h&e&\mathbf{h}&d&c&d&\mathbf{h}&g&f&\mathbf{d}&c&\mathbf{b}&b&c&\mathbf{d}&\mathbf{f}&g&\mathbf{h}\\
d&\mathbf{d}&a&h&h&g&e&\mathbf{h}&c&d&d&g&f&\mathbf{h}&c&b&\mathbf{d}&c&\mathbf{d}&\mathbf{b}&g&\mathbf{h}&\mathbf{f}\\
\mathbf{g}&\mathbf{h}&\mathbf{h}&a&\mathbf{d}&\mathbf{d}&d&c&h&\mathbf{e}&\mathbf{b}&\mathbf{d}&c&\mathbf{f}&\mathbf{h}&\mathbf{g}&\mathbf{f}&d&b&\mathbf{c}\\
\mathbf{h}&\mathbf{g}&\mathbf{h}&\mathbf{d}&a&d&d&c&d&\mathbf{h}&\mathbf{e}&\mathbf{h}&\mathbf{d}&c&b&\mathbf{g}&\mathbf{f}&\mathbf{f}&g&h&\mathbf{b}&\mathbf{c}&d\\
\mathbf{h}&\mathbf{h}&\mathbf{g}&d&\mathbf{d}&a&c&d&\mathbf{d}&\mathbf{e}&\mathbf{h}&\mathbf{d}&c&b&\mathbf{d}&\mathbf{g}&\mathbf{f}&h&g&\mathbf{h}&\mathbf{f}&\mathbf{c}&d&b\\
h&\mathbf{h}&\mathbf{e}&\mathbf{d}&\mathbf{d}&\mathbf{c}&a&d&\mathbf{d}&g&h&h&b&d&\mathbf{c}&\mathbf{f}&\mathbf{h}&g&\mathbf{h}&f&g&d&\mathbf{b}&\mathbf{c}\\
\mathbf{h}&\mathbf{e}&h&\mathbf{d}&\mathbf{c}&\mathbf{d}&d&a&h&h&g&\mathbf{c}&b&\mathbf{h}&\mathbf{g}&\mathbf{f}&f&g&\mathbf{h}&\mathbf{b}&\mathbf{c}&d\\
\mathbf{e}&h&\mathbf{h}&\mathbf{c}&\mathbf{d}&\mathbf{d}&\mathbf{d}&a&h&h&g&\mathbf{c}&b&d&g&\mathbf{f}&\mathbf{h}&g&\mathbf{h}&f&\mathbf{c}&\mathbf{d}&\mathbf{b}\\
\mathbf{d}&\mathbf{d}&\mathbf{c}&\mathbf{h}&e&\mathbf{g}&\mathbf{h}&\mathbf{h}&a&\mathbf{d}&\mathbf{f}&\mathbf{h}&g&\mathbf{b}&\mathbf{d}&c&\mathbf{d}&\mathbf{b}&\mathbf{c}&h&\mathbf{f}&\mathbf{g}\\
\mathbf{d}&\mathbf{c}&\mathbf{d}&h&e&\mathbf{h}&\mathbf{h}&\mathbf{g}&\mathbf{h}&\mathbf{d}&a&\mathbf{d}&\mathbf{h}&g&\mathbf{f}&\mathbf{d}&\mathbf{c}&\mathbf{b}&\mathbf{b}&\mathbf{c}&\mathbf{d}&\mathbf{f}&\mathbf{g}&h\\
\mathbf{c}&\mathbf{d}&\mathbf{d}&\mathbf{e}&h&\mathbf{h}&\mathbf{h}&\mathbf{g}&\mathbf{d}&\mathbf{c}&\mathbf{b}&\mathbf{h}&\mathbf{f}&\mathbf{d}&\mathbf{c}&b&\mathbf{d}&\mathbf{f}&\mathbf{g}&h&\mathbf{c}&\mathbf{d}&\mathbf{d}&\mathbf{b}\\
\mathbf{f}&h&\mathbf{g}&\mathbf{b}&\mathbf{d}&\mathbf{c}&\mathbf{b}&\mathbf{d}&\mathbf{f}&h&\mathbf{g}&\mathbf{d}&\mathbf{d}&\mathbf{c}&\mathbf{h}&\mathbf{f}&\mathbf{g}&\mathbf{b}&\mathbf{d}&\mathbf{c}&\mathbf{d}&\mathbf{h}&\mathbf{e}&\mathbf{h}&\mathbf{g}\\
\mathbf{g}&\mathbf{f}&h&\mathbf{c}&\mathbf{b}&\mathbf{d}&\mathbf{c}&\mathbf{b}&\mathbf{d}&\mathbf{g}&f&\mathbf{h}&\mathbf{d}&\mathbf{d}&a&h&h&\mathbf{g}&\mathbf{e}&\mathbf{h}&c&\mathbf{d}&\mathbf{d}\\
\mathbf{b}&\mathbf{d}&\mathbf{c}&f&\mathbf{h}&g&f&\mathbf{h}&\mathbf{g}&\mathbf{b}&\mathbf{d}&\mathbf{c}&\mathbf{g}&\mathbf{h}&\mathbf{h}&a&\mathbf{d}&\mathbf{d}&\mathbf{d}&\mathbf{c}&\mathbf{h}&\mathbf{e}\\
d&\mathbf{c}&\mathbf{b}&\mathbf{h}&g&f&\mathbf{h}&\mathbf{g}&\mathbf{f}&\mathbf{d}&\mathbf{c}&\mathbf{b}&h&\mathbf{g}&\mathbf{f}&\mathbf{d}&\mathbf{c}&\mathbf{b}&\mathbf{h}&\mathbf{h}&\mathbf{g}&d&d&\mathbf{e}&\mathbf{h}\\
\mathbf{c}&\mathbf{b}&d&g&f&\mathbf{h}&\mathbf{g}&f&\mathbf{h}&\mathbf{c}&\mathbf{b}&\mathbf{d}&\mathbf{h}&\mathbf{h}&\mathbf{g}&d&a&c&d&d&e&\mathbf{h}\\
d&\mathbf{b}&\mathbf{c}&h&f&\mathbf{g}&\mathbf{h}&\mathbf{f}&\mathbf{g}&\mathbf{d}&\mathbf{b}&\mathbf{c}&\mathbf{h}&\mathbf{e}&\mathbf{d}&\mathbf{d}&\mathbf{c}&\mathbf{a}&\mathbf{d}&\mathbf{d}&g&\mathbf{h}&h\\
b&\mathbf{c}&d&f&\mathbf{g}&\mathbf{h}&\mathbf{f}&\mathbf{g}&\mathbf{h}&\mathbf{b}&\mathbf{c}&\mathbf{d}&\mathbf{h}&e&\mathbf{h}&\mathbf{d}&\mathbf{c}&\mathbf{d}&\mathbf{d}&a&\mathbf{d}&g&\mathbf{h}&h\\
\mathbf{c}&d&\mathbf{b}&\mathbf{g}&\mathbf{h}&\mathbf{f}&\mathbf{g}&\mathbf{h}&\mathbf{f}&\mathbf{c}&\mathbf{d}&\mathbf{b}&e&\mathbf{h}&\mathbf{c}&\mathbf{d}&\mathbf{d}&\mathbf{d}&\mathbf{d}&a&\mathbf{h}&\mathbf{h}&g\\
h&\mathbf{f}&\mathbf{g}&\mathbf{d}&\mathbf{b}&\mathbf{c}&\mathbf{d}&\mathbf{b}&\mathbf{c}&\mathbf{h}&\mathbf{f}&\mathbf{g}&\mathbf{d}&\mathbf{d}&\mathbf{c}&\mathbf{h}&\mathbf{e}&\mathbf{g}&\mathbf{h}&\mathbf{h}&\mathbf{d}&\mathbf{d}&a\\
\mathbf{f}&g&\mathbf{h}&\mathbf{b}&\mathbf{c}&\mathbf{d}&\mathbf{b}&\mathbf{c}&\mathbf{d}&\mathbf{f}&\mathbf{g}&\mathbf{h}&\mathbf{d}&\mathbf{c}&\mathbf{d}&\mathbf{e}&\mathbf{h}&\mathbf{h}&\mathbf{g}&\mathbf{h}&\mathbf{d}&\mathbf{d}&a\\
\mathbf{g}&h&f&\mathbf{c}&\mathbf{d}&\mathbf{b}&c&\mathbf{d}&\mathbf{b}&\mathbf{g}&\mathbf{h}&\mathbf{f}&\mathbf{c}&\mathbf{d}&\mathbf{d}&\mathbf{e}&\mathbf{h}&\mathbf{h}&\mathbf{h}&\mathbf{g}&\mathbf{h}&\mathbf{d}&\mathbf{d}&a
\end{pmatrix}$$

K: an OD(24;1,1,2,2,3,3,6,6)

2.5 Constructions, Existence, and Special Forms

2.68 **Theorem** If $W = W(n, n-1)$, then either $n \equiv 2 \pmod 4$ and W is equivalent to a symmetric matrix, or $n \equiv 0 \pmod 4$ and W is equivalent to a skew matrix.

2.69 **Remark** $W(n,w)$ have been classified for $w \le 5$ [447] and for $n \le 13$ [1693]. The block structure of $W(n, n-a)$ has been determined for $a \le 4$ [614]; for example, if $n > 3$ and $a = 2$, then the matrix is equivalent to one partitioned into 2×2 blocks, whose diagonal blocks are zero and all others are rank 1 if $n \equiv 2 \pmod 4$, or rank 2 otherwise.

2.70 **Theorem** (see [891]) For square w, if n is large enough, then $W(n,w)$ exists. If w is a sum of two squares and $n \equiv 0 \pmod 2$ is large enough, then $W(n,w)$ exists. For any w, if $n \equiv 0 \pmod 4$ is large enough, then $W(n,w)$ exists.

2.71 **Construction** If W is a skew $W(n,w)$, then

1. $aW + bI$ is an OD$(n; w, 1)$;
2. $\begin{pmatrix} aW + bI & aW \\ aW & -aW + bI \end{pmatrix}$ is an OD$(2n; 2w, 1)$.
3. $\begin{pmatrix} aW + bI & -aW - aI \\ aW + aI & aW + bI \end{pmatrix}$ is an OD$(2n; 2w+1, 1)$.

Conversely, OD$(n; w, 1)$ implies a skew $W(n,w)$; from part 3, a skew $W(n,w)$ gives a skew $W(2n, 2w+1)$.

2.72 **Example** From Tables 2.89 to 2.91, skew W(n,w) matrices exist for all $w < n$, $n = 8, 24, 40, 56, 72, 88$. Therefore, there exist skew W(n,w) for all $w < n$, $n = 2^t p$, $p \le 11$, $t \ge 3$.

2.73 **Theorem** If W is a $W(n,w)$ with diagonal 0, then

1. $\begin{pmatrix} aW+bI & aW-bI \\ aW^T-bI & -aW^T-bI \end{pmatrix}$ is an OD$(2n;2w,2)$, and
2. $\begin{pmatrix} aW+bI & bW-aI \\ bW^T-aI & -aW^T-bI \end{pmatrix}$ is an OD$(2n;w+1,w+1)$.

2.74 **Theorem** If an OD$(4n;s_1,s_2,\ldots,s_k)$ exists and $\sum_{i=1}^k s_i = 4n-1$, then there exists an OD$(4n;s_1,\ldots,s_k,1)$.

2.75 **Theorem** If $\sum_{i=1}^k x_i P_k$ is an OD$(n;a_1,\ldots,a_k)$ and $A_1,\ldots,A_k$ are amicable $m\times m$ $(0,\pm1)$-matrices with $\sum_{i=1}^k a_i A_i {A_i}^T = wI$, then $\sum_{i=1}^k A_i \otimes P_i$ is a $W(mn,w)$.

2.76 **Theorem** (see [612, 891]) If q is any prime power, then there is a circulant $W(q^2+q+1,q^2)$. Further, if q is odd, then there exist a $W(q^k+\cdots+q^2+q+1,q^k)$, a symmetric $W(2q^2,q^2)$ when $k\geq 0$, and and a symmetric $W(q^2+h(q+1),q^2)$ when $h\geq q$.

2.77 **Remark** The case $k=1$ in Theorem 2.76 gives conference matrices, $W(q+1,q)$.

2.78 **Theorem** If there is a $W(p+1,p)$, then for all $k\geq 0$, there exist $W((p+1)p^k,(p+1)p^k-1)$ and $W(p^k+1,p^k)$.

2.79 **Theorem** If $w\leq \min\{n_1,\ldots,n_k\}$ and $W(n_1+1,w),\ldots,W(n_k+1,w)$ exist, then so does $W(n_1\cdots n_k+1,w^k)$. If an even number of the given matrices are skew and the remainder are symmetric, then the resulting matrix is symmetric. If an odd number of them are skew and the remainder are symmetric, then the resulting matrix is skew.

2.80 **Theorem** Let M be a $(0,1)$-matrix having row sums $r_1,\ldots,r_m$ and column sums $c_1,\ldots,c_n$, and let $a,b\in\mathbb{Z}^+$. If for $1\leq i\leq m$ there exists a $W(r_i,a)$ and for $1\leq j\leq n$ there exists a $W(c_j,b)$, then:

1. There is a $W(r_1+\cdots+r_m,ab)$.
2. If M is symmetric, then there is a symmetric $W(r_1+\cdots+r_m,a^2)$.
3. If M is symmetric with zero diagonal, then there is a skew $W(r_1+\cdots+r_m,a^2)$.

2.81 **Remarks** Theorem 2.80 uses a very general technique, *weaving* (see [613]). More generally if one replaces $W(c_j,b)$ with $OD(c_j;b_1,\ldots,b_u)$ for all j, where $b_1,\ldots,b_u$ are given positive integers, the construction for part 1 gives $OD(r_1+\cdots+r_m;ab_1,\ldots,ab_u)$.

2.82 **Theorem** Suppose there are k $(0,\pm1)$-sequences of length n having zero periodic autocorrelation (§V.7) and weight w.

1. If $k=1$, then there is a circulant $W(n,w)$.
2. If $k=2$, then there is a block-circulant $W(2n,w)$ (2×2 blocks).
3. If $k=4$, then there is a $W(4n,w)$.

2.83 **Theorem** [891] Let $a,b\in\mathbb{Z}^+$ such that a,b and $a+b$ are all sums of two squares. Then there exists $N\in\mathbb{Z}^+$ such that OD$(2n;a,b)$ exists for all $n\geq N$.

2.6 Existence of Weighing Matrices (One Parameter Designs)

2.84 **Remark** Tables 2.85 through 2.90 use the conventions: if n appears without parentheses in the record corresponding to w, then a $W(n,w)$ is known to exist; if n appears in parentheses, then its existence is unresolved; if n does not appear, then a $W(n,w)$ does not exist. Consecutive admissible n that exist are indicated by dots; similarly for consecutive unresolved orders, but within parentheses. For example, in Table 2.86, the entry for $w=37$, ends with "68,(70),72...", indicating that $W(n,37)$ exists for

n =68, 72, and all subsequent even numbers, but is unresolved for $n = 70$. In places "$\ldots 2k, (2k+1)\ldots$" is used to indicate that all even orders in the indicated range are known, while all odd orders are unresolved; similarly, "$\ldots 4k, (4k+2)\ldots$" indicates that orders $\equiv 0 \pmod 4$ are known but those $\equiv 2 \pmod 4$ are unresolved.

2.85 Table $W(n, w)$, $w = a^2 \leq 256$ (all n admissible).

w	n
1	1...
4	4,6,7,8,10...
9	10,12...
16	16,18,20,21,22,(23),24,(25),26,(27),28,(29),30...
25	26,28,30...34,(35)...$2k$, $(2k+1)$...54...
36	36,38,40,42,44,(45)...$2k$,$(2k+1)$...56,(57,58,59),60,(61),62,63,64,(65),66,(67), 68,(69),70,(71),72...
49	50,52,54,56,57,(58,59),60,(61,62,63),64,(65,66,67),68,(69,70,71),72,(73,74,75),76, (77),78,(79),80,(81,82,83),84,(85,86,87),88,(89,90,91),92,(93,94,95),96,(97)...$2k$, $(2k+1)$...104...114, (115), 116, 117, 118, (119), 120, 121, 122, (123), 124, 125, 126, (127), 128, 129, 130, (131), 132...138, (139), 140, 141, 142, (143), 144...150, (151), 152...
64	64,66,68,70,72,73,74,(75)...$2k$, $(2k+1)$...116...
81	82,84,(86),88,90,91,92,(93,94,95),96,(97,98,99),100,(101,102,103),104,(105,106, 107),108,109,110,(111),112,(113,114,115),116,117,118,(119),120,121,122,(123), 124,(125),126,127,128,(129),130...
100	100,(102),104,(106),108,110,112,(113)...$2k$, $(2k+1)$...186...
121	122,(124,126),128,(130),132,133,(134...143),144,145,(146...155),156,(157,158, 159), 160, (161...165), 166, (167), 168, (169...175), 176, (177, 178, 179), 180, (181...191),192,(193,194,195),196,197,198,(199),200,(201,202,203),204,(205,206, 207),208,(209),210,(211),212,(213,214,215),216,(217,218,219),220,(221,222,223), 224,(225),226,(227),228,(229,230,231),232,(233,234,235),236,(237,238,239),240, (241),242,(243),244,(245,246,247),248,(249),250,(251),252...256,(257),258,(259), 260,261,262,(263),264,265,266,(267),268,(269,270,271),272,273,(274,275),276, 277,278,(279)...$2k$,$(2k+1)$...288,289,290,(291),292,293,294,(295),296,(297), 298...302,(303),304,305,(306,307),308,309,310,(311),312,313,314,(315),316,317, 318,(319),320,321,322,(323),324,325,326,(327),328...334,(335),336,337,338,(339), 340...346, (347), 348, 349, 350, (351), 352...366, (367), 368, 369, 370, (371), 372...
144	144,(146,148,150,152,154,156,158,159),160,(161...167),168,(169...179),180,(181, 182,183),184,(185,186,187),188,(189)...$2k$, $(2k+1)$...212...
169	170,(172,174,176,178,180),182,183,(184...195),196,(197...207),208,(209),210, (211...221),222,(223)...$2k$, $(2k+1)$...350...354,(355),...$2k$,$(2k+1)$...364,365, 366,(367),368,(369),370,(371),372,(373),374,(375),376,(377),378...
196	196, (198), 200, (202, 204, 206), 208, (210...225), 226, (227), 228, (229...239), 240, (241...255),256,(257...271),272,(273...285),286,(287),288,(289...299),300,(301, 302,303),304,(305...311),312,(313...319),320,(321,322,323),324,(325,326,327), 328, (329, 330, 331), 332, (333, 334, 335), 336, (337, 338, 339), 340, (341)...$2k$, $(2k+1)$...352,(353,354,355),356,357...
225	226, (228, 230, 232, 234, 236, 238), 240, (241...255), 256, 260, (261...271), 272, (273...285), 286, (287), 288, (289...299), 300, (301, 302, 303), 304, (305...313), 314,(315)...$2k$, $(2k+1)$...342...
256	256,258,260,262,264,266,268,270,272,273,274,(275),...$2k$,$(2k+1)$...,314,315, 316,(317),...$2k$,$(2k+1)$...,340,341,342,(343),...$2k$,$(2k+1)$...,356,357,358, (359),...$2k$,$(2k+1)$...,380,381,382,(383),...$2k$,$(2k+1)$...,398,399,400,(401), ...$2k$,$(2k+1)$...,420...

2.86 Table $W(n,w)$, $a^2 \neq w = b^2 + c^2 < 60$, $w \in \{80, 104, 125, 128\}$ (n even).

w	n (even)
For $w = 2, 5, 8, 10, 13, 17, 18, 20, 26, 29, 32, 34, 40, 52, 80, 104, 128$: $W(n,w)$ exists for even $n > w$ and also for $n = w$ in cases $w = 2, 8, 20, 32, 40, 52, 80, 104, 128$.	
37	38. . .52,(54),56,(58),60,62,64,(66),68,(70),72. . .
41	42,44,46,. . . $4k$,$(4k+2)$ . . .,60,62,64,(66),68,(70),72,(74),76,(78),80,(82),84. . .
45	46,48,50,52,54,56,(58),60,(62),64. . .72,(74),76. . .
50	52,(54),56,(58),60. . .
53	54,56,(58),. . . $2k$,$(2k+1)$ . . .,104,(106),108. . .
58	60,(62),64,(66),68,(70),72,(74),76. . .
125	126, 128, (130. . .142), 144, (146. . .154), 156, (158), 160, (162, 164, 166), 168, (170, 172,174),176,(178),180. . .

2.87 Table $W(n,w)$, $a^2 + b^2 \neq w < 100$, ($n \equiv 0 \pmod 4$ only).

w	n ($= 4k$ only)
For w =3,6,7,11,12,14,15,19,21,22,23,24,27,28,30,31,33,35,38,39,42,43,44,46,47,48, 51,54,55,56,57,59,60,62,63,66,67,69,70,71,75,76,77,78,83,86,88,92,94,96: $W(4k,w)$ exists whenever $w \leq 4k$.	
79	80,84,88,(92),96,100,104,108,112,(116),120. . .
87	88,92,96,(100),104,(108),112. . .
91	92, 96, (100), 104, 108, 112, (116), . . . $8k$, $(8k+4)$ . . ., 152, 156, 160, (164), 168, (172), 176. . .
93	96,(100),104,(108),112,(116),120. . .
95	96,(100),104,108,112,(116),120. . .
99	100,104,(108),112,(116)120,(124),128. . .

2.88 Table Symmetric weighing matrices $W(n,w)$, $w = a^2 \leq 81$ (all n admissible).

w	n
1	1. . .
4	4,6,7,8,10. . .
9	10,12,13,(14),15,16,17,18,(19),20,(21),22. . .
16	16,18,20,21,(22,23),24,(25),26,(27),28,(29),30. . .
25	26, (28, 30), 31, (32), 33, (34, 35), 36, (37. . .41), 42, (43), 44, (45, 46, 47), 48, (49), 50, (51),52,(53),54,(55),56. . .60,(61),62,(63),64,(65),66,(67),68. . .74,(75),76. . .
36	36,(38),40,(42),(44. . .47),48,(49),50,(51),52,(53,54,55),56,(57,58,59),60,(61),62, (63),64,(65),66,(67,68,69),70,(71),72,(73,74,75),76,(77,78,79),80,(81,82,83),84, (85),86,(87),88,(89),90,91,92,(93,94,95),96,(97),98,(99),100,(101),102,(103),104, 105, 106, (107), . . . $2k$, $(2k+1)$ . . ., 126, 127, 128, (129), 130. . .134, (135), 136, (137), 138. . .148,(149),150. . .158,(159),160. . .
49	50, (52, 54, 56), 57, (58. . .63), 64, (65. . .71), 72, (73. . .77), 78, (79), 80, (81. . ., 87), 88, (89. . .97),98,(99),100,(101,102,103),104. . .108,(109),110,(111),112,113,114,(115), 116,(117,118,119),120,121,122,(123),124,(125,126,127),128,129,130,(131),132, (133),134. . .138,(139),140,(141),142,(143),144,145,(146),147,148,(149),150,(151), 152,(153),154. . .
64	64,(66,68,70),72,73,(74. . .79),80,(81),. . . $2k$,$(2k+1)$ . . .126,127,128,(129),. . . $2k$, $(2k+1)$ . . ., 136, 137, 138, (139), 140, (141), 142, (143), 144. . .148, (149), 150, (151),152. . .
81	82,(84,86,88,90),91,92,(93,94,95),96,(97,98,99),100,(101. . .108),109,(110,111), 112,(113. . .116),117,118,(119),120,121,122,(123),124,(125),126,127,128,(129), 130. . .

2.89 **Table** Skew weighing matrices $W(n,w)$, $w=a^2\le 81$ ($n\equiv 0 \pmod 2$ only).

w	n
1	2...
4	6...
9	12,14,16,(18),20...
16	20...
25	28,(30),32,(34),36,(38),40...
36	(38),40,(42),44,(46),48,50,52,(54),56,(58),60,62,64,(66),68,(70),72,(74),76,78, 80,(82),84,(86),88...
49	52,(54),...$4k$,$(4k+2)$...,76,78,80,(82),...$4k$,$(4k+2)$...104,106,108,(110),112, 114,116,(118),120,122,124,(126),128...
64	(66),68,(70),72,(74),76,(78),80,(82),84,(86),88...
81	84,(86),...$4k$,$(4k+2)$...,108,110,112,(114),116,118,120,122,124,(126),128...

2.90 **Table** Skew weighing matrices $W(n,w)$, $a^2\ne w=b^2+c^2+d^2<100$ (except $w=93,94$, $n\equiv 0 \pmod 4$ only).

w	n
For $w=$ 2,3,5,6,8,10,11,12,13,14,17,18,19,20,21,22,24,26,27,29,30,32,33,34,35,37,38, 40,41,43,44,45,46,48,50,51,52,53,54,56,57,58,59,62,65,67,68,69,70,72,73,74,75,76,80, 83,84,88,96: skew $W(4k,w)$ exists whenever $4k>w$.	
42	48...
61	64...112,(116),120...
66	72...
77	80,84,88,(92),96,(100),104,108,112,(116),...$8k$,$(8k+4)$...,160...
78	80,84,88,(92),96,(100),104,108,112,(116),...$8k$,$(8k+4)$...,160...
82	84,88,(92),96,(100),104,108,112,(116),...$8k$,$(8k+4)$...,168...
85	88,(92),96,(100),104,108,112,(116),...$8k$,$(8k+4)$...,176...
86	88,(92),96,(100),104,108,112,(116),...$8k$,$(8k+4)$...,176...
89	(92), 96, (100), 104, 108, 112, (116), ... $8k$, $(8k+4)$..., 176, 180, 184, (188), 192, (196),200...
90	92,96,(100),104,108,112,(116),...$8k$,$(8k+4)$...,176...
91	92,96,(100),...$8k$,$(8k+4)$...,184...
97	(100),104,108,112,(116),...$8k$,$(8k+4)$...,192,196,200,(204),208...
98	(100),...$8k$,$(8k+4)$...,152,156,160,(164),...$8k$,$(8k+4)$...,208,212,216,(220), 224,228,232,(236),240,244,248,(252),256...
99	100,104,(108),...$8k$,$(8k+4)$...,152,156,160,(164),...$8k$,$(8k+4)$...,200...

2.91 **Table** Unresolved cases of skew weighing matrices $W(n,w)$, $a^2+b^2+c^2\ne w\le 100$. All other admissible cases ($w\le n\equiv 0 \pmod 8$) exist.

$W(136,79)$, $W(152,79)$, $W(104,95)$, $W(136,95)$, $W(152,95)$, $W(184,95)$

2.7 Orthogonal Designs with More than One Parameter

2.92 An orthogonal design is 2-*type*, (or *constructible from two type I matrices*) if it is obtained from the 2-*array*: $\begin{pmatrix} A & B \\ B^T & -A^T \end{pmatrix}$ where both A and B are type I matrices.

2.93 **Remark** A very fruitful way to construct orthogonal designs of order $n\equiv 2 \pmod 4$ in two parameters is to search for type I matrices of odd order to use in the 2-array.

2.94 **Table** OD$(n; a, b)$ for small $n \equiv 0 \pmod 2$, a, b satisfying Condition 1 of Theorem 2.21. Bold numbers abbreviate parameter lists; see [1332].

n	OD$(n; a, b)$ Known to Exist	No 2-Types	Unresolved
2	**1**=(1,1)	none	none
6	**1**,**2**=(1,4),**3**=(2,2)	none	none
10	**1**,**2**,**3**,**4**=(4,4)	none	none
14	**1**,**2**,**3**,**4**,**5**=(1,9),**6**=(4,9), **7**=(5,5)	**6**	none
18	**1**,**2**,**3**,**4**,**7**,**8**=(2,8)	**5**, **6**	**5**,**6**
22	**1**,**2**,**3**,**4**,**7**,**8**,**9**=(1,16),**10**=(4,16),**11**=(8,8), (9,9)	**5**,**6**, **12**=(2,18)	**5**,**6**,**12**
26	**1**,**2**,**3**,**4**,**5**,**7**,**8**,**9**,**10**,**11**,(9,9),(10,10),**12**	**6**	**6**
30	**1**,**2**,**3**,**4**,**5**,**6**,**7**,**8**,**9**,**10**,**11**,(9,9),(10,10),(13,13)	**6**	**12**,**13**=(1,25) **14**=(4,25),**15**=(8,18) **16**=(9,16),**17**=(5,20)
34	**1**,**2**,**3**,**4**,**5**,**6**,**7**,**8**,**9**,**10**,**11**,(9,9),(10,10),(13,13), (16,16)	**6**	**12**,**13**, **14**,**15**,**16**,**17**

2.95 An orthogonal design is 4-*type* (or *constructible from four type I matrices*) if it is obtained using type I matrices A, B, C, D in the Goethals–Seidel array (see §V.1.5).

2.96 **Theorem** (see [768]) There is a 4-type OD$(4n; a, b, c, d)$ only if there is an integer matrix E satisfying EE^T=diag(a, b, c, d) (and $abcd$ is a square).

2.97 **Remark** The most common constructions for orthogonal designs of order $n \equiv 4 \pmod 8$ in four or fewer variables employ 4-type orthogonal designs.

2.98 **Table** Nonexistent OD$(n; a, b)$s, for small $n \equiv 4 \pmod 8$. In these orders, 4-type OD$(n; a, b)$s exist for all other 2-tuples (a, b) satisfying Condition 2 of Theorem 2.21 [1332].

n	OD$(n; a, b)$ Eliminated
4	none
12	(1,7),(4,7),(3,5)
20	(1,7), (1,15), (2,14), (3,5), (3,13), (3,16), (4,7), (4,15), (5,11), (5,12), (6,10), (6,13),(7,9),(7,12)
28	(1,7),(1,15),(1,23),(2,14,),(3,5),(3,13),(3,20),(3,21),(4,7),(4,15),(4,23),(5,11), (5,12), (5,19), (5,22), (6,10), (7,9), (7,16), (7,17), (7,20), (8,14), (9,15), (10,17), (11,13),(11,16),(12,13),(12,15)

2.99 **Table** Unresolved OD$(n; a, b, c, d)$s, for small $n \equiv 4 \pmod 8$. Proper quadruples not listed but satisfying Condition 4 of Theorem 2.21 are realized as 4-type designs.

n	Unresolved OD$(n; a, b, c, d)$
12	none
20	(1,3,6,8),(1,4,4,9),(2,2,5,5)
28	(1,4,9,9),(1,8,8,9),(2,8,9,9),(3,6,8,9),(4,4,4,9)
36	(1,2,8,16), (1,2,8,25), (1,4,4,25), (1,8,8,16), (1,9,13,13), (2,2,9,16), (2,2,9,16), (2,2,13,13), (2,3,4,24), (2,6,7,21), (2,8,9,9), (3,6,8,16), (3,8,10,15), (4,8,8,9), (8,8,9,9)

2.100 **Theorem** For $n \equiv 0 \pmod 4$, the existence of an OD$(n; s_1, \cdots, s_k)$ with $\sum_{i=1}^{k} s_i = n - 1$ implies the existence of an OD$(n; 1, s_1, \cdots, s_k)$.

2.101 **Theorem** Suppose OD$(n; a, b, c)$ exists for all $a, b, c > 0$, $a + b + c = n$. Then for all $t \geq 0$, OD$(2^t n; p, q, r)$ exists for all $p, q, r > 0$, $p + q + r = 2^t n$.

2.102 An orthogonal design is 8-*type* (or *constructible from eight type I matrices*) if it is obtained from the K-array (of Remark 2.58), using special amicable matrices.

2.103 Remark A good way to construct orthogonal designs of order $n \equiv 8 \pmod{16}$ in eight or fewer variables is by obtaining matrices of order $\frac{n}{8}$ for use in the K-array. Most designs in Theorems 2.104, 2.105 and 2.106 are of 8-type.

2.104 Theorem [889] All full 3-tuples (no zeros) are the types of orthogonal designs of order $n = 56$.

2.105 Theorem [1128] All 3-tuples are the types of orthogonal designs of order $n = 40$.

2.106 Theorem [1127, 891] All full 4-tuples are the types of orthogonal designs of order $n = 4, 24, 48, 64, 128, 256, 512$.

2.107 Theorem [891] All 5-tuples are the types of orthogonal designs of order $n = 16$.

2.108 Theorem [891, 1286] All full 6-tuples are the types of orthogonal designs of order $n = 8, 32$.

2.109 Theorem [891] All 6-tuples are the types of orthogonal designs of order 16, except those of types $(1, 1, 1, 1, 4, 7)$ and $(1, 1, 2, 2, 2, 7)$, which do not exist.

2.110 Table [891, 1286] Unresolved full orthogonal designs of order 32 and in 7 variables. In this table a_k means a is repeated k times.

Don't Exist	Unresolved 7-tuples
$(1_6, 26)$, $(1_5, 2, 25)$, $(1_5, 3, 24)$, $(1_5, 4, 23)$, $(1_5, 5, 22)$, $(1_5, 6, 21)$, $(1_5, 7, 20)$, $(1_5, 8, 19)$, $(1_5, 10, 17)$, $(1_5, 11, 16)$, $(1_5, 13, 14)$	$(1_4, 2, 13_2)$, $(1_4, 3, 6, 19)$, $(1_4, 4, 5, 19)$, $(1_4, 4, 11, 13)$, $(1_4, 5, 10, 13)$, $(1_3, 2_3, 23)$, $(1_3, 2, 5_2, 17)$, $(1_3, 3, 4, 5, 17)$, $(1_3, 4, 5, 7, 13)$, $(1_3, 5_3, 14)$, $(1_3, 5_2, 7, 12)$, $(1_3, 5_2, 8, 11)$, $(1_3, 5, 6, 7, 11)$, $(1_2, 2_3, 5, 19)$, $(1_2, 2, 5_3, 13)$, $(1_2, 3, 4_3, 15)$, $(1_2, 4_3, 5, 13)$, $(1_2, 4_3, 7, 11)$, $(1_2, 4_2, 5_2, 12)$, $(1_2, 4_2, 5, 7, 10)$, $(1_2, 4, 5_2, 7, 9)$, $(1_2, 5_4, 10)$, $(1_2, 5_3, 6, 9)$, $(1_2, 5_2, 6, 7_2)$, $(1_2, 5, 6_3, 7)$, $(1, 2_3, 3, 5, 17)$, $(1, 2_3, 5_2, 15)$, $(1, 2_3, 5, 9, 11)$, $(1, 2_2, 3_2, 8, 13)$, $(1, 2_2, 3, 5_2, 14)$, $(1, 2_2, 3, 5, 8, 11)$, $(1, 2_2, 4_3, 15)$, $(1, 2_2, 4_2, 5, 14)$, $(1, 2_2, 4, 5_2, 13)$, $(1, 2_2, 4, 5, 7, 11)$, $(1, 2_2, 5_3, 12)$, $(1, 2_2, 5_2, 6, 11)$, $(1, 2_2, 5_2, 7, 10)$, $(1, 2, 4_3, 7, 10)$, $(1, 2, 4_2, 5, 7, 9)$, $(1, 2, 4, 5_3, 10)$, $(1, 2, 5_4, 9)$, $(1, 2, 5_3, 7_2)$, $(1, 2, 5_2, 6_2, 7)$, $(1, 3_4, 5, 14)$, $(1, 3_3, 7_2, 8)$, $(1, 3_2, 4_3, 13)$, $(1, 3, 4_3, 5, 11)$, $(1, 3, 4_3, 7, 9)$, $(1, 3, 4, 5, 6_2, 7)$, $(1, 3, 5_3, 6, 7)$, $(1, 3, 5_2, 6_3)$, $(1, 4_3, 5_2, 9)$, $(1, 4_3, 5, 7_2)$, $(1, 4_2, 5_2, 6, 7)$, $(1, 4, 5_4, 7)$, $(1, 4, 5_3, 6_2)$, $(1, 5_5, 6)$, $(2_3, 3, 7_2, 9)$, $(2_3, 4_2, 7, 11)$, $(2_3, 5_3, 11)$, $(2_2, 4, 5_2, 7_2)$, $(2_2, 5_4, 8)$, $(2, 3_4, 5, 13)$, $(2, 3_3, 7_3)$, $(2, 4_2, 5_3, 7)$, $(2, 5_6)$, $(3_4, 4, 5, 11)$, $(3_4, 5, 7, 8)$, $(3_2, 4_3, 5, 9)$, $(3_2, 4_3, 7_2)$, $(3, 4_3, 5_2, 7)$, $(4_3, 5_4)$

2.8 Conjectures

2.111 Conjecture (*Weighing Matrix Conjecture* [891]).

1. If $n \equiv 0 \pmod{4}$ and $w \leq n$, then $W(n, w)$ exists.
2. If n is even and $w = a^2 + b^2 < n$, then $W(n, w)$ exists.

2.112 Conjecture (*Skew Weighing Matrix Conjecture* [891]) There exists a skew $W(n, w)$ (or, equivalently, $\mathrm{OD}(n; w, 1)$) for all $w < n$:

1. if $n \equiv 0 \pmod{8}$;
2. if $n \equiv 4 \pmod{8}$, $w = a^2 + b^2 + c^2$, $a, b, c \in \mathbb{Z}$, $w \neq n - 2$; and
3. if $n \equiv 4 \pmod{8}$, $w = n - 2 = a^2 + b^2$, $a, b \in \mathbb{Z}$.

2.113 Conjecture If there is a $W(n, w)$, n odd, then there is a symmetric $W(n, w)$.

2.114 Conjecture (*Conference Matrix Conjecture*) A conference matrix $W(n, n-1)$ exists for all $n \equiv 2 \pmod 4$ as long as $n-1$ is a sum of two squares.

2.115 Conjecture There exists an OD$(4t; t, t, t, t)$ for every positive integer t.

2.116 Conjecture There exists an OD$(8t; t, t, t, t, t, t, t, t)$ for every positive integer t.

2.117 Conjecture There exists an OD$(128; 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8)$.

2.118 Conjecture (*Seberry Conjecture*) All 3-tuples $(a, b, 2^t s - a - b)$ are types of orthogonal designs in order $2^t s$, s odd, $t \geq 3$.

2.119 Remarks

1. Part 1 of Conjecture 2.111 is proven for $n = 4k \leq 88$. Part 2 is proven for $n \leq 32$. The corresponding statement for odd orders is false—there is no $W(9, 4)$.
2. Conjecture 2.112 has been confirmed for $n = 8k + 4 \leq 88$ and $n = 8k \leq 96$. It is also true for $2^t p$, where $p = 3, 5, 7, 9, 13$ $(t \geq 3)$ and $p = 15, 21$ $(t \geq 4)$. As for the case $n \equiv 2 \pmod 4$, it is known that there is no skew $W(18, 16)$.
3. Conjecture 2.113 is confirmed up to order 13; there exists a $W(35, 16)$ that is not equivalent to a symmetric matrix. It is also true that, up to order 13, $W(n, w)$, n odd, implies a regular $W(n, w)$.
4. Conjecture 2.114 is confirmed for $n = 2k \leq 62$ with k odd. For the case $n \equiv 0 \pmod 4$ see Table V.1.51, as these are skew-Hadamard matrices.
5. Conjecture 2.115 is confirmed for many even values of t and all odd values of $t \leq 73$.
6. Conjecture 2.116 is confirmed for many even values of t and all odd values of $t \leq 21$.

See Also

§V.1	Hadamard matrices are one-parameter ODs; some of the most important constructions for Hadamard matrices involve ODs.
§V.6.1	Much more information on conference matrices.
§V.8	Sequences with zero autocorrelation are used to construct weighing matrices and ODs.
§VII.2	A $W(k^2 + k + 1, k^2)$ is always complementary to a projective plane of order k. If there is a conference matrix of order $k + 1$, the reverse implication also holds.
[612]	Constructions for weighing matrices with square weights.
[613]	Weaving and its use in constructing weighing matrices.
[891]	The main reference for ODs and weighing matrices.
[1866]	A more recent extensive survey on similar material.
[1331]	Some recent results on existence of ODs.
[890, 2165]	Concerning the number of variables in an OD.

References Cited: [447, 612, 613, 614, 768, 889, 890, 891, 1125, 1126, 1127, 1128, 1284, 1286, 1331, 1332, 1693, 1808, 1866, 2165]

3 D-Optimal Matrices

Hadi Kharaghani
William Orrick

3.1 Definitions and Notation

3.1 An (α,β)-*matrix* is a square matrix with entries in the set $\{\alpha,\beta\}$. A (±1)-matrix B of order n is a *D-optimal matrix* if the determinant of B is the maximum determinant among all (±1)-matrices of order n. This maximum determinant is denoted by α_n.

3.2 **Remark** The maximum determinant of a $(0,1)$ matrix of order n is $\alpha_{n+1}/2^n$.

3.3 A (±1)-matrix A with $AA^t=(n-1)I_n+J_n$ is a *Barba matrix.* I_n denotes the identity matrix of order n, and J_n is the matrix of order n with all entries 1. A (±1)-matrix B with $BB^t=B^tB=\begin{pmatrix} M & 0\\ 0 & M\end{pmatrix}$, where $M=(n-2)I_{n/2}+2J_{n/2}$, is an *EW (Ehlich–Wojtas) matrix.* An EW matrix is an *Ehlich matrix* if it can be written in the form $\begin{pmatrix} A & B\\ -B^t & A^t\end{pmatrix}$, where A and B are circulant matrices.

3.4 **Examples** A_5 is a circulant Barba matrix of order 5, E_6 is an Ehlich matrix of order 6, and E_{10} is an Ehlich matrix of order 10.

$$A_5=\begin{pmatrix} - & 1 & 1 & 1 & 1\\ 1 & - & 1 & 1 & 1\\ 1 & 1 & - & 1 & 1\\ 1 & 1 & 1 & - & 1\\ 1 & 1 & 1 & 1 & -\end{pmatrix}\qquad E_6=\begin{pmatrix} 1 & 1 & 1 & - & 1 & 1\\ 1 & 1 & 1 & 1 & - & 1\\ 1 & 1 & 1 & 1 & 1 & -\\ 1 & - & - & 1 & 1 & 1\\ - & 1 & - & 1 & 1 & 1\\ - & - & 1 & 1 & 1 & 1\end{pmatrix}\qquad E_{10}=\begin{pmatrix} 1 & 1\\ - & 1\end{pmatrix}\otimes A_5$$

3.5 Let $n=r_1+\cdots+r_k$ with each $r_i>0$. For all $1\le\ell\le k$, let $R_\ell=\sum_{i=1}^{\ell}r_i$ and also define $R_0=0$. A matrix of order n is a *block matrix* with block sizes $r_1,\ldots,r_k$ if its elements m_{ij} satisfy (1) $m_{ii}=n$, (2) $m_{ij}=3$ for $R_{\ell-1}+1\le i\ne j\le R_\ell$ for all $1\le\ell\le k$, and (3) $m_{ij}=-1$ otherwise.

3.6 **Example** R_7, a D-optimal matrix of order 7 is on the left. $R_7R_7^t=R_7^tR_7=B$ is on the right. B is a block matrix with block sizes 2, 2, 2, and 1.

$$R_7=\begin{pmatrix} - & 1 & 1 & 1 & - & - & -\\ 1 & - & 1 & 1 & - & - & -\\ 1 & 1 & - & - & - & 1 & -\\ 1 & 1 & - & - & 1 & - & -\\ - & - & - & 1 & 1 & 1 & -\\ - & - & 1 & - & 1 & 1 & -\\ - & - & - & - & - & - & 1\end{pmatrix}\qquad B=\begin{pmatrix} 7 & 3 & -1 & -1 & -1 & -1 & -1\\ 3 & 7 & -1 & -1 & -1 & -1 & -1\\ -1 & -1 & 7 & 3 & -1 & -1 & -1\\ -1 & -1 & 3 & 7 & -1 & -1 & -1\\ -1 & -1 & -1 & -1 & 7 & 3 & -1\\ -1 & -1 & -1 & -1 & 3 & 7 & -1\\ -1 & -1 & -1 & -1 & -1 & -1 & 7\end{pmatrix}.$$

3.7 Two (±1) matrices, A and B, are *equivalent* if there exist monomial matrices P and Q such that $B=PAQ$.

3.2 Determinant Inequalities

3.8 Theorems The upper bound on α_n depends on n modulo 4 as follows.

1. For $n \equiv 0 \pmod 4$, $\alpha_n \le n^{n/2}$. Equality occurs if and only if there is a (± 1)-matrix H of order n with $HH^t = nI_n$ (a Hadamard matrix). (See §V.1).
2. [1149] For $n \equiv 1 \pmod 4$, $\alpha_n \le \sqrt{2n-1}\,(n-1)^{(n-1)/2}$. Equality occurs if and only if there is a Barba matrix of order n.
3. [1149] For $n \equiv 2 \pmod 4$, $\alpha_n \le (2n-2)\,(n-2)^{(n-2)/2}$. Equality occurs if and only if there is an EW matrix of order n.
4. [771] For $n \equiv 3 \pmod 4$, $\alpha_n \le (n-3)^{(n-s)/2}(n-3+4r)^{u/2}(n+1+4r)^{v/2}[1 - ur/(n-3+4r) - v(r+1)/(n+1+4r)]^{1/2}$ where $n = ur + v(r+1)$, $u+v=s$, $r = \lfloor \frac{n}{s} \rfloor$, and $s = 5$ for $n = 7$, $s = 5$ or 6 for $n = 11$, $s = 6$ for $15 \le n \le 59$, and $s = 7$ for $n \ge 63$. Equality occurs if and only if there is a (± 1)-matrix C such that $CC^t = C^tC$ is a block matrix with u blocks of size r and v blocks of size $r+1$.

3.9 Remark A Barba matrix exists only if $n = q^2+(q+1)^2$ for some integer q. The problem of finding a Barba matrix is equivalent to finding a symmetric balanced incomplete block design with parameters $(v,k,\lambda) = (q^2+(q+1)^2, q^2, q(q-1)/2)$.

An EW matrix exists only if $2n-2$ is a sum of two squares. It is not known whether equality in (4) of Theorem 3.8 ever holds.

3.3 Existence Results

3.10 Theorem Let A, B be circulant (± 1)-matrices of order $n/2$ with $AA^t + BB^t = (n-2)I_{n/2} + 2J_{n/2}$. Then there is an Ehlich matrix of order n.

3.11 Theorem [1329] If there exists a cyclic projective plane of order q^2, then there exist two circulant (± 1)-matrices A, B of order $1+q+q^2$, such that

$$AA^t + BB^t = (2q^2+2q)I_{1+q+q^2} + 2J_{1+q+q^2}.$$

3.12 Corollary [1329] There exist Ehlich matrices of order $n = 2(q^2+q+1)$ where q is a prime power.

3.13 Theorem If there is a Barba matrix of order $n \equiv 1 \pmod 4$, then there is an EW matrix of order $2n$.

3.14 Theorem There exists a Barba matrix of order $n = 2q^2+2q+1$, where q is an odd prime power.

3.15 Theorem There exist Barba matrices of orders 5, 13, and 41.

3.16 Remark There are circulant D-optimal matrices of orders 1, 3, 4, 5, and 13.

3.17 Table [1149] Known α_n not included in Theorems 3.14 and 3.15, for $n \equiv 1 \pmod 4$.

n	9	17	21
α_n	$2^{11} \cdot 7$	$16^7 \cdot 80$	$20^9 \cdot 116$

3.18 Theorem There are Ehlich matrices of order $n = 6$, 10, 14, 18, 26, 30, 38, 42, 46, 50, 54, 62, 66, 74, 82, 86, 90, 98, 102, 110, 114, 118, 122, 126, 146, 158, 182, 186, 194, 226, 266, and 290.

3.19 Theorem In addition to the EW matrices whose existence is implied by Corollary 3.12, Theorems 3.13 through 3.15, and Theorem 3.18, there is an EW matrix of order 150.

3.20 **Table** [1702] Known α_n for $n \equiv 3 \pmod 4$.

n	3	7	11	15
α_n	4	$2^6 \cdot 9$	$5 \cdot 2^{16}$	$140 \cdot 12^6$

3.21 **Table** Known lower bounds on the maximal determinant.

n	19	22	23	27	29	31
α_n	$833 \cdot 4^{15}$	$2 \cdot 20^{11}$	$678576 \cdot 40^6$	$364 \cdot 24^{12}$	$5120 \cdot 28^{12}$	$16 \cdot 28^{16}$

3.22 **Table** The number of equivalence classes of D-optimal matrices of order n, N_n, for $11 \le n \le 21$. (Up to order 10, all D-optimal designs of a given order are equivalent.)

n	11	12	13	14	15	16	17	18	19	20	21
N_n	3	1	1	1	1	5	3	3	?	3	7

3.4 Constructions

3.23 **Table** First rows for some Ehlich matrices.

n	Row A	Row B
14	`-111111`	`11-1---`
18	`--1111111`	`-111-11-1`
26	`1111111-11--1`	`11---1-11-1-1`
	`1111111-11--1`	`111--1-1-1--1`
	`1111-1--111-1`	`1111-1--111-1`
30	`11111-11-11-1-1`	`11-111----111-1`
	`1111111--11-1-1`	`111--1--111-1-1`
	`1111111--11-1-1`	`1111--11-1-1--1`

3.24 **Examples** A D-optimal matrix of order 9 and the three inequivalent D-optimal matrices of order 11.

$$\begin{pmatrix} 1&-&-&-&-&-&-&-&-\\ -&1&-&-&-&-&-&-&-\\ -&-&1&1&1&-&-&-&-\\ -&-&1&-&-&-&-&1&1\\ -&-&1&-&-&1&1&-&-\\ -&-&-&-&1&-&1&-&1\\ -&-&-&-&1&1&-&1&-\\ -&-&-&1&-&-&1&1&-\\ -&-&-&1&-&1&-&-&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1&-&-&1&1&-&-&-\\ 1&1&1&1&-&1&-&-&1&-&-\\ 1&1&1&-&1&-&-&-&-&-&-\\ 1&1&-&1&1&-&-&-&-&1&1\\ -&-&1&1&-&-&-&-&-&1&1\\ -&1&-&-&-&-&-&1&1&1&-\\ 1&-&-&-&-&-&1&1&-&1&-\\ 1&-&-&-&-&1&1&-&-&1&-\\ -&1&-&-&1&1&-&-&-&-&1\\ -&-&1&1&1&-&1&-&-&-&-\\ -&-&-&1&-&1&-&1&1&-&-\end{pmatrix}, \begin{pmatrix} 1&1&1&1&1&1&1&1&1&-&-&-\\ 1&-&1&1&-&1&1&-&1&-&-&-\\ 1&1&-&1&1&-&-&-&-&-&-&-\\ 1&1&1&1&1&-&-&-&1&1&1&-\\ 1&-&1&1&-&-&-&1&-&1&1&-\\ 1&1&-&-&-&-&1&1&1&-&1&-\\ 1&1&-&-&-&-&1&1&1&1&-&-\\ 1&-&-&-&1&1&-&-&1&1&-&-\\ -&1&-&1&-&-&1&1&-&1&1&-\\ -&-&1&1&-&1&-&1&1&1&-&-\\ -&-&-&1&1&1&-&1&1&1&-&-\end{pmatrix}, \begin{pmatrix} -&1&1&1&1&-&-&-&-&-&-\\ 1&1&1&1&1&-&1&-&1&-&1\\ 1&1&1&1&1&-&1&1&-&-&-\\ 1&1&1&1&1&1&1&-&-&1&-\\ 1&1&1&1&1&1&-&1&-&-&1\\ -&-&-&1&1&-&-&1&1&1&1\\ -&1&1&-&-&-&-&1&1&1&1\\ -&-&1&-&1&1&1&-&-&1&1\\ -&1&-&1&-&1&1&-&-&1&1\\ -&-&1&1&-&1&1&1&1&-&-\\ -&1&-&-&1&1&1&1&1&-&-\end{pmatrix}$$

3.25 **Remark** A D-optimal matrix is referred to in statistics as an exact D-optimal first order saturated design with n observations. A typical application is the determination of the weights of n objects in n weighings on a chemical balance. D-optimal weighing matrices minimize the generalized variance of the estimated weights [1770].

See Also

§II.6	Symmetric designs.
§V.1	Hadamard designs and matrices.
[1149]	A survey of maximum determinant problems.
[737]	Multicirculant generalization of Ehlich matrices.
[1124]	An extension to complex D-optimal matrices.
[1770, 851]	Application of D-optimal matrices in statistics.

References Cited: [737,771,851,1124,1149,1329,1702,1770]

4 Bhaskar Rao Designs

Warwick de Launey

4.1 GBRDs: Definition and Example

4.1 A *generalized Bhaskar Rao design* GBRD$(v, b, r, k, \lambda; G)$ is a $v \times b$ array whose nonzero entries are drawn from the group G of finite order g so that

1. each row contains precisely r nonzero entries,
2. each column contains precisely k nonzero entries, and
3. for any pair of distinct rows $(x_1, x_2, \cdots, x_b)$ and $(y_1, y_2, \cdots, y_b)$, the list $x_1 y_1^{g-1}, x_2 y_2^{g-1}, \cdots, x_b y_b^{g-1}$ contains each nonzero group element exactly λ/g times.

4.2 **Remarks** Replacing the nonzero entries by 1 produces a balanced block design; consequently, $r = 1 + \lambda(v-1)/k$ and $b = rv/k$, and so GBRD$(v, b, r, k, \lambda; G)$ is usually just written as GBRD$(v, k, \lambda; G)$. When $v > k$, the underlying $(0, 1)$ design is incomplete, and then $b \geq v$. The cases where $v = k$ or $b = v$ or $G = \mathbb{Z}_2$ are dealt with in §V.5, §V.6 and §4.3, respectively.

4.3 **Example** A GBRD$(4, 3, 6; \mathbb{Z}_6)$.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & \omega^4 & \omega^2 & \omega^3 & \omega & \omega^5 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & \omega^2 & \omega^4 & 0 & 0 & 0 & \omega^3 & \omega & \omega^5 & \omega^3 & \omega & \omega^5 \\ 0 & 0 & 0 & 1 & \omega^2 & \omega^4 & \omega^3 & \omega^5 & \omega & 1 & \omega^2 & \omega^4 \end{pmatrix}$$

4.2 Existence of Generalized Bhaskar Rao Designs

4.4 **Theorem** A GBRD$(v, k, \lambda; H)$ is obtained by applying the surjective group homomorphism $\phi : G \to H$ entrywise to a GBRD$(v, k, \lambda; G)$.

4.5 **Remarks** Some general techniques [1864, 1865] are known for obtaining families of designs with $k > 5$; however, attempts to determine the spectrum of admissible parameters v, b, r, k, λ, G have been restricted to $k \in \{3, 4, 5\}$. A family of GBRD$(k + 1, k, k^2 - k; G)$ and all the GBRD$(k + 1, k, \ell k - l; G)$s with $k \in \{3, 4, 5\}$ and ℓ small appear in [899]. Theorem 4.6 is a complete asymptotic result for odd order groups and large k.

4.6 **Theorem** [648] Let G be any group of odd order g. For all $k, t > 0$, there is an integer M such that for all $v > M$, there exists a GBRD$(v, k, tg; G)$ if and only if $tg(v-1) \equiv 0 \pmod{k-1}$ and $tgv(v-1) \equiv 0 \pmod{k(k-1)}$.

4.7 **Theorem** [871] Let G be an abelian group of order g. Then a GBRD$(v, 3, \lambda; G)$ exists if and only if $\lambda \equiv 0 \pmod{g}$; $\lambda(v-1)$ is even; $\lambda v(v-1) \equiv 0 \pmod{6}$ for g odd and $\lambda v(v-1) \equiv 0 \pmod{24}$ for g even; and if $v = 3$ and the Sylow 2-subgroup of G is nontrivial and cyclic, then $\lambda \equiv 0 \pmod{2g}$.

4.8 **Remark** The solution for nonabelian groups is far from completed. Theorem 4.9 gives an infinite class of nonabelian groups for which existence is settled.

4.9 **Theorem** [29] A GBRD$(v, 3, \lambda; D_n)$ exists if and only if $\lambda \equiv 0 \pmod{2n}$ and $\lambda v(v-1) \equiv 0 \pmod{24}$ (D_n is the dihedral group of order $2n$).

4.10 Let $EA(g)$ denote the order g direct product of prime order cyclic groups.

4.11 **Theorem** [870] For $t > 1$, a GBRD$(v, 4, tg; EA(g))$ exists if and only if $tg(v-1)$ is even and $tgv(v-1) \equiv 0 \pmod{12}$, except possibly when $g = 9h$, $t = 2$, and $\gcd(6, h) = 1$. For $t = 1$ the necessary conditions are sufficient for $v > 46$.

4.12 **Remark** There is no GBRD$(5, 4, 6; \mathbb{Z}_6)$ or GBRD$(7, 4, 4; \mathbb{Z}_2 \times \mathbb{Z}_2)$ [657].

4.3 Bhaskar Rao Designs

4.13 A *Bhaskar Rao design* BRD(v, k, λ) is a GBRD$(v, k, \lambda; G)$ where $v > k$ and $G = \mathbb{Z}_2$.

4.14 **Remarks** Bhaskar Rao [1777, 1778] named these designs *balanced orthogonal designs*. Bhaskar Rao designs are often defined to include a wider class of $(0, \pm 1)$-matrices where the underlying design is a PBIBD instead of a BIBD, and the between class inner products are fully specified but not necessarily zero. Bhaskar Rao designs have been studied at this level of generality in [1986, 1990].

4.15 **Theorem** [1778] A BRD(v, k, λ) can exist only if the following equations have nonnegative integer solutions:

$$x_3 + 3x_5 + 6x_7 + \cdots + \tfrac{(k^2-1)}{8} x_k = b\tfrac{(k-1)}{8} \quad \text{for } k \text{ odd},$$
$$-x_0 + 3x_2 + 8x_4 + \cdots + \tfrac{(k^2-4)}{4} x_k = b\tfrac{(k-4)}{4} \quad \text{for } k \text{ even}.$$

4.16 **Corollary** of Theorem 4.7. A BRD$(v, 3, 2t)$ exists for $v \geq 3$ whenever $tv(v-1) \equiv 0 \pmod{12}$.

4.17 **Example** A BRD$(7, 4, 4)$ is given on the right.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 1 \\
1 & 1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 & 0 & -1 & 1 & 0 & -1 \\
1 & 1 & 0 & 0 & -1 & 0 & 0 & -1 & -1 & 1 & 0 & -1 & 1 & 0 \\
0 & 0 & 0 & -1 & 1 & 0 & 1 & -1 & 0 & 1 & 1 & 0 & -1 & -1 \\
0 & 0 & 1 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & 1 & -1 & 0 & -1 \\
0 & 0 & -1 & 1 & 0 & 1 & -1 & 0 & 1 & 1 & 0 & -1 & -1 & 0
\end{pmatrix}$$

4.18 **Theorem** [872] A BRD$(v, 4, \lambda)$ with $v > 4$ exists if and only if $\lambda \equiv 0 \pmod{2}$ and $\lambda(v-1) \equiv 0 \pmod{3}$ with the exception of a BRD$(10, 4, 2)$. A BRD$(4, 4, \lambda)$ exists if and only if $\lambda \equiv 0 \pmod{4}$.

4.19 **Remark** BRDs with block size five are considered in [462]. Theorem 4.20 states some of the results therein obtained.

4.20 **Theorem** [462] Existence results for BRDs.

1. A BRD$(v, 5, \lambda)$ exists only when λ is even, $\lambda(v-1) \equiv 0 \pmod{4}$, and $\lambda v(v-1) \equiv 0 \pmod{40}$.
2. A BRD$(v, 5, 4)$ exists when $v \equiv 0, 1 \pmod{5}$ except when $v = 5$ and possibly when $v \in \{15, 16, 26, 35, 75, 85, 86, 95, 135, 215\}$.
3. A BRD$(v, 5, 4t)$ exists with $t > 1$ exists when $v \equiv 0, 1 \pmod{5}$ except possibly when $(v, t) \in \{(15, 3), (35, 2), (35, 3), (35, 7)\}$.
4. A BRD$(v, 5, 20)$ exists when $v \geq 5$ except possibly when $v = 32$.

4.21 **Theorem** [648, Theorem 5.1.1(ii)] For all $k, t > 0$, there is an integer M such that there is a BRD$(v, k, 2t; \mathbb{Z}_2)$ whenever $2t(v-1)/(k-1)$ and $2tv(v-1)/k(k-1)$ are integers and $v > M$. When $k \equiv 2, 3 \pmod{4}$, it is necessary that $2t(v-1)/(k-1)$ and $2tv(v-1)/k(k-1)$ be integers.

4.22 A *c-Bhaskar Rao design*, c-BRD(v,k,λ) is a $v\times b$ matrix with entries from $\{0,\pm1\}$ in which any two distinct rows have inner product equal to c, and the pattern of nonzero entries forms the incidence matrix of a (v,k,λ)-design. Taking $c=0$ recovers the usual notion of BRD.

4.23 **Theorems** [687] Existence results for $c-$BRDs.

1. For $v\equiv 1,4 \pmod{12}$ and $v>4$ there is a (-1)-BRD$(v,4,5)$.
2. For $v\equiv 1 \pmod 3$ and $v>4$ there is a (-2)-BRD$(v,4,8)$.
3. If $v\equiv 1 \pmod 3$, the necessary conditions for the existence of a 2-BRD$(v,4,4)$, namely that $v\neq 4$, are sufficient.
4. If $v\geq 4$, then the necessary conditions for the existence of a 4-BRD$(v,4,6)$, namely that $v\neq 4$, are sufficient with the exception of $v=5$.

See Also

§IV.1	A GBRD$(v,k,\lambda;G)$ is equivalent to a group divisible design with G acting regularly on the points and semi-regularly on the lines.
§V.5	A GH(g,λ) over G is a GBRD$(\lambda g,\lambda g,\lambda g;G)$.
§V.6	A GC$(G;\lambda)$ is a GBRD$(\lambda g+2,\lambda g+1,\lambda g;G)$. A BGW$(v,k,\lambda;G)$ is a GBRD$(v,k,\lambda;G)$.
§VI.17	A $(g,k;\lambda)$-difference matrix over G is a GBRD$(k,k,g\lambda;G)$.
[687]	Results and references on c-BRDs.

References Cited: [29, 462, 648, 657, 687, 870, 871, 872, 899, 1777, 1778, 1864, 1865, 1986, 1990]

5 Generalized Hadamard Matrices

Warwick de Launey

5.1 Definition and Examples

5.1 A *generalized Hadamard matrix* GH(g,λ) is a $(g,g\lambda;\lambda)$-difference matrix. It is *normalized* if all the symbols in the first row and first column are the identity element of the group. The *core* of a normalized GH-matrix is obtained by removing the first row and column.

5.2 Let EA(g) denote the order g direct product of prime order cyclic groups.

5.3 **Examples** A normalized GH$(4,1)$ over EA(4) with circulant core, a circulant GH$(5,1)$, and a GH$(3,2)$ over $\mathbb{Z}_3$.

$$\begin{pmatrix} 1 & 1 & 1 & 1\\ 1 & ab & a & b\\ 1 & b & ab & a\\ 1 & a & b & ab \end{pmatrix} \qquad \begin{pmatrix} 1 & w & w^4 & w^4 & w\\ w & 1 & w & w^4 & w^4\\ w^4 & w & 1 & w & w^4\\ w^4 & w^4 & w & 1 & w\\ w & w^4 & w^4 & w & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & w & w & w^2 & w^2\\ 1 & 1 & w^2 & w^2 & w & w\\ w & w^2 & w & w^2 & w & w^2\\ w & w^2 & w^2 & w & w^2 & w\\ w^2 & w & w & w^2 & w^2 & w\\ w^2 & w & w^2 & w & w & w^2 \end{pmatrix}$$

5.4 **Remark** By Remark VI.17.11, a GH(g,λ) over the group G is a generalized Bhaskar Rao design GBRD$(g\lambda,g\lambda,g\lambda;G)$.

5.5 **Remark** A GH(g,λ) is a $(g,k;\lambda)$-difference matrix with $k=g\ell$ as large as possible (see Theorem VI.17.5).

5.6 **Theorem** A Hadamard matrix $H(4n)$ is a $\mathrm{GH}(2, 2n)$ over the group $(\{-1, +1\}, \cdot)$.

5.7 **Theorem** [1222] Let G be a group of order g. There exists a $\mathrm{GH}(g, 1)$ over G if and only if there exists a projective plane Π of order g with an incident point-line pair (p, L) such that the group of all (p, L)-elations is isomorphic to G.

5.2 Existence

5.8 **Theorem** Suppose that there is an epimorphism from G of order g to a group H of order h. If there is a $\mathrm{GH}(g, n/g)$ over the group G, then there is a $\mathrm{GH}(h, n/h)$ over the group H.

5.9 **Theorem** [650] For any group G of prime power order q and any integer $t > 0$, there is a $\mathrm{GH}(q, q^{2t-1})$ over G.

5.10 **Table** Direct constructions over $\mathrm{EA}(g)$.

g	λ	Conditions	Refs.
p^n	p^{m-n}	$m \geq n \geq 1$, p a prime	[225]
p^n	$2p^{m-n}$	$m \geq n \geq 1$, p a prime	[225]
p^n	$4p^{m-n}$	$m \geq n \geq 1$, p a prime	[647]
q	8	$19 < q < 200$, q prime power	[654]
p	8	$p > 19$ a prime	[654]
q	k	$q > ((k-2)2^{k-2})^2$, $\exists$ Hadamard matrix of order k	[655]

5.11 **Theorem** [748] If there is a $\mathrm{GH}(g, \lambda_1)$ and a $\mathrm{GH}(g, \lambda_2)$ over the group G, then there is a $\mathrm{GH}(g, g\lambda_1\lambda_2)$ over G.

5.12 **Theorem** [647] Let $q = g\lambda - 1$ be a prime power. If there is a $\mathrm{GH}(g, \lambda)$ over the group G, then there are $\mathrm{GH}(g, \lambda q^t)$ over G for all $t \geq 0$.

5.13 **Table** The existence of $\mathrm{GH}(g, \lambda)$ matrices over $\mathrm{EA}(g)$ with $n = g\lambda$. The large numbers in the table indicate the group orders g for which a $\mathrm{GH}(g, n/g)$ is known to exist over $\mathrm{EA}(g)$. The numbers in the superscript indicate group orders g for which a $\mathrm{GH}(g, n/g)$ is known not to exist over $\mathrm{EA}(g)$. By Theorem 5.8, the entry $3, 5^2$ at the end of the row headed by 0 means that $\mathrm{GH}(3, 30)$ and $\mathrm{GH}(5, 18)$ are known and that no $\mathrm{GH}(2t, 45/t)$ can exist over $\mathrm{EA}(2t)$; for $g \in \{9, 15, 45\}$, it is not known whether a $\mathrm{GH}(g, 90/g)$ exists.

n	0	10	20	30	40	50	60	70	80	90
0		5^2	$2, 5$	3^2	2	25^2	2	^{2}	$2, 5$	$3, 5^2$
1		11	3^7	31	41	^{3,17}	61	71	81	^{7,13}
2	2	$3, 4$	11^2	32	^{2}	$2, 13$	31^2	$2, 9$	41^2	$2, 23$
3	3	13	23	^{3}	43	53		73	83	^{31}
4	4	7^2	$2, 3$	17^2	$2, 11$	27^2	64	37^2	2	47^2
5	5	^{3,5}	25	^{5,7}	^{3}	^{5,11}	^{5,13}	^{5}	^{5}	
6	3^2	16	13^2	$4, 9$	23^2	8	^{2}	$2, 19$	43^2	$3, 4$
7	7	17	27	37	47	^{19}	67	^{11}	^{3,29}	97
8	8	9^2	$2, 7$	19^2	$3, 4$	29^2	$2, 17$	^{2}	2	47^2
9	9	19	29		49	59	^{3}	79	89	^{3}

5.14 **Theorem** [646]Let G be abelian group of order g. Let p be an odd prime dividing g. A $\mathrm{GH}(g, \lambda)$ of odd order $g\lambda$ exists over G only if every positive integer $m \not\equiv 0 \pmod{p}$ that divides the squarefree part of $g\lambda$ has odd multiplicative order modulo p. In particular, for all divisors t of g and all primes p, the Hilbert norm $(q, (-1)^{(t-1)/2}t)_p = 1$; hence, there exists a nontrivial solution for the equation $nx^2 + (-1)^{(t-1)/2}ty^2 = z^2$.

5.15 Remark Theorem 5.14 is true for nilpotent G. If $g = \prod p_i^{k_i}$ is the prime power decomposition of g and for all pairs i and j, $p_i \not| p_j^{k_j} - 1$, then G must be nilpotent. The only odd values $g < 100$ for which this is not true are 39, 55, 63, and 75.

5.16 Theorem [328] A GH(g, λ) with $n = g\lambda$ odd exists over a group G only if a nontrivial solution in integers x, y, z to $z^2 = nx^2 + (-1)^{(t-1)/2}ty^2$ exists for every order t of a homomorphic image of G.

5.3 Conjectures and Smallest Test Cases

5.17 Remark Little is known about the spectrum of orders and groups for which there exists a GH-matrix. Some general observations:

1. All known GH-matrices are over p-groups.
2. GH-matrices over nonelementary abelian groups are only known for square orders.
3. There are no nonexistence results for even order GH-matrices over EA(q) when q is odd.
4. Little is known about the orders for which there exist a GH-matrix over EA(2^t).

5.18 Conjectures

1. There are no GH-matrices over non-prime-power order groups.
2. There is a GH-matrix of order $4tq$ over EA(q) for all odd prime powers q and positive integers t.
3. There is a GH-matrix of order $2tq$ over EA(q) for all odd prime powers q and positive integers t.
4. For p an odd prime, there is a GH-matrix of odd order n over EA(p) if and only if all the prime divisors of the squarefree part of n have odd order modulo p.
5. There is a GH-matrix of order $4k$ over EA(4) for any positive integer k.

5.19 Remarks

1. The evidence for Conjecture 5.18.1 is strong. The first test case is order 12 over EA(12).
2. The evidence for Conjecture 5.18.2 is strong. (See the last line of Table 5.10.) The smallest unresolved case is order 40 over EA(5).
3. The evidence for Conjecture 5.18.3 is weak. The conjecture is made because there are no known nonexistence results for even order GH-matrices over EA(q) where q is odd. The smallest test case is order 30 over EA(5).
4. The existence of a GH-matrix of order 21 over EA(3) supports Conjecture 5.18.4. The smallest test case is order 39 over EA(3).
5. A GH-matrix of order $4k$ over EA(4) is equivalent to a pair of order $4k$ Hadamard matrices whose Hadamard product (entrywise product) is also a Hadamard matrix. So there is some support for Conjecture 5.18.5. The smallest test case is order 20 over EA(4).

5.20 Example The $GH(4, 1)$ over EA(4) in Example 5.4 corresponds to the three Hadamard matrices in the following identity.

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

5.4 Generalized Hadamard Matrices with Special Structure

5.21 A matrix H over the group G is *developed modulo the group* M if it has the form $(h(xy))_{x,y\in M}$ where $h : M \to G$.

For G abelian, a *cocycle* is a map $f : M \times M \to G$ such that $f(x,y)f(xy,z) = f(y,z)f(x,yz)$ for all $x,y,z \in M$.

A matrix H over the group G is *cocyclic* with *indexing group* M if it has the form $(f(x,y)h(xy))_{x,y\in M}$ where $f : M \times M \to G$ is a cocycle and $h : M \to G$.

5.22 **Example** For $M = EA(4)$, writing the cocycle identity additively, it may be viewed as a system of 64 linear equations on the 16 quantities $\{f(x,y) \mid x,y \in EA(4)\}$. In this small case, one can solve the equations by hand. The general solution is displayed (using multiplicative notation) as the 4×4 array:

$$M = \begin{pmatrix} Z & Z & Z & Z \\ Z & AZ & E^{-1}Z & AEZ \\ Z & B^{-1}Z & FZ & BFZ \\ Z & ABZ & EFZ & AEFBZ \end{pmatrix}$$

Here A, B, E, F and Z are commuting indeterminates satisfying the constraint $E^2 = B^2$. The indexing of the rows and columns is $1, a, b, ab$; so, for example, $f(ab,a) = ABZ$ and $f(b,b) = FZ$.

5.23 A GH-matrix is *cocyclic with indexing group* M (*developed modulo* M) if it is equivalent to a matrix that is cocyclic with indexing group M (developed modulo M, respectively).

A GH-matrix H has a *core developed modulo the group* M if it is equivalent to a normalized matrix with core developed modulo M. If M is cyclic, then the core is *circulant*.

5.24 **Example** A cocyclic conference matrix, GH-matrix over EA(4), and orthogonal design (from left to right).

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & ab \\ 1 & ab & a & b \\ 1 & b & ab & a \end{pmatrix} \qquad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & -x_1 & -x_4 & x_3 \\ x_3 & x_4 & -x_1 & -x_2 \\ x_4 & -x_3 & x_2 & -x_1 \end{pmatrix}$$

These are obtained by substituting in M of Example 5.22 $h(1) = 0, h(a) = h(b) = h(ab) = 1$, $A = E = F = -1$, $B = Z = 1$; $h(1) = h(a) = h(b) = h(ab) = 1$, $A = a, B = ab, E = b, F = a$, $Z = 1$; and $h(1) = x_1, h(a) = x_2, h(b) = x_3, h(ab) = x_4$, and $A = E = F = -1$, $B = Z = 1$, respectively.

5.25 **Theorems**

1. For p an odd prime, a circulant GH(p, p^{t-1}) exists if and only if $t \in \{1,2\}$.
2. Let q be an odd prime power. Then the matrix $((x-y)^2)_{x,y\in\mathbb{F}_q}$ is an EA(q)-developed GH$(q,1)$ over EA(q).
3. There is a EA(q)-developed GH(q,q) over any group of order q.
4. Let ω denote a primitive element of $\mathbb{F}_q^*$. The $(q-1)\times(q-1)$ matrix $[\omega^{j-i}]_{i,j\in\mathbb{F}_q^*}$ is a circulant core for a GH$(q,1)$ over EA(q). Also, $1w^2www^2$ is the first row of a circulant core of a GH$(3,2)$.
5. [651] Identify EA(q) with the additive group of the Galois field of order q. For $x, y \in$EA(q), let $f(x,y) = x \cdot y$ where "$\cdot$" is the field multiplication. Then the matrix $(f(x,y))_{x,y}$ is a cocyclic GH$(q,1)$ over EA(q) with cocycle f.

6. [653] Let q be a prime power. If there is a cocyclic $\mathrm{GH}(g,(q+1)/g)$ over a group G and a $\mathrm{GH}(g,(q+1)/g)$ over a group G with $\mathrm{EA}(q)$-developed core, then there is a cocyclic $\mathrm{GH}(g,q^2(q+1)/g)$ over G. In particular, there is a cocyclic $\mathrm{GH}(2^t,2^{s-t}(2^s-1)^2)$ over $\mathrm{EA}(2^t)$ whenever $s\geq t$ and 2^s-1 is prime.
7. The Kronecker product of two group-developed (cocyclic) GH-matrices is group-developed (cocyclic, respectively).
8. Any homomorphic image of group-developed (cocyclic) GH-matrices is group-developed (cocyclic, respectively).

5.26 **Remark** See [652] for references to the results on group-developed GH-matrices as well as a table on the existence of group-developed GH-matrices with orders $n\leq 50$.

5.5 Other Kinds of Generalized Hadamard Matrices

5.27 Let ζ_m denote a complex root of unity of order m. A (n,m)-*Butson Hadamard matrix* (or (n,m)-*BHM*) is an $n\times n$ matrix $H=(h_{ij})$ with entries from the integer powers of ζ_m, such that, if $H^*=(h_{ji}^{-1})$, then $HH^*=nI_n$ over the complex field.

5.28 **Remark** Many $(n,4)$-BHMs are known, corresponding to the complex Hadamard matrices. There has been no systematic study for other nonprime values of m.

5.29 **Example** A $(7,6)$-BHM found by Brock [328], and a $(13,6)$-BHM found by Compton and de Launey. Here $0,1,2,3,4,5$ correspond to $1,-w^2,w,-1,w^2,-w$.

$$\begin{pmatrix}
-1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & w & w^2 & w & 1 & -w\\
1 & -w & 1 & w & w^2 & w & 1\\
1 & 1 & -w & 1 & w & w^2 & w\\
1 & w & 1 & -w & 1 & w & w^2\\
1 & w^2 & w & 1 & -w & 1 & w\\
1 & w & w^2 & w & 1 & -w & 1
\end{pmatrix}$$

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&2&3&3&3&3&3&4\\
0&0&0&2&3&3&5&0&0&2&3&4&3\\
0&0&2&2&4&5&4&2&4&5&0&2&2\\
0&1&3&5&2&4&2&5&3&1&0&5&3\\
0&2&0&4&3&4&2&4&0&5&2&2&0\\
0&2&4&1&5&3&5&4&2&2&5&2&0\\
0&2&5&4&0&2&4&1&3&5&3&0&2\\
0&3&4&0&3&1&1&2&0&4&5&4&2\\
0&4&1&4&3&1&5&3&3&2&1&5&0\\
0&4&2&4&0&2&3&0&0&3&0&2&4\\
0&4&3&2&0&4&2&2&5&1&3&5&0\\
0&4&3&2&2&0&0&5&2&5&3&1&4
\end{pmatrix}$$

5.30 **Theorems** Assorted theorems concerning Butson Hadamard matrices.

1. If an (n,m)-BHM exists, then there is an (n,mt)-BHM for any integer $t\geq 1$.
2. [408] Let p be a prime. There is an (n,p)-BHM if and only if there is a GH-matrix of order n over $\mathrm{EA}(p)$.
3. [2157] Let p be a prime. If there is an (n,p^f)-BHM, then p divides n.
4. [595] There is a (group-developed) (n,m)-BHM for all n,m such that (a) every prime dividing n divides m, and (b) if n is even, then 4 also divides m.
5. [328] If there is an (n,m)-BHM, where n is odd, then no prime p dividing the squarefree part of m has even order f mod m such that $p^{f/2}\equiv -1 \pmod m$.
6. [595] There is a $(2(q+1),2p)$-BHM for any prime power $q\equiv 1 \pmod p$.

5.31 **Remarks**

1. The matrix in Theorem 5.30.4 is formed by taking the Kronecker product of matrices supplied by Theorem 5.25.1 and, when n is even, the matrix $[i^{(a+b)^2}]_{a,b=0,1}$.
2. An $(n,6)$-BHM exists for $n\in\{1,2,3,4,6,7,8,9,10,12,13,14,16,18,20\}$, but not for $n\in\{5,11,15,17\}$. The smallest undecided order is $n=19$ [595].

5.32 Let R be a ring with unity 1 and group of units R^* whose characteristic does not divide the positive integer v. A square matrix $M = (m_{ij})$ of order $v \geq 2$ with entries from a subgroup N of R^* is a *generalized Butson Hadamard matrix* (or (v, N)-*GBHM*) if $MM^* = M^*M = vI_v$, where $M^* = (m_{ij}^{-1})^\top$.

5.33 **Example** Let $R = \mathbb{Z}[i, j, k \mid i^2 = j^2 = k^2 = -1, ij = k]$ denote the ring of quaternions over the integers $\mathbb{Z}$. Then $(\pm 1 \pm i \pm j \pm k)/2$ is a unit. If A_i $(i = 1, 2, 3, 4)$ are $t \times t$ $(1, -1)$-matrices, then $M = A_1 + iA_2 + jA_3 + kA_4$ is a GBHM over R if and only if the array on the right is a Hadamard matrix. Stafford observed that in this case, N is isomorphic to SL(2,3).

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & -A_1 & A_4 & -A_3 \\ A_3 & -A_4 & -A_1 & A_2 \\ A_4 & A_3 & -A_2 & -A_1 \end{pmatrix}$$

5.34 **Remark** GBHMs include the orthogonal matrices studied by Sylvester [1997], and the power Hadamard matrices of Craigen and Woodford [617].

See Also

§IV.1	A GH-matrix gives a complete resolvable transversal design.
§V.4	A GH(g, λ) over G is a GBRD$(\lambda g, \lambda g, \lambda g; G)$.
§V.6	By Theorem 6.66, a GH$(g, 1)$ with core developed modulo M is equivalent to a projective plane and a generalized conference matrix with special structure.
§VI.17	A GH is a difference matrix with the maximum number of rows.
§VI.18	A cocyclic GH-matrix is equivalent to semi-regular central relative difference set [1131].
§VII.1	GH-matrices have many applications in coding theory.
[645, 1563]	GH-matrices with other special structure.

References Cited: [225, 328, 408, 595, 617, 645, 646, 647, 650, 651, 652, 653, 654, 655, 748, 1131, 1222, 1563, 1997, 2157]

6 Balanced Generalized Weighing Matrices and Conference Matrices

Yury J. Ionin
Hadi Kharaghani

6.1 Conference Matrices

6.1 A *conference matrix* of order n is an $n \times n$ $(0, \pm 1)$-matrix C with zero diagonal satisfying $CC^T = (n-1)I$. A conference matrix is *normalized* if all entries in its first row and first column are 1 (except the (1,1) entry which is 0). The *core* of a normalized conference matrix C consists of all the rows and columns of C except the first row and column.

6.2 **Remark** A conference matrix or order n is a weighing matrix $W(n, n-1)$. See §V.2.

6.3 **Theorem** If there exists a conference matrix of order n, then n is even; furthermore, if $n \equiv 2 \pmod 4$, then, for any prime $p \equiv 3 \pmod 4$, the highest power of p dividing $n - 1$ is even.

6.4 **Examples** A is a symmetric conference matrix of order 2; B is a skew-symmetric conference matrix of order 4; C is a normalized symmetric conference matrix of order 6. Other examples are given in Example V.2.3.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 & 1 & 1 \\ - & 0 & 1 & - \\ - & - & 0 & 1 \\ - & 1 & - & 0 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{pmatrix}$$

6.5 **Theorem** The core of every normalized conference matrix of order $n \equiv 2 \pmod 4$ is symmetric and the core of every normalized conference matrix of order $n \equiv 0 \pmod 4$ is skew-symmetric.

6.6 **Theorem** There is a skew-type Hadamard matrix of order $4n$ (see §V.1) if and only if there is a skew-symmetric conference matrix of order $4n$.

6.7 **Theorem** (Paley) Let q be an odd prime power:

1. If $q \equiv 1 \pmod 4$, then there is a symmetric conference matrix of order $q+1$.
2. If $q \equiv 3 \pmod 4$, then there is a skew-symmetric conference matrix of order $q+1$.

6.8 **Construction** Let A be a $(0, \pm 1)$-matrix of order n and B a ± 1-matrix of order n such that $AB = BA$ and $AA^T + BB^T = (2n-1)I$. Then the matrix $C = \begin{pmatrix} A & B \\ B^T & -A^T \end{pmatrix}$ is a conference matrix of order $2n$.

6.9 The conference matrix C in Construction 6.8 is *constructible from two circulant matrices* or for short *two circulants type*.

6.10 **Table** Conference matrices of order $2n$ for small n. E denotes exists, DNE means doesn't exist and U stands for existence being unresolved.

n	Status	Comments
$8 \neq n < 11$	E	Theorem 6.7
8	E	Theorem 6.6
11	DNE	$21 = 3 \cdot 7$ and Theorem 6.3
$11 < n < 17$	E	Theorem 6.7
17	DNE	$33 = 3 \cdot 11$ and Theorem 6.3
18	E	Theorem 6.6
$18 < n \neq 20 < 23$	E	Theorem 6.7
20	E	Theorem 6.6
23	E	$q = 3$ in Theorem 6.12
$23 < n < 26$	E	Theorem 6.7
26	E	Theorem 6.6
27	E	Theorem 6.7
28	E	Theorem 6.6
29	DNE	$57 = 3 \cdot 19$ and Theorem 6.3
$29 < n < 32$	E	Theorem 6.7
32	E	Theorem 6.6
33	U	not of two circulants type

6.11 **Theorem** If $q \equiv 1 \pmod 4$ is a prime power, then there is a symmetric conference matrix C of order $q+1$ of two circulants type.

6.12 **Theorem** There is a symmetric conference matrix of order $q^2(q+2)+1$ whenever q is a prime power, $q \equiv 3 \pmod 4$, and $q+3$ is the order of a conference matrix.

6.13 **Theorem** There are conference matrices of order $5(9^{2t+1})+1$, $t \geq 0$.

6.14 **Remark** The smallest order for which a conference matrix is not known to exist is $n = 66$. A conference matrix of order 66 cannot be of the two circulants type. See Conjecture V.2.114 for the *Conference Matrix Conjecture*.

6.2 Generalized Conference Matrices

6.15 A *generalized conference matrix* of index λ over a multiplicatively written finite group G, or a $GC(G;\lambda)$, is a square matrix $W = [\omega_{ij}]$ with $\omega_{ii} = 0$ and $\omega_{ij} \in G$ whenever $i \neq j$, such that, for any distinct row indices i and h, the multiset $\{\omega_{ij}\omega_{hj}^{-1} : j \neq i, j \neq h\}$ contains precisely λ copies of every element of G.

6.16 **Remark** The order of $GC(G;\lambda)$ is $\lambda|G|+2$. If $G = \{\pm 1\}$, then $GC(G;\lambda)$ is a conference matrix of order $2\lambda+2$. A generalized conference matrix is a special case of a balanced generalized weighing matrix (§6.3).

6.17 **Examples** A $GC(\mathbb{Z}_7;1)$, a $GC(\mathbb{Z}_3;2)$, and a $GC(Q_8;1)$.

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & \omega & \omega^3 & \omega^2 & \omega^6 & \omega^4 & \omega^5 \\
1 & 1 & 0 & \omega^3 & \omega & \omega^6 & \omega^2 & \omega^5 & \omega^4 \\
1 & \omega & \omega^3 & 0 & 1 & \omega^4 & \omega^5 & \omega^2 & \omega^6 \\
1 & \omega^3 & \omega & 1 & 0 & \omega^5 & \omega^4 & \omega^6 & \omega^2 \\
1 & \omega^2 & \omega^6 & \omega^4 & \omega^5 & 0 & 1 & \omega & \omega^3 \\
1 & \omega^6 & \omega^2 & \omega^5 & \omega^4 & 1 & 0 & \omega^3 & \omega \\
1 & \omega^4 & \omega^5 & \omega^2 & \omega^6 & \omega & \omega^3 & 0 & 1 \\
1 & \omega^5 & \omega^4 & \omega^6 & \omega^2 & \omega^3 & \omega & 1 & 0
\end{pmatrix}
\qquad
\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 \\
1 & 1 & 0 & 1 & \omega^2 & \omega & \omega \\
1 & \omega^2 & 1 & 0 & 1 & \omega^2 & \omega \\
1 & \omega & \omega^2 & 1 & 0 & 1 & \omega^2 \\
1 & \omega & \omega & \omega^2 & 1 & 0 & 1 \\
1 & \omega^2 & \omega & \omega & \omega^2 & 1 & 0
\end{pmatrix}
\qquad
\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 0 & -1 & 1 & -i & -k & -j & i & j & k \\
-1 & 1 & 0 & -1 & -j & -i & -k & k & i & j \\
-1 & -1 & 1 & 0 & -k & -j & -i & j & k & i \\
-1 & i & j & k & 0 & -1 & 1 & -i & -k & -j \\
-1 & k & i & j & 1 & 0 & -1 & -j & -i & -k \\
-1 & j & k & i & -1 & 1 & 0 & -k & -j & -i \\
-1 & -i & -k & -j & i & j & k & 0 & -1 & 1 \\
-1 & -j & -i & -k & k & i & j & 1 & 0 & -1 \\
-1 & -k & -j & -i & j & k & i & -1 & k & 0
\end{pmatrix}$$

6.18 **Example** A $GC(\mathbb{Z}_3;9)$:
$\mathbf{j}$ is the 9×1 all-one column and A, B, C, D, E, and F are symmetric circulant matrices of order 9 whose first rows are $(0\ 1\ \omega\ \omega\ \omega^2\ \omega^2\ \omega\ \omega\ 1)$, $(\omega^2\ \omega^2\ 1\ \omega\ 1\ 1\ \omega\ 1\ \omega^2)$, $(\omega\ \omega^2\ \omega\ 1\ \omega^2\ \omega^2\ 1\ \omega\ \omega^2)$, $(0\ \omega^2\ 1\ \omega^2\ \omega\ \omega\ \omega^2\ 1\ \omega^2)$, $(1\ \omega\ \omega\ \omega^2\ 1\ 1\ \omega^2\ \omega\ \omega)$, and $(0\ \omega\ \omega^2\ 1\ 1\ 1\ 1\ \omega^2\ \omega)$, respectively.

$$\begin{pmatrix}
0 & 1 & \mathbf{j}^\top & \mathbf{j}^\top & \mathbf{j}^\top \\
1 & 0 & \mathbf{j}^\top & \omega\mathbf{j}^\top & \omega^2\mathbf{j}^\top \\
\mathbf{j} & \mathbf{j} & A & B & C \\
\mathbf{j} & \omega\mathbf{j} & B & D & E \\
\mathbf{j} & \omega^2\mathbf{j} & C & E & F
\end{pmatrix}$$

6.19 **Theorem** Let $f\colon G \to G'$ be a surjective group homomorphism Replacing every nonzero entry ω_{ij} of a $GC(G;\lambda)$ by $f(\omega_{ij})$ yields a $GC(G';\lambda|G|/|G'|)$.

6.20 A $GC(G;1)$ is *normalized* if all nonzero entries in its first row and first column are equal to 1. Removing the first row and column of a normalized $GC(G;1)$ yields the *core* of this matrix.

6.21 **Theorem** A matrix $C = [c_{ij}]$ is the core of a $GC(G;\lambda)$ if and only if every row of C contains precisely λ copies of every element of G and, for any distinct row indices i and h, the multiset $\{c_{ij}c_{hj}^{-1} : j \neq i, j \neq h\}$ contains precisely λ copies of every nonidentity element of G and $\lambda - 1$ copies of the identity.

6.22 A *nearfield* is an algebraic structure $(F, +, \cdot)$ such that $(F, +)$ is an abelian group, $(F^* = F \setminus \{0\}, \cdot)$ is a group, $(x+y)z = xz + yz$ for all $x, y, z \in F$, and $x \cdot 0 = 0$ for all $x \in F$. A *proper nearfield* is a nearfield that is not a field.

6.23 **Remark** A proper nearfield of order m exists if and only if $m = q^n$ where q is a prime power, every prime divisor of n divides $q-1$, and, if $q \equiv 3 \pmod 4$, then $n \not\equiv 0$

(mod 4). In particular, for any odd prime power q, there exists a proper nearfield of order q^2. The multiplicative group of a proper nearfield is nonabelian. See [1170] for the complete list of finite nearfields and their multiplicative groups.

6.24 Theorem Let $F = \{a_1, a_2, \ldots, a_m\}$ be a finite nearfield (or field). Then $C = [a_i - a_j]$ is the core of a $GC(F^*; 1)$.

6.25 Corollary For any prime power q and for any divisor n of $q-1$, there exists a $GC(\mathbb{Z}_n; (q-1)/n)$.

6.26 Theorem For every $m \geq 2$, there exists a $GC(\mathbb{Z}_n; \lambda)$ with $n = 2^m - 1$ and $\lambda = 2^{m+1} + 1$.

6.27 Remark For all known matrices $GC(G; 1)$, the group G is the multiplicative group of a field or a nearfield. All known matrices $GC(G; \lambda)$ with $\lambda > 1$ are the matrices of Theorem 6.26 and those obtained by applying Theorem 6.19.

6.28 The core C of a $GC(G; \lambda)$ is *skew-symmetric* if the group G has a unique element ε of order 2 and $C^\top = \varepsilon C$.

6.29 Theorem Let C be the core of a $GC(G; \lambda)$ and let the group G be abelian. If λ is odd and G has a unique element of order 2, then C is skew-symmetric. Otherwise, C is symmetric.

6.3 Balanced Generalized Weighing Matrices

6.30 Let G be a multiplicatively written finite group. A *balanced generalized weighing matrix with parameters* (v, k, λ) *over* G, or a $BGW(v, k, \lambda; G)$, is a matrix $W = [\omega_{ij}]$ of order v with entries from $G \cup \{0\}$ such that (i) every row of W contains exactly k nonzero entries and (ii) for any distinct $i, h \in \{1, 2, \ldots, v\}$, every element of G is contained exactly $\lambda/|G|$ times in the multiset $\{\omega_{ij}\omega_{hj}^{-1} : 1 \leq j \leq v, j \neq i, j \neq h\}$.

6.31 Remark A $GC(G; \lambda)$ is a $BGW(\lambda|G| + 2, \lambda|G| + 1, \lambda|G|; G)$. A generalized Hadamard matrix $GH(G; \lambda)$ (see §V.5) is a $BGW(\lambda|G|, \lambda|G|, \lambda|G|; G)$. If $|G| = 2$, then a $BGW(v, k, \lambda; G)$ is a balanced weighing matrix. These matrices were studied in [1655].

6.32 Remark Replacing all nonzero entries of a $BGW(v, k, \lambda; G)$ by 1 yields an incidence matrix of a symmetric (v, k, λ)-design.

6.33 Examples A $BGW(5, 4, 3; \mathbb{Z}_3)$ and a $BGW(7, 4, 2; \mathbb{Z}_2)$.

$$\begin{pmatrix} 0 & w^2 & w & w^2 & w^2 \\ e & 0 & w^2 & w & w^2 \\ e & e & 0 & w^2 & w \\ w^2 & e & e & 0 & w^2 \\ e & w^2 & e & e & 0 \end{pmatrix} \qquad \begin{pmatrix} -1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

6.34 Theorem For $f : G \to G'$ a surjective group homomorphism, replacing every nonzero entry ω_{ij} of a $BGW(v, k, \lambda; G)$ by $f(\omega_{ij})$ yields a $BGW(v, k, \lambda; G')$.

6.35 Theorem If $W = [\omega_{ij}]$ is a $BGW(v, k, \lambda; G)$, then so is $W^* = [\omega_{ji}^*]$ where $\omega^* = \omega^{-1}$ if $\omega \neq 0$ and $0^* = 0$.

6.36 Remark A $BGW(v, k, \lambda; G)$ can be regarded as a matrix over the group ring $\mathbb{Z}G$.

6.37 Theorem Let G be a finite group. A matrix W of order v over $\mathbb{Z}G$ with entries from $G \cup \{0\}$ is a $BGW(v, k, \lambda; G)$ if and only if it satisfies $WW^* = kI + \frac{\lambda}{|G|}G(J - I)$, where G represents the sum of all elements of G in $\mathbb{Z}G$.

6.38 **Theorem** Let G and S be finite groups, $|S| = q \geq 2$. If there exist a $BGW(q+1, q, q-1; G)$ and a $GH(S; 1)$, then, for any positive integer t, there exists a $BGW(v, k, \lambda; G)$ with $v = (q^{t+1}-1)/(q-1)$, $k = q^t$, and $\lambda = q^t - q^{t-1}$.

6.39 **Theorem** Let q be a prime power and t a positive integer. Let $v = (q^{t+1}-1)/(q-1)$, $k = q^t$, and $\lambda = q^t - q^{t-1}$. A $BGW(v, k, \lambda; G)$ exists in each of the following cases:

1. G is a cyclic group whose order n divides $q-1$; furthermore, if $q(q-1)/n$ is even, then there exists a symmetric $BGW(v, k, \lambda; G)$ with zero diagonal and, if n is even and $(q-1)/n$ is odd, then there exists a skew-symmetric $BGW(v, k, \lambda; G)$;
2. G is the multiplicative group of a nearfield or a homomorphic image of such a group;
3. q is a square and G is any group whose order divides $\sqrt{q}+1$;
4. q is even and G is a cyclic group whose order divides $2q-2$; and
5. q is even, $t = 6$, and $G = \mathbb{Z}_2 \times \mathbb{Z}_n$ where n divides $2q-2$.

6.40 **Remark** The only known parameters of BGW matrices in addition to Theorem 6.39 that are neither generalized conference matrices nor generalized Hadamard matrices are $BGW(13, 9, 6; S_3)$, $BGW(15, 7, 3; \mathbb{Z}_3)$, $BGW(19, 9, 4; \mathbb{Z}_2)$, and $BGW(45, 12, 3; \mathbb{Z}_3)$.

6.41 **Example** A circulant $BGW(13, 9, 6; S_3)$ exists with $(0, a, e, ab, 0, e, e, ba, a, ba, 0, ab, 0)$ as first row, where $a = (12)$ and $b = (123)$ generate the symmetric group S_3.

6.42 **Example** A $BGW(15, 7, 3; \mathbb{Z}_3)$

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & w & 0 & w^2 & 0 & 0 & 0 & 1 & w^2 & 0 & w & 0 & 0 & 0 \\
1 & 0 & 1 & w & 0 & w^2 & 0 & 0 & 0 & 1 & w^2 & 0 & w & 0 & 0 \\
1 & 0 & 0 & 1 & w & 0 & w^2 & 0 & 0 & 0 & 1 & w^2 & 0 & w & 0 \\
1 & 0 & 0 & 0 & 1 & w & 0 & w^2 & 0 & 0 & 0 & 1 & w^2 & 0 & w \\
1 & w^2 & 0 & 0 & 0 & 1 & w & 0 & w & 0 & 0 & 0 & 1 & w^2 & 0 \\
1 & 0 & w^2 & 0 & 0 & 0 & 1 & w & 0 & w & 0 & 0 & 0 & 1 & w^2 \\
1 & w & 0 & w^2 & 0 & 0 & 0 & 1 & w^2 & 0 & w & 0 & 0 & 0 & 1 \\
0 & 1 & w^2 & 0 & w & 0 & 0 & 0 & 0 & 0 & w^2 & 0 & w^2 & w^2 & 1 \\
0 & 0 & 1 & w^2 & 0 & w & 0 & 0 & 1 & 0 & 0 & w^2 & 0 & w^2 & w^2 \\
0 & 0 & 0 & 1 & w^2 & 0 & w & 0 & w^2 & 1 & 0 & 0 & w^2 & 0 & w^2 \\
0 & 0 & 0 & 0 & 1 & w^2 & 0 & w & w^2 & w^2 & 1 & 0 & 0 & w^2 & 0 \\
0 & w & 0 & 0 & 0 & 1 & w^2 & 0 & 0 & w^2 & w^2 & 1 & 0 & 0 & w^2 \\
0 & 0 & w & 0 & 0 & 0 & 1 & w^2 & w^2 & 0 & w^2 & w^2 & 1 & 0 & 0 \\
0 & w^2 & 0 & w & 0 & 0 & 0 & 1 & 0 & w^2 & 0 & w^2 & w^2 & 1 & 0
\end{pmatrix}$$

6.43 **Example** A $BGW(19, 9, 4; \mathbb{Z}_2)$.

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & - & 1 & - & 0 & 0 & - & - & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & - & 1 & 0 & 0 & 1 & - & - & 0 & - & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & - & 1 & - & 0 & 1 & - & - & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & - & 0 & 0 & 0 & 0 & 1 & 0 & - & 0 & 0 & 1 & 0 & - & - & 0 & 1 & 0 \\
1 & 0 & 1 & - & 0 & 0 & 0 & - & 1 & 0 & 1 & 0 & 0 & - & 0 & - & 0 & 0 & 1 \\
1 & - & 0 & 1 & 0 & 0 & 0 & 0 & - & 1 & 0 & 1 & 0 & - & - & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & - & 1 & - & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & - & - \\
1 & - & 1 & 0 & 0 & 1 & - & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & - & 0 & - \\
1 & 0 & - & 1 & - & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & - & - & 0 \\
0 & 0 & - & - & 0 & 1 & 0 & 0 & 0 & 1 & - & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & - & 0 & - & 0 & 0 & 1 & 1 & 0 & 0 & 1 & - & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & - & - & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & - & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & - & - & 0 & 1 & 0 & 0 & 0 & 1 & - & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & - & 0 & - & 0 & 0 & 1 & 1 & 0 & 0 & 1 & - & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & - & - & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & - & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & - & - & 0 & 1 & 0 & 0 & 0 & 1 & - & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & - & 0 & - & 0 & 0 & 1 & 1 & 0 & 0 & 1 & - & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & - & - & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & -
\end{pmatrix}$$

6.44 **Remark** A necessary condition for the existence of a $BGW(v,k,\lambda;G)$ is the existence of a symmetric (v,k,λ)-design. Another necessary condition is given by Theorem 6.45.

6.45 **Theorem** Suppose that there exists a $BGW(v,k,\lambda;G)$ with v odd and a surjective homomorphism from G onto $\mathbb{Z}_p$ where p is an odd prime. If $m \not\equiv 0 \pmod p$ is an integer dividing the squarefree part of k, then the order of m modulo p is odd.

6.4 BGW Matrices and Other Combinatorial Designs

6.46 Let $\mathcal{M}$ be a nonempty set of $(0,1)$-matrices of the same size $m \times n$. A group G of bijections $\mathcal{M} \to \mathcal{M}$ is a *group of symmetries of* $\mathcal{M}$ if it satisfies the following two conditions:

1. $(\sigma X)(\sigma Y)^\top = XY^\top$ for all $X, Y \in \mathcal{M}$ and all $\sigma \in G$;
2. for each $X \in \mathcal{M}$, there is an integer $t(X)$ such that $\sum_{\sigma\in G} \sigma X = t(X)J$, where J is the $m \times n$ all-one matrix.

6.47 **Examples** Let $\mathcal{M}$ be the set of all incidence matrices of the affine plane of order 2. For each $X \in \mathcal{M}$, let $\sigma X = J - X$ where J is the 4×6 all-one matrix. Then the group G of order 2 generated by σ is a group of symmetries of $\mathcal{M}$.

6.48 **Examples** Let $\mathcal{H}$ be the set of all Bush-type Hadamard matrices (see §V.1) of order 16 and let $\mathcal{M} = \{\frac{1}{2}(J - H) \colon H \in \mathcal{H}\}$. Then each $X \in \mathcal{M}$ is an incidence matrix of a symmetric $(16,6,2)$-design. Let $X = [X_{ij}] \in \mathcal{M}$ where X_{ij} are 4×4 blocks. Let $\sigma X = Y = [Y_{ij}]$ where $Y_{ij} = X_{i,j-1}$ for $j = 2,3,4$, $Y_{i1} = O$ if $X_{i4} = O$, and $Y_{i1} = J - X_{i4}$ if $X_{i4} \neq O$. Let G be the cyclic group generated by σ. Then $|G| = 8$ and G is a group of symmetries of $\mathcal{M}$.

6.49 **Theorem** Let $\mathcal{M}$ be a nonempty set of incidence matrices of (v,b,r,k,λ)-designs. Let G be a group of symmetries of $\mathcal{M}$ and let $W = [\sigma_{ij}]$ be a $BGW(w,l,\mu;G)$ such that $kr\mu = v\lambda l$. For $X \in \mathcal{M}$, let N denote the block matrix of order vw obtained by replacing every nonzero entry σ_{ij} of W with the matrix $\sigma_{ij}X$ and every zero entry of W with the $m \times n$ zero matrix. Then N is an incidence matrix of a $(vw, bw, rl, kl, \lambda l)$-design.

6.50 **Remark** If the parameters (w,l,μ) of the matrix W in Theorem 6.49 are $((q^{t+1}-1)/(q-1), q^t, q^t - q^{t-1})$, then the equation $kr\mu = v\lambda l$ is equivalent to $q = kr/(r-\lambda)$.

6.51 **Corollary** Let $\mathcal{M}$ be a nonempty set of incidence matrices of symmetric (v,k,λ)-designs and let G be a cyclic group of symmetries of $\mathcal{M}$. If $q = k^2/(k-\lambda)$ is a prime power and $|G|$ divides $q-1$, then, for any positive integer t, there exists a symmetric design with parameters $(v(q^{t+1}-1)/(q-1), kq^t, \lambda q^t)$.

6.52 **Examples** The set $\mathcal{M}$ and group G of Example 6.48 yield an infinite family of symmetric designs with parameters $(2(9^{t+1}-1), 6\cdot 9^t, 2\cdot 9^t)$.

6.53 **Theorem** Let $\mathbf{D}$ be a symmetric (v,r,λ)-design with r a prime power. Let B be a block of $\mathbf{D}$ and let X and Y be incidence matrices of the residual design $\mathbf{D}^B$ and the derived design $\mathbf{D}_B$, respectively, corresponding to the same orderings of points and blocks of $\mathbf{D}$. Let $\mathcal{M}$ be a set of $(v-r) \times (v-1)$ matrices that contains X and admits a cyclic group G of symmetries. Let $|G|$ divide $r-1$ and let $(\sigma X)Y = \lambda J$ for all $\sigma \in G$. Then, for any positive integer t, there exists a symmetric design with parameters $(1 + (v-1)(r^{t+1}-1)/(r-1), r^{t+1}, \lambda r^t)$.

6.54 **Examples** The symmetric $(7,3,1)$-design $\mathbf{D}$ with the set $\mathcal{M}$ and group G of Example 6.47 satisfies the conditions of Theorem 6.53 and, therefore, yields an infinite family of symmetric designs with parameters $(3^{t+2}-2, 3^{t+1}, 3^t)$.

6.55 **Remark** If an incidence matrix of a symmetric design is symmetric with zero diagonal, then it serves as an adjacency matrix of a strongly regular graph. Given a prime power q and positive integers m and n, Theorem 6.39(1) can be applied to obtain strongly regular graphs with parameters (v, k, λ, λ) for the following (v, k, λ): (i) $(q^{n+1}(s^{4m}-1)/((q-1)(s+1)), q^n s^{4m-1}, q^n s^{4m-2}(q^n+1)(q-1))$ where $s = q^{n+1}+q-1$ is a prime power; and (ii) $(2\cdot 3^{n+1}(s^{4m}-1)/(s+1), 3^n s^{4m-1}, 3^n(3^n+1)s^{4m-2}/2)$ where $s = (3^{n+1}+1)/2$ is a prime power.

6.56 **Remark** Skew-symmetric BGW matrices can be used for constructing infinite families of doubly regular digraphs [1166].

6.57 Let G be a group of order mn and N a normal subgroup of G of order n. A k-subset R of G, where $0 < k < mn$, is a *relative (m, n, k, λ)-difference set, or an (m, n, k, λ)-RDS, in G relative to N* if the multiset $\{xy^{-1} : x, y \in R\}$ contains no nonidentity element of N and contains exactly λ copies of every element of the set $G \setminus N$.

6.58 **Theorem** If there exists an (m, n, k, λ)-*RDS* in a group G relative to a subgroup N, then there exists a $BGW(m, k, \lambda n; N)$.

6.59 Let G be a group of order n and $M = [M(x, y)]_{x,y\in G}$ a matrix of order n whose rows and columns are indexed by elements of G. The matrix M is *G-invariant* if $M(xz, yz) = M(x, y)$ for all $x, y, z \in G$.

6.60 **Theorem** Let H and N be finite groups, $|H| = m$, $|N| = n$, and let $G = H \times N$. The following statements are equivalent:

1. there exists an (m, n, k, λ)-*RDS* in G relative to N; and
2. there exists an H-invariant $BGW(m, k, \lambda n; N)$.

6.61 **Corollary** Let q be a prime power and let G be a cyclic group whose order divides $q-1$. A circulant $BGW((q^{t+1}-1)/(q-1), q^t, q^t - q^{t-1}; G)$ exists if and only if $|G|$ and $(q^{t+1}-1)/(q-1)$ are relatively prime.

6.62 Let ω be a generator of a cyclic group G. A matrix $W = [\sigma_{ij}]$ of order n over $\mathbb{Z}G$ is *ω-circulant* if, for $i, j \in \{1, 2, \ldots, n-1\}$, $\sigma_{i+1,j+1} = \sigma_{ij}$ and $\sigma_{i+1,1} = \omega\sigma_{in}$.

6.63 **Theorem** Let G be a cyclic group of order mn and let $N = \langle\omega\rangle$ be the unique subgroup of G of order n. The following statements are equivalent:

1. there exists an (m, n, k, λ)-*RDS* in G relative to N; and
2. there exists an ω-circulant $BGW(m, k, \lambda n; N)$.

6.64 **Theorem** Let G be a group of order $n-1$. The following statements are equivalent:

1. there exists a $GC(G; 1)$; and
2. there exists a projective plane Π of order n with a nonincident point-line pair (p, L) such that the group of all (p, L)-homologies of Π is isomorphic to G.

6.65 **Remark** The projective plane equivalent to the matrix $GC(Q_8; 1)$ of Examples 6.17 is a nondesarguesian projective plane of the least order.

6.66 **Theorem** Let G be a group of order $n-1$ and E a group of order n. The following statements are equivalent:

1. there exists a $GC(G; 1)$ with E-invariant core;
2. there exists a $GH(E; 1)$ with G-invariant core; and
3. there exists a projective plane Π of order n with distinct points p and q and distinct lines L and M such that $p \in M$, $q \in L$, $q \in M$, the group of all (p, L)-homologies of Π is isomorphic to G, and the group of all (q, M)-elations of Π is isomorphic to E.

See Also

§II.6	BGW matrices are used to construct twin symmetric designs and siamese twin symmetric designs.
§V.2	BGW matrices reduce to balanced weighing matrices.
§V.5	BGW matrices are related to generalized Hadamard matrices.
§VI.18	BGW matrices and relative difference sets are closely related.
§VII.11	Symmetric BGW matrices with zero diagonal are used to construct strongly regular graphs and doubly regular digraphs.
[657]	Nonexistence results.
[900]	Sporadic BGW matrices.
[1167, 1166]	BGW matrices and regular graphs.
[1170]	A comprehensive source for theory of BGW matrices and their applications to symmetric designs.
[1222, 1227]	BGW matrices, relative difference sets, and projective planes.
[1231]	A recent survey of BGW matrices.
[1237, 1238]	Code-theoretic construction of BGW matrices of minimal rank.
[1655]	Generalized weighing matrices.

References Cited: [657, 900, 1166, 1167, 1170, 1222, 1227, 1231, 1237, 1238, 1655]

7 Sequence Correlation

Tor Helleseth

7.1 Definitions

7.1 The periodic *crosscorrelation* function $\theta_{u,v}(\tau)$ (at *shift* τ) between two sequences $\{u_t\}$ and $\{v_t\}$ of period n, having symbols from the alphabet $\mathbb{Z}_q = \{0, 1, 2, \cdots, q-1\}$, is $\theta_{u,v}(\tau) = \sum_{t=0}^{n-1} \omega^{u_{t+\tau} - v_t}$ where ω is a primitive complex q-th root of unity.

7.2 **Remark** Binary sequences are the most important for applications. In this case, $q = 2$, $\omega = -1$, and the crosscorrelation equals the number of agreements minus the number of disagreements between $\{u_{t+\tau}\}$ and $\{v_t\}$.

7.3 The *autocorrelation* of $\{u_t\}$ with itself is the crosscorrelation $\theta_{u,u}$, denoted by θ_u.

7.4 **Example** Let $\{u_t\}$ be the periodic sequence of period 7 given by 0010111. Then $\theta_u(\tau)$ is $7, -1, -1, -1, -1, -1, -1$ for $\tau = 0, 1, \cdots, 6$.

7.5 **Remark** In any modern communication system, sequences with good correlation properties play a fundamental role. Applications include signal synchronization, navigation, radar ranging, random number generation, spread-spectrum communications, and stream ciphers in cryptography. Applications demand both single sequences with low autocorrelation and large families of sequences with low maximum auto- and crosscorrelation among all pairs of sequences.

7.2 Binary Sequences with Low Autocorrelation

7.6 A sequence is *balanced* if the numbers of 0s and 1s differ by at most one during a period of the sequence.

7.7 A *binary maximal length sequence* (*m-sequence*) $\{s_t\}$ is a sequence of period $n = 2^r - 1$ satisfying a linear recurrence relation of degree r of the form $\sum_{i=0}^{r} f_i s_{t+i} = 0$ for all $t \geq 0$ where $f_i \in \mathbb{F}_2 = \{0, 1\}$, $f_0 = f_r = 1$. The *characteristic polynomial* of the recursion is $f(x) = \sum_{i=0}^{r} f_i x^i$.

7.8 **Theorem** An m-sequence $\{s_t\}$ of period $n = 2^r - 1$ is obtained if and only if the characteristic polynomial is a primitive polynomial and the initial state $(s_0, ..., s_{r-1})$ is nonzero. For every integer $r \geq 1$, m-sequences are known to exist.

7.9 **Example** The recursion $s_{t+3} + s_{t+1} + s_t = 0$ has characteristic polynomial $f(x) = x^3 + x + 1$. Starting from $(s_0, s_1, s_2) = (001)$, one generates the m-sequence 0010111 of period 7.

7.10 **Theorem** An m-sequence $\{s_t\}$ of period $n = 2^r - 1$ is balanced (during a period there are 2^{r-1} ones and $2^{r-1} - 1$ zeroes) and has two-level autocorrelation with the two values given by

$$\theta_s(\tau) = \begin{cases} n & \text{if } \tau = 0, \\ -1 & \text{if } \tau \neq 0. \end{cases}$$

7.11 The *Legendre sequence* $\{s_t\}$ of period a prime p is

$$s_t = \begin{cases} 1 & \text{if } t = 0 \text{ or } t \text{ is a quadratic nonresidue } (\text{mod } p)), \\ 0 & \text{otherwise.} \end{cases}.$$

7.12 **Theorem** The Legendre sequence is balanced and has two-level autocorrelation if $p \equiv 3 \pmod 4$ with out-of-phase autocorrelation -1.

7.13 **Example** The quadratic residues modulo 11 are $\{1, 3, 4, 5, 9\}$. The Legendre sequence is 10100011101 and has two-level autocorrelation with out-of-phase autocorrelation -1.

7.14 **Remark** When $p \equiv 1 \pmod 4$, the out-of-phase autocorrelation of the Legendre sequence has three values; the two out-of-phase values are -1 and 3.

7.15 **Remark** Sequences $\{s_t\}$ of period n with θ_s having autocorrelation as given in Theorem 7.10 correspond to *cyclic Hadamard difference sets*. For example, the Singer difference sets are obtained by defining a subset of $\mathbb{Z}_{2^r-1}$ by $S = \{t | s_t = 0\}$. See §V.1 and §VI.18. A recently discovered family of sequences is of period $n = 2^r - 1$, balanced with 2^{r-1} ones, and with ideal two-level autocorrelation with out-of-phase autocorrelation value of 1. This is optimal (lowest possible magnitude) for binary sequences of odd period. A recent construction is given in Theorem 7.16.

7.16 **Theorem** [707] Let $d = 2^{2k} - 2^k + 1$ where $1 \leq k < r/2$ and $\gcd(k, r) = 1$. Let $\Delta = \{(x+1)^d + x^d + 1 \mid x \in \mathbb{F}_{2^r}\}$. Let α be a primitive element of $\mathbb{F}_{2^r}$ and define the binary sequence $\{s_t\}$ by $s_t = 1$ if $\alpha^t \in \mathbb{F}_{2^r} \setminus \Delta$, and $s_t = 0$ otherwise. Then the sequence $\{s_t\}$ is balanced and has 2^{r-1} ones and $2^{r-1} - 1$ zeroes and two-level autocorrelation with out-of-phase value -1.

7.17 **Remark** No balanced binary sequence of odd period n has two-level autocorrelation function when $n \equiv 1 \pmod 4$. For balanced sequences of even length the optimal case for applications is to have out-of-phase autocorrelation values 0, -4 when $n \equiv 0 \pmod 4$ and -2, $+2$ when $n \equiv 2 \pmod 4$.

7.18 Let α be a primitive element of the finite field $\mathbb{F}_{p^r}$. The binary *Sidelnikov sequence* $\{s_t\}$ of period p^r-1 is $s_t = \begin{cases} 1 & \text{if } \alpha^t+1 \text{ is a nonsquare in } \mathbb{F}_{p^r}, \\ 0 & \text{otherwise.} \end{cases}$

7.19 **Theorem** [1909] The Sidelnikov sequences of period $n = p^r - 1$ are balanced and have three-level autocorrelation with out-of-phase values $0, -4$ when $n \equiv 0 \pmod 4$ and -2, $+2$ when $n \equiv 2 \pmod 4$.

7.20 **Remark** Besides Sidelnikov sequences there is another construction of a family of sequences of period n with these correlation values [709].

7.3 q-ary Sequences with Low Autocorrelation

7.21 A sequence $\{s_t\}$ over $\mathbb{Z}_q$ has *ideal autocorrelation* when its autocorrelation function satisfies $\theta_s(\tau) = \begin{cases} n & \text{if } \tau = 0 \\ 0 & \text{if } \tau \neq 0 \end{cases}$

7.22 **Theorem** Let n be a positive integer and let $q = n$ for odd n and $q = 2n$ for even n. The sequences given by $s_t = \begin{cases} t^2 \pmod q & \text{when } n \text{ is even} \\ \frac{t(t+1)}{2} \pmod q & \text{when } n \text{ is odd} \end{cases}$ have ideal autocorrelation for any period n.

7.23 **Example** For $n = 10$ the sequence is $\{s_t\} = 0, 1, 4, 9, 16, 5, 16, 9, 4, 1$ over an alphabet of size $q = 20$. For $n = 7$ the sequence is $\{s_t\} = 0, 1, 3, 6, 3, 1, 0$ over an alphabet of size $q = 7$.

7.4 Families of Sequences with Low Crosscorrelation

7.24 **Remark** Crosscorrelation is important in code-division multiple-access (CDMA) communication systems. Each user is assigned a distinct signature sequence; to minimize interference with other users, signature sequences have pairwise low crosscorrelation. For synchronization, signature sequences have low autocorrelation.

7.25 Let $\mathcal{F} = \{\{s_t^{(i)}(t)\} \mid 1 \le i \le M\}$ be a family of M sequences $\{s_t^{(i)}\}$ over $\mathbb{Z}_q$ each of period n. Let $\theta_{i,j}(\tau)$ denote the crosscorrelation between the i-th and j-th sequence at shift τ: $\theta_{i,j}(\tau) = \sum_{t=0}^{n-1} \omega^{s_{t+\tau}^{(i)} - s_t^{(j)}}$, $0 \le \tau \le n-1$.

7.26 **Remark** Sequence design for CDMA systems seeks to minimize $\theta_{max} = \max\{|\theta_{i,j}(\tau)| \mid \text{either } i \neq j \text{ or } \tau \neq 0\}$ for fixed n and M. Bounds on the minimum possible value of θ_{max} for given period n, family size M, and alphabet size q are available, including the most efficient bounds due to Welch, Sidelnikov, and Levenshtein; see [1089].

7.27 Let r be odd and $d = 2^k + 1$ where $k, 1 \le k \le r-1$, is an integer satisfying $\gcd(k, r) = 1$. Let $\{s_t\}$ be an m-sequence of period $n = 2^r - 1$. The *Gold* family of $2^r + 1$ sequences is $\mathcal{G} = \{s_t\} \cup \{s_{dt}\} \cup \{\{s_t + s_{d(t+\tau)}\} \mid 0 \le \tau \le n-1\}$.

7.28 **Theorem** The parameters of the Gold family $\mathcal{G}$ are $n = 2^r - 1$, $M = 2^r + 1$, $\theta_{max} \le \sqrt{2^{r+1}} + 1$.

7.29 **Remark** The Sidelnikov bound implies that for the family $\mathcal{G}$ of binary sequences, θ_{max} is as small as it can be for the given n and M; in this way the family $\mathcal{G}$ is optimal.

7.30 Let $r = 2k$ and $d = 2^k + 1$. Let $\{s_t\}$ be an m-sequence of period $n = 2^r - 1$. The family of *Kasami sequences* is given by $\mathcal{K} = \{s_t\} \cup \{\{s_t + s_{d(t+\tau)}\} \mid 0 \le \tau \le 2^k - 2\}$.

7.31 **Theorem** The parameters of the Kasami family are $n = 2^r - 1$, $M = 2^k$, $\theta_{max} = 1 + 2^k$.

7.32 **Remark** The Welch bound implies that the Kasami family is optimal in terms of having the smallest possible value of θ_{max} for given n and M.

7.33 The *Kerdock family* is a family of binary sequences with parameters $n = 2(2^r - 1)$, $M = 2^r$, $\theta_{max} \leq \sqrt{2^{r+1}} + 2$ where r is odd.

7.5 Quaternary Sequences with Low Crosscorrelation

7.34 Let $f(x)$ be the characteristic polynomial of a binary m-sequence of length $2^r - 1$ for some integer r. Consider $f(x)$ as a polynomial over $\mathbb{Z}_4$ and form the product $(-1)^r f(x)f(-x)$, a polynomial in x^2. The polynomial $g(x)$ over $\mathbb{Z}_4$ of degree r is defined by $g(x^2) = (-1)^r f(x)f(-x)$.

7.35 **Example** Let $f(x) = x^3 + x + 1$ be the characteristic polynomial of the m-sequence $\{s_t\}$. Then, over $\mathbb{Z}_4$, $g(x^2) = (-1)^3 f(x)f(-x) = x^6 + 2x^4 + x^2 + 3$ so that $g(x) = x^3 + 2x^2 + x + 3$.

7.36 **Remark** Families of quaternary sequences can have better crosscorrelation properties than the binary Gold and Kasami sequences. Family $\mathcal{A}$ in the next definition gives such an example. A global standard involving the third generation mobile communication uses quaternary sequences containing family $\mathcal{A}$ as well as the Gold sequences (considered as $\{0, 2\}$ sequences) as subsets.

7.37 Let $g(x) = \sum_{i=0}^{r} g_i x^i$ be obtained from a primitive polynomial $f(x)$. Consider the set of all quaternary sequences $\{s_t\}$ satisfying the recursion $\sum_{i=0}^{r} g_i s_{t+i} = 0$ for all t. All nonzero sequences generated in this way have period $2^r - 1$. *Family* $\mathcal{A}$ contains the $2^r + 1$ cyclically distinct quaternary sequences generated by the recursion.

7.38 **Theorem** The parameters of family $\mathcal{A}$ are $n = 2^r - 1$, $M = 2^r + 1$, $\theta_{max} \leq 1 + \sqrt{2^r}$.

7.39 **Remark** Family $\mathcal{A}$ has a value of θ_{max} lower than the binary Gold family by a factor of $\sqrt{2}$ for the same family size. Compared with the set of Kasami sequences it provides a much larger family size for the same bound on θ_{max}.

7.40 **Example** The sequences in family $\mathcal{A}$ generated by the recursion $s_{t+3} + 2s_{t+2} + s_{t+1} + 3s_t = 0 \pmod 4$ consist of 9 cyclically distinct sequences of length 7. In this case, $\theta_{max} \leq 1 + \sqrt{8}$.

7.6 Aperiodic Correlation

7.41 Let $\{x\} = (x_0, x_1, \ldots, x_{n-1})$ be a binary $\{-1, +1\}$ sequence of length n. The *aperiodic correlation* $\rho_x(\tau)$ is given by

$$\rho_x(\tau) = \sum_{t=0}^{n-1} x_{t+\tau} x_t$$

where $x_t = 0$ for $t < 0$ or $t \geq n$.

7.42 A binary $\{-1, +1\}$ sequence $\{s_t\}$ of length n is a *Barker sequence* if the aperiodic autocorrelation values $\rho_s(\tau)$ satisfy $\mid \rho_s(\tau) \mid \leq 1$ for all $\tau, 0 \leq \tau \leq n - 1$.

7.43 **Remarks** Barker sequences are the least autocorrelated binary sequences and are used for pulse compression of radar signals. The Barker property is preserved under the transformations $s_t \to -s_t$, $s_t \to (-1)^t s_t$ and $s_t \to s_{n-1-t}$. Only the following Barker sequences (and equivalent sequences by applying the transformations given)

are known:

$n = 2$ 11 $n = 3$ $11-$
$n = 4$ $111-$ $n = 5$ $111-1$
$n = 7$ $111--1-$ $n = 11$ $111---1--1-$
$n = 13$ $11111--11-1-1$

7.44 **Remark** It is known that if any other Barker sequence exists, it must have length $n > 1,898,884$ that is a multiple of 4.

7.7 Sequences with Low Merit Factor

7.45 The *merit factor* F of a $\{-1,+1\}$ sequence $\{s_t\}$ of length n is $F = \frac{n^2}{2\sum_{\tau=1}^{n-1} \rho_s^2(\tau)}$.

7.46 **Remark** The merit factor is one measure of the aperiodic autocorrelation properties of a binary $\{-1,+1\}$ sequence. The highest known merit factor of an individual sequence is 14.08, obtained from the Barker sequence of length 13. The largest merit factor of an infinite family of sequences is apparently greater than 6.34 [297, 1362], but there is no proof of this at this time.

See Also

§V.1	Hadamard designs and matrices.
§V.8	Complementary, Base, and Turyn Sequences.
§VI.18	Cyclic difference sets give sequences with low autocorrelation.
[636, 1191]	Barker arrays, a generalization of Barker sequences to higher dimensions. For dimension at least 2, the only Barker array is 2×2 (of dimension 2).
[928]	Thorough treatment of sequence correlation.

References Cited: [297, 636, 707, 709, 928, 1089, 1191, 1362, 1909]

8 Complementary, Base, and Turyn Sequences

Hadi Kharaghani
Christos Koukouvinos

8.1 Basic Definitions

8.1 For the $\{0, \pm 1\}$-sequence $A = a_1, a_2, \cdots, a_n$ of length n the *periodic autocorrelation function* P_A of A is

$$P_A(i) = \sum_{j=1}^{n} a_j a_{i+j} \text{ for } i = 0, 1, \cdots, n-1,$$

where $i + j$ is reduced mod n and $P_A(i) = P_A(j)$ iff $i \equiv j \bmod n$. The *nonperiodic autocorrelation function* N_A of A is

$$N_A(i) = \sum_{j \in Z} a_j a_{i+j}, \text{ where } a_k = 0, \text{ if } k < 1 \text{ or } k > n.$$

8.2 **Remark** Because $P_A(i) = \sum_{j \equiv i \bmod n} N_A(j)$, $N_A(-i) = N_A(i)$ for all $i \in Z$ and $P_A(i) = N_A(i) + N_A(n-i)$ for $0 \le i \le n-1$.

8.3 The polynomial $A(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ corresponding to the sequence $A = a_1, a_2, \cdots, a_n$ is the *Hall polynomial* of the sequence A. Viewing this polynomial as an element of the Laurent polynomial ring $Z[x, x^{-1}]$, one can see that $A(x)A(x^{-1}) = \sum_{j \in Z} N_A(j)x^j$. The *weight of* A, denoted $w(A)$, is $w(A) = A(x)A(x^{-1}) \in Z[x, x^{-1}]$.

8.4 A family of $\{0, \pm 1\}$-sequences $\{A_i\}$, $1 \le i \le q$, all of length n, for which $\sum_1^q N_{A_i}(j) = 0$ ($\sum_{i=1}^q P_{A_i}(j) = 0$) for $j \ne 0$, or equivalently: if $\sum_{i=1}^q w(A_i)$ is a constant function (mod $x^n - 1$, respectively), is a family of *nonperiodic* (*periodic*, respectively) *complementary sequences* and is denoted by $NCS(n, q)$ ($PCS(n, q)$, respectively).

8.5 A family of $\{0, \pm 1\}$-sequences $\{A_i\}$, $1 \le i \le q$, all of length n, that satisfy $\sum_1^q N_{A_i}(j) = 0$ for all $j \ne 0$ is a family of *nonperiodic complementary sequences* and is denoted by $NCS(n, q)$. If it satisfies $\sum_{i=1}^q P_{A_i}(j) = 0$ for $j \ne 0$, it is a family of *periodic complementary sequences* and denoted $PCS(n, q)$).

8.6 An $NCS(n, q)$ is also a $PCS(n, q)$. For binary sequences $NCS(n, 2)$ is a *Golay complementary pair* (or *Golay sequences*) of length n, and denoted $GCP(n)$.

8.2 Complementary Sequences

8.7 **Remark** All sequences in this chapter are assumed to be $\{\pm 1\}$-sequences.

8.8 **Proposition** If there exist $NCS(n, q)$ and $NCS(n, r)$, then there exists an $NCS(n, q+r)$. Similarly, if there exist $PCS(n, q)$ and $PCS(n, r)$, then there exists a $PCS(n, q+r)$.

8.9 **Proposition** If there exists a $PCS(n, q)$ and $n \ge 2$, then

1. $nq = \sum_{i=1}^q c_i^2$, where c_i are integers and $c_i \equiv n \pmod 2$, $1 \le i \le q$, and
2. $nq \equiv 0 \pmod 4$.

8.10 **Theorem** If there exist $NCS(n_i, q_i)$ for $1 \le i \le s$, then an $NCS(n_1n_2 \cdots n_s, \frac{q_1q_2 \cdots q_s}{2^{s-1}})$ exists.

8.11 **Theorems**

1. If $n > 1$ and a $GCP(n)$ exists, then all odd prime divisors of n are congruent to 1 (mod 4).
2. If a $PCS(n, 2)$ exists, $n = p^{2\ell}u$, $u \not\equiv 0 \pmod p$, p is a prime power, and $p \equiv 3 \pmod 4$, then $u \ge 2p^\ell$.

8.12 **Theorem** (see [298, 739]) There is only one $GCP(2)$ and $GCP(26)$, and two $GCP(10)$ up to equivalence. They are:

$n = 2$ (11;1-)
$n = 10$ (-11-1-111-;-111111--1)
$n = 10$ (1-1-1111--;1111-11--1)
$n = 26$ (1-11--1----1-1----11---1-1;-1--11-1111-------11---1-1)

8.13 **Remarks** The *Golay numbers*, $n = 2^a10^b26^c$ for $a, b, c \ge 0$, are the only values for which a $GCP(n)$ is known to exist. There is a $PCS(34, 2)$ [740], and, hence, $PCS(34, 2m)$ exist for all $m \ge 1$.

8.14 **Table** Number of distinct $GCP(n)$ and inequivalent $GCP(n)$ (denoted N_D and N_E, respectively) for $N < 100$ [739, 298].

n	N_D	N_E	n	N_D	N_E	n	N_D	N_E	n	N_D	N_E
1	4	1	2	8	1	4	32	1	8	192	5
10	128	2	16	1536	36	20	1088	25	26	64	1
32	15360	336	40	9728	220	52	512	12	64	184320	3840
80	102912	open									

8.15 **Conjecture** There is a $GCP(n)$ only if $n = 2^a 10^b 26^c$ with $a, b, c \geq 0$.

8.16 **Remark** Conjecture 8.15 is verified for all lengths up to 106.

8.17 **Table** Unresolved $PCS(n, p)$ with $p \leq 12$ and $n \leq 50$ [740].

p	n	p	n
2	50	7	40,44,48
3	40,44,48	9	40,44,48
5	40,44,48	10	38,42,44,46,50
6	38,42,44,46,50	11	40,44,48

8.3 Base Sequences

8.18 A quadruple of binary sequences $(A; B; C; D)$ where A, B are of lengths m, C, D are of lengths n, and $w(A) + w(B) + w(C) + w(D) = 2(m + n)$ is a *base sequence* and is denoted $BS(m, n)$. Note that $BS(n, n) = NCS(n, 4)$.

8.19 **Examples** $BS(n + 1, n)$ for $n = 1, \ldots, 5$.

$n = 1$ `(11;1-;1;1)`
$n = 2$ `(111;1--;1-;1-)`
$n = 3$ `(11-1;11--;111;1-1)`
$n = 4$ `(1111-;1---1;11-1;11-1)`
$n = 5$ `(11-1-1;111---;11-11;11-11)`

8.20 **Construction** Let $(X; Y)$ be a Golay complementary pair of length n. Then the quadruple $(X, 1; X, -; Y; Y)$ is a $BS(n + 1, n)$, where A, B denotes the concatenation of the sequences A and B.

8.21 **Theorem** [738] If $m \geq 2n$, $n > 1$, and $m + n$ is odd, then there is no $BS(m, n)$.

8.22 **Theorem** [738] If $n > 1$ is odd, then there is no $BS(2n - 1, n)$.

8.23 **Conjecture** (*Base Sequence Conjecture* [738]) There is a $BS(n + 1, n)$ for all integers $n \geq 0$.

8.24 **Remark** Conjecture 8.23 is verified for all $n \leq 35$ and all Golay numbers n.

8.4 Turyn Sequences

8.25 A sequence $A = a_1, a_2, \ldots, a_n$ is *symmetric* if $A = A^*$, where $A^* = a_n, \ldots, a_2, a_1$ is the reverse of the sequence A. A base sequence $BS(n+1, n)$ $(A; B; C; D)$ is a *Turyn sequence*, denoted $TU(n)$, if $A^* = A$, $C^* = -C$, whenever n is even and $A^* = -A$, $C^* = C$, whenever n is odd.

8.26 **Example** Turyn sequences for $n = 6$ and $n = 7$.
$n = 6$ `(111-111;11---1-;11-1--;11-1--)`
$n = 7$ `(11-1-1--;1111---1;111-111;1--1--1)`

8.27 **Theorem** Turyn sequences $TU(n)$ exist for $n = 1, 2, 3, 4, 5, 6, 7, 12, 14$, and are known not to exist for all $n \in \{8 \le n \le 51, n \ne 12, 14\}$.

8.28 **Theorem** If a $TU(n)$ exist, then a $BS(2n + 2, 2n + 1)$ exists.

8.5 Turyn Type Sequences

8.29 Four binary sequences $(A; B; C; D)$ where A, B, C are of lengths n, D is of length $n-1$, and $w(A)+w(B)+2w(C)+2w(D) = 6n-2$ are *Turyn type sequences* denoted $TUT(n)$.

8.30 **Example** Turyn type sequences for $n = 4$.
$n = 4$ `(1111;1-11;11--;1-1)`

8.31 **Construction** If $(A; B; C; D)$ is a $TUT(n)$, then $(C, D; C, -D; A; B)$ is a $BS(2n-1, n)$.

8.32 **Theorems**

1. If there is a $TUT(n)$, then n is even.
2. $TUT(n)$ exist for all even n, $2 \le n \le 36$.

8.6 Normal and Near Normal Sequences

8.33 The ordered sequences $(X; Y; Z)$ of lengths n are *normal sequences*, denoted $NS(n)$, if X is a binary sequence and Y and Z are disjoint $(0, \pm 1)$-sequences for which $w(X)+w(Y)+w(Z) = 2n$. An ordered quadruple of binary sequences $(A; B; C; D)$, which is a $BS(n + 1, n)$, is a *near normal sequence*, denoted $NNS(n)$, if n is even, $b_i = (-1)^{i-1}a_i$, $1 \le i \le n$, and $a_n = 1, b_n = -1$.

8.34 **Example** A $NS(7)$ and a $NNS(4)$:
$n = 7$ `(1-111--;11010-1;0010100)`
$n = 4$ `(1---1;11-1-;1111;1--1)`

8.35 **Theorem** [2176] There is a $NS(n)$ for each Golay number n.

8.36 **Theorem** If there is a $TU(n)$, then there is a $NS(2n + 1)$.

8.37 **Corollary** There is a $NS(2n + 1)$ for $n \le 7$, $n = 12$, and $n = 14$.

8.38 **Theorem** There is no $NS(n)$ for $n = 6, 14, 17, 21, 22, 23, 24, 27, 28, 30$ (all other orders of $n < 31$ exist). $NS(31)$ is the first unknown case.

8.39 **Conjecture** (Yang) There is a $NNS(n)$ for each even integer n.

8.40 **Remark** Conjecture 8.39 is verified for all even integers $n \le 30$.

8.41 An odd integer $2n + 1$ for which at least one of $NS(n)$ or $NNS(n)$ exists is a *Yang number*.

8.42 **Theorems**

1. An odd integer $n \le 61$ is a Yang number if and only if $n \ne 35, 43, 47, 55$.
2. If n is a Golay number, then $2n + 1$ is a Yang number.

8.7 Base Sequences and T-Sequences

8.43 An ordered quadruple $(A;B;C;D)$ of $(0,\pm1)$-sequences of the same length n for which $w(A)+w(B)+w(C)+w(D)=n$, and exactly one of a_i,b_i,c_i,d_i is nonzero for $1\le i\le n$, is a *T-sequence of length* n, denoted $TS(n)$.

8.44 **Construction** (Turyn) If $(A;B;C;D)$ is a $BS(m,n)$, then

$$(\frac{1}{2}(A+B),0_n;\frac{1}{2}(A-B),0_n;0_m,\frac{1}{2}(C+D);0_m,\frac{1}{2}(C-D)),$$

is a $TS(m+n)$. (Here 0_k denotes the zero sequence of length k).

8.45 **Theorem** (Yang multiplications [1330, 2176])

1. If there is a $NS(t)$ and a $BS(m,n)$, then there is a $TS((2t+1)(m+n))$.
2. If there is a $NNS(t)$ and a $BS(m,n)$, then there is a $TS((2t+1)(m+n))$.

8.46 **Conjecture** (T-Sequence Conjecture) There is a $TS(n)$ for each odd integer $n\ge1$.

8.47 **Remark** The T-sequence conjecture (Conjecture 8.46) is verified for all odd integers $n<200$ except for $n=$ 73, 79, 97, 103, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 183, 191, 193, 197, 199.

See Also

§V.1	Sequences are used in the construction of Hadamard matrices.
§V.2	Sequences are used in the construction of orthogonal designs.
§V.2	T-sequences of length n provide T-matrices of order n.
§V.7	Sequences with low autocorrelation.
§VI.18	There is a relationship between periodic complementary sequences and a subclass of cyclic difference sets.
[298]	A complete description of Golay pairs for lengths up to 100.
[738]	A complete listing of all $BS(n+1,n)$, $TU(n)$, $NS(n)$, and $NNS(n)$ for different values of $n\le51$.
[740]	A number of periodic and nonperiodic complementary sequences.
[810]	Recursive construction of periodic and nonperiodic complementary sequences.

References Cited: [298, 738, 739, 740, 810, 1330, 2176]

9 Optical Orthogonal Codes

Tor Helleseth

9.1 The *Hamming correlation* between a pair of binary $\{0,1\}$ sequences $\{s_t^{(1)}\}$ and $\{s_t^{(2)}\}$ each having period n, is $\theta_{12}(\tau)=\sum_{t=0}^{n-1}s_{t+\tau}^{(1)}s_t^{(2)}$ where $0\le\tau\le n-1$ and θ_{12} is calculated as an integer.

9.2 **Remark** Such correlation is of interest in optical communication systems where the 1s and 0s in a sequence correspond to the presence or absence of pulses of transmitted light. Sequences with low Hamming crosscorrelation are also of interest in frequency-hopping multiple-access communication systems. Here each user's signal hops over the entire transmission bandwidth in a pseudorandom fashion, and it is desired that collisions, simultaneous transmissions over the same frequency subband between the signals of different users, are minimized.

9.3 An (n, w, λ) optical orthogonal code (OOC) is a family $\mathcal{F} = \{\{s_t^{(i)}\} \mid i = 1, 2, \cdots, M\}$ of M binary sequences of period n, constant Hamming weight w and $\theta_{ij}(\tau) \leq \lambda$ when either $i \neq j$ or $\tau \neq 0$.

9.4 **Remark** OOCs are closely related to constant weight error correcting codes. An (n, w, λ) OOC supplemented by every cyclic shift of each sequence yields a constant weight code with minimum distance $d_{min} \geq 2(w - \lambda)$. Conversely a cyclic constant weight code of length n, weight w, and minimum distance d_{min} yields an (n, w, λ) OOC with $\lambda \leq w - \frac{d_{min}}{2}$, by partitioning the code into cyclic equivalence classes and selecting one representative from each class of size n. Therefore, one can derive bounds on the size of an OOC from known bounds on the size of constant weight codes.

9.5 **Theorem** The number $M(n, w, \lambda)$ of codewords in an (n, w, λ) OOC does not exceed $\frac{1}{w}\left\lfloor \frac{n-1}{w-1} \cdots \left\lfloor \frac{n-\lambda+1}{w-\lambda+1} \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \right\rfloor \cdots \right\rfloor$ and $M(n, w, \lambda) \leq \max\left(1, \left\lfloor \frac{\omega-\lambda}{\omega^2-n\lambda)} \right\rfloor\right)$, $\omega^2 > n\lambda$.

9.6 An OOC that achieves the bound in Theorem 9.5 is *optimal*.

9.7 **Table** Table of OOC constructions. See [1699] for references not given. For current results on OOCs with "small" weight, see also [23, 459] for $(v, 4, 1)$, [504, 505] for $(v, 4, 2)$, and [1491] for $(v, 5, 1)$.

Construction	Parameters	Code size
Singer construction (Chung–Salehi–Wei)	$(q^2+q+1, q+1, 1)$ $q = p^m$	1
Projective geometry	$(\frac{q^{d+1}-1}{q-1}, q+1, 1)$ $q = p^m$	$\frac{q^d-1}{q^2-1}$, d even $\frac{q^d-q}{q^2-1}$, d odd
[23]	$(n, 3, 1)$, $n \not\equiv 14, 20 \pmod{24}$	$\lfloor \frac{n-1}{6} \rfloor$
Chung–Kumar	$(p^{2m}-1, p^m+1, 2)$	$p^m - 2$
Chung–Kumar (Wilson)	$(p = \omega(\omega-1)r+1, \omega, 1)$ $\omega = 2m$ or $\omega = 2m+1$	r
[1699]	$(q^2-1, q, 1)$, $q = p^m$	1
[1699]	$(q^a-1, q, 1)$, $q = p^m$	$\frac{q^{a-1}-1}{q-1}$

See Also

§VI.16	Difference families over cyclic groups construct OOCs.
§VI.18	Cyclic difference sets give sequences with low autocorrelation.
§VI.19	"Strict" OOCs are equivalent to difference triangle sets [510].
§VI.53	Skolem sequences produce optimal $(v, 3, 1)$-OOCs [23].
§VII.1	OOCs are cyclic constant weight codes.
§VII.2	Conics in finite geometries are used to construct OOCs [1619].

References Cited: [23, 459, 504, 505, 510, 1491, 1619, 1699]

Part VI

Other Combinatorial Designs

1 Association Schemes

Christopher D. Godsil
Sung Y. Song

1.1 Definitions and Examples

1.1 Let d denote a positive integer, and let X be a nonempty finite set. A *d-class symmetric association scheme* on X is a sequence $R_0, R_1, \ldots, R_d$ of nonempty subsets of the Cartesian product $X \times X$, satisfying

1. $R_0 = \{(x, x) \mid x \in X\}$,
2. $X \times X = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$,
3. for all $i \in \{0, 1, \ldots, d\}$, $R_i^T = R_i$ where $R_i^T := \{(y, x) \mid (x, y) \in R_i\}$,
4. for all integers $h, i, j \in \{0, 1, \ldots, d\}$, and for all $x, y \in X$ such that $(x, y) \in R_h$, the number $p_{ij}^h := |\{z \in X \mid (x, z) \in R_i,\ (z, y) \in R_j\}|$ depends only on h, i, j, and not on x or y.

1.2 **Remarks** The numbers p_{ij}^h are the *intersection numbers* of the scheme. The set R_i is the ith *associate class* and is represented by the ith *associate matrix* A_i. That is, A_i is the $\{0, 1\}$-matrix of order $|X|$ whose rows and columns are indexed by the elements of X and whose entries satisfy $(A_i)_{xy} = \begin{cases} 1 & \text{if } (x, y) \in R_i \\ 0 & \text{otherwise} \end{cases}$. The following is an equivalent definition.

1.3 A *d-class symmetric association scheme* $\mathcal{A}$ with vertex set X is a sequence of nonzero $\{0, 1\}$-matrices $A_0, \ldots, A_d$ with rows and columns indexed by X, such that

$1'$. $A_0 = I$,
$2'$. $\sum_{i=0}^{d} A_i = J$, where J denotes the all-1 matrix,
$3'$. $A_i^T = A_i$ for all $i \in \{0, 1, \ldots, d\}$,
$4'$. $A_i A_j$ lies in the real span of $A_0, \ldots, A_d$: $A_i A_j = \sum_h p_{ij}^h A_h$.

1.4 **Remarks** $3'$ and $4'$ imply that the product $A_i A_j$ is symmetric, and $A_i A_j = A_j A_i$. They also imply that the vector space formed by the real span $\langle \mathcal{A} \rangle$ of $A_0, \ldots, A_d$ is a matrix algebra, the *Bose–Mesner algebra* of the association scheme. Various generalizations of the notion of an association scheme have been proposed. Delsarte [673] introduced the following notion, often referred to as a commutative scheme.

1.5 A *d-class association scheme* with vertex set X is a sequence $R_0, R_1, \ldots, R_d$ of nonzero relations on X such that axioms 1, 2, and 4 hold together with the following 5 and 6 (instead of 3):

5. for every $i \in \{0, 1, \ldots, d\}$, there exists $j \in \{0, 1, \ldots, d\}$ such that $R_i^T = R_j$,
6. $p_{ij}^h = p_{ji}^h$ for all $h, i, j \in \{0, 1, \ldots, d\}$.

Equivalently, a *d-class association scheme* $\mathcal{A}$ with vertex set X is a sequence of nonzero $\{0, 1\}$-matrices $A_0, \ldots, A_d$ with rows and columns indexed by X such that axioms $1', 2'$, and $4'$ hold, along with

$5'$. if $A_i \in \mathcal{A}$, then $A_i^T \in \mathcal{A}$,
$6'$. $A_i A_j = A_j A_i$ for all i and j.

1.6 **Example** Let a group G act transitively on a finite set X. Then G acts naturally on the set $X \times X$ by $(x, y)g = (xg, yg)$. Under this action, the set $R_0 = \{(x, x) : x \in X\}$ is an orbit, and the number of orbits is at least 2. Let $X \times X$ be decomposed into the $d+1$ orbits $R_0, R_1, \ldots, R_d$. This set of orbits forms a d-class symmetric association scheme if and only if for any two distinct elements $x, y \in X$, there is $g \in G$ such that $xg = y$ and $yg = x$. (Such a group is *generously transitive*.) In terms of group characters, the set of orbits forms a symmetric association scheme if and only if the permutation character is multiplicity-free and every irreducible representation associated with each irreducible character that appears in the decomposition of the permutation character is realizable in the real number field. However, the orbits form a commutative association scheme if and only if the permutation character is multiplicity-free. In particular, any transitive permutation group gives rise to a more general configuration that satisfies the axioms 1, 2, 4, and 5, what Higman [1097] calls a *homogeneous coherent configuration*.

1.7 **Remark** Nonsymmetric schemes do not provide the strength needed in the design theory context, although most of the results discussed in what follows remain true for commutative schemes with some modification (mainly replacing the real by the complex field in the algebraic arguments). In what follows all schemes are assumed to be symmetric unless otherwise specified. Important classes of schemes are P-polynomial and Q-polynomial schemes, in particular, the Hamming and Johnson schemes.

1.8 The *Hamming scheme* $H(n, q)$ has the set F^n of all words of length n over an alphabet F of q symbols as its vertex set. Two words are ith associates if and only if the Hamming distance between them is i. The *Johnson scheme* $J(v, k)$, with $k \leq \frac{1}{2}v$, has the set of all k-subsets of a set of size v as its vertices. Two k-sets α and β are ith associates if and only if $|\alpha \cap \beta| = k - i$.

1.2 P- and Q-Polynomial Schemes

1.9 **Remark** Given a d-class scheme $\mathcal{A}$, the symmetric matrices $A_1, \ldots, A_d$ can be viewed as adjacency matrices of graphs $G_1, \ldots, G_d$; thus, a d-class scheme may be viewed as a partition of the edge set of a complete graph into d spanning subgraphs. (Where necessary, the ith class R_i of $\mathcal{A}$ is viewed as the edge set $E(G_i)$ of unordered pairs.)

1.10 A d-class scheme is *primitive* if each of the graphs $G_1, \ldots, G_d$ is connected; otherwise, it is *imprimitive*.

1.11 **Remark** If $\mathcal{A}$ is an imprimitive scheme with graph G_i disconnected, then the relations of $\mathcal{A}$ induced on a connected component of G_i form a *subscheme*, and there is a natural way to define a *quotient scheme* on the components of G_i [912, pp. 232–234].

1.12 **Example** A two-class scheme is equivalent to a complementary pair of strongly regular graphs (see VII.11). In the imprimitive case, one relation is the edge set of a complete multipartite graph and the other is a disjoint union of pairwise isomorphic complete graphs. Both the subschemes and the quotient scheme are complete in this case.

1.13 A graph G of diameter d is *distance-regular* if there exist integers a_i, b_i, and c_i $(0 \leq i \leq d)$ such that, for any two vertices x and y of G at distance i, vertex y has c_i neighbors at distance $i-1$ from x, a_i neighbors at distance i from x, and b_i neighbors at distance $i+1$ from x. Such a graph is necessarily regular of valency $k = b_0$.

1.14 **Remark** Just as a t-(v, k, λ) design can be viewed as a combinatorial generalization of a t-transitive permutation group action, a distance-regular graph is a combinatorial generalization of a *distance-transitive* graph, one where the automorphism group is

transitive on pairs of vertices at distance i for each i.

1.15 A d-class scheme $\mathcal{A}$ is *metric* with respect to the ordering $R_0, R_1, \ldots, R_d$ of its relations if the following hold
(1) $p_{ij}^h = 0$ unless $|i-j| \le h \le i+j$ for all h, i, j, and
(2) $p_{ij}^h > 0$ whenever $i + j = h \le d$.

1.16 A d-class scheme $\mathcal{A}$ is *P-polynomial* (with respect to the ordering $A_0, A_1, \ldots, A_d$) if there are polynomials $v_0, v_1, \ldots, v_d$, where v_i has degree i, so that $A_i = v_i(A_1)$ for all i.

1.17 Theorem For a d-class scheme $\mathcal{A}$ with associate matrices A_i and corresponding graphs G_i, the following are equivalent:
(1) $\mathcal{A}$ is metric with respect to the ordering $A_0, A_1, \ldots, A_d$;
(2) $\mathcal{A}$ is P-polynomial with respect to the ordering $A_0, A_1, \ldots, A_d$; and
(3) G_1 is a distance-regular graph of diameter d and G_i is the distance-i graph of G_1 for each i.

1.18 Remark The polynomials v_i can be recovered from the intersection numbers p_{1i}^h via the three-term recurrence $A_1 A_i = p_{1i}^{i+1} A_{i+1} + p_{1i}^i A_i + p_{1i}^{i-1} A_{i-1}$.

1.19 Remarks The Hamming and Johnson schemes are metric schemes. The distance-regular graphs that give rise to these schemes are the *Hamming* and *Johnson graphs*. It can happen that more than one associate graphs in a scheme is distance-regular; so the scheme can be metric in more than one way (see [137, §I.4] or [343]).

1.20 Remarks Let $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$ be a d-class scheme on the vertex set X. As the matrices in the Bose–Mesner algebra $\langle \mathcal{A} \rangle$ are normal and commute, $\mathbb{R}^X$ can be expressed as the direct sum of its eigenspaces. There are exactly $d+1$ eigenspaces and the orthogonal projections onto them are denoted by $E_0, \ldots, E_d$, where $E_0 = |X|^{-1} J$ and $E_i E_j = \delta_{ij} E_i$. As E_i is primitive idempotent, its trace and its rank are equal, and both are equal to the dimension of the corresponding eigenspace.

1.21 The ith *multiplicity* is defined to be the dimension of the ith eigenspace and is denoted f_i. The ith *valency* is defined to be p_{ii}^0 and denoted k_i, which is the row sum of A_i.

1.22 Theorem Let $A_0, \ldots, A_d$ form an association scheme and let $E_0, \ldots, E_d$ be its primitive idempotents. Then $\{A_0, A_1, \ldots, A_d\}$ and $\{E_0, E_1, \ldots, E_d\}$ are two distinct bases for $\langle \mathcal{A} \rangle$. Hence, there are numbers $p_i(j)$ such that $A_i = \sum_j p_i(j) E_j$ and numbers $q_j(i)$ such that $E_j = |X|^{-1} \sum_i q_j(i) A_i$.

1.23 The $p_i(j)$ are the *eigenvalues* of the scheme, while the $q_i(j)$ are the *dual eigenvalues*. Define the $(d+1) \times (d+1)$ base change matrices P and Q by $(P)_{i,j} := p_j(i)$ and $(Q)_{i,j} := q_j(i)$, respectively. The entries of the ith column of P are the eigenvalues of A_i. Then $PQ = |X| I$ and also $f_j p_i(j) = k_i q_j(i)$.

1.24 Theorem In a scheme, $\sum_r k_r q_i(r) q_j(r) = \delta_{ij} |X| f_i$ and $\sum_h f_h p_i(h) p_j(h) = \delta_{ij} |X| k_i$.

1.25 Theorem For the Hamming scheme $H(n, q)$, $k_i = f_i = (q-1)^i \binom{n}{i}$ and
$$q_i(j) = p_i(j) = \textstyle\sum_{r=0}^{i} (-1)^r (q-1)^{i-r} \binom{n-j}{i-r} \binom{j}{r}.$$

1.26 Theorem For the Johnson scheme $J(v, k)$, with the convention that $\binom{v}{-1} = 0$, one has
$$k_i = \textstyle\binom{k}{i}\binom{v-k}{i}, \qquad f_i = \binom{v}{i} - \binom{v}{i-1},$$
$$p_i(j) = \textstyle\sum_{r=0}^{i} (-1)^{i-r} \binom{k-r}{i-r} \binom{v-k+r-j}{r} \binom{k-j}{r}, \text{ and}$$
$$q_i(j) = \textstyle\binom{v-2i}{k-i}^{-1} \binom{v}{k} \sum_{r=0}^{i} (-1)^{i-r} \binom{v+1-i-r}{i-r}^{-1} \binom{k-r}{i-r}^2 \binom{k-j}{r}.$$

1.27 **Remark** For a d-class scheme $\mathcal{A}$, the Bose–Mesner algebra $\langle\mathcal{A}\rangle$ of $\mathcal{A}$ is closed under the entry-wise product $\circ$ (Hadamard product) as $A_i \circ A_j = \delta_{ij} A_i$. Thus, $E_i \circ E_j$ is also in $\langle\mathcal{A}\rangle$, and there exist nonnegative real numbers q_{ij}^h (*Krein parameters*) such that $E_i \circ E_j = |X|^{-1} \sum_{h=0}^{d} q_{ij}^h E_h$.

1.28 A d-class scheme $\mathcal{A}$ is *cometric* with respect to the ordering $E_0, E_1, \ldots, E_d$ of its primitive idempotents if the following hold
(1) $q_{ij}^h = 0$ unless $|i-j| \le h \le i+j$ for all h, i, j, and
(2) $q_{ij}^h > 0$ whenever $i + j = h \le d$.

1.29 A d-class scheme $\mathcal{A}$ is *Q-polynomial* (with respect to the ordering $E_0, E_1, \ldots, E_d$) if there are polynomials $w_0, w_1, \ldots, w_d$, where w_i has degree i, so that $|X|E_i = w_i(|X|E_1)$ for all i where these polynomials are computed using the Hadamard product $\circ$ as the multiplication operation.

1.30 **Theorem** For a d-class scheme $\mathcal{A}$ with primitive idempotents E_i, the following are equivalent:
(1) $\mathcal{A}$ is cometric with respect to the ordering $E_0, E_1, \ldots, E_d$; and
(2) $\mathcal{A}$ is Q-polynomial with respect to the ordering $E_0, E_1, \ldots, E_d$.

1.3 Codes and Designs in P- and Q-Polynomial Schemes

1.31 If S is a subset of the vertex set X of a P-polynomial scheme, then the *minimum distance* of S is the minimum distance in G_1 between two distinct vertices of S. If S has minimum distance δ, then $\lfloor \frac{\delta-1}{2} \rfloor$ is the *packing radius* of S; the *covering radius* of S is the maximum distance of any vertex in X from S. If the packing radius of S is equal to its covering radius, S is a *perfect code*.

1.32 If S is a subset of the vertex set X of a d-class scheme with size $b > 0$ and characteristic vector $\mathbf{u}$, (that is, $u_x = 1$ if $x \in S$; $u_x = 0$ if $x \in X - S$), then the vector $\mathbf{a}$ in $\mathbb{R}^{d+1}$ given by $a_i = b^{-1}|R_i \cap (S \times S)| = b^{-1}\mathbf{u}^T A_i \mathbf{u}$, $i \in \{0, 1, \ldots, d\}$ is the *inner distribution* of S. Observe that $a_0 = 1$, $a_0 + a_1 + \cdots + a_d = |S|$. The number of positive indices i such that $a_i \neq 0$ is the *degree* of S; it represents the number of distinct nonzero distances that occur among the members of S.

1.33 **Example** In the trivial case $S = X$, $a_i = k_i$ for all i.

1.34 The *dual degree* of a subset S of X with characteristic vector $\mathbf{u}$ is the cardinality of $\{i > 0 : E_i\mathbf{u} \neq \mathbf{0}\}$. For $T \subseteq \{1, 2, \ldots, d\}$, S is referred to as a *Delsarte T-design* if $E_i\mathbf{u} = \mathbf{0}$ for all indices i in T. If $\mathcal{A}$ is cometric with respect to ordering $E_0, E_1, \ldots, E_d$, then the *strength* of S (as a Delsarte design) is the largest t for which S is a Delsarte $\{1, 2, \ldots, t\}$-design.

1.35 **Remark** Covering radius and dual degree are interesting and useful concepts in coding theory, but have not received much attention in design theory yet.

1.36 **Lemma** Let $\mathcal{A}$ be a P-polynomial scheme with vertex set X, and let S be a subset of X with covering radius r and dual degree s^*. Then $r \le s^*$.

1.37 The *outer distribution matrix* of S is the matrix with columns $A_0\mathbf{u}, A_1\mathbf{u}, \ldots, A_d\mathbf{u}$. The dual degree of S is also one less than the rank of the outer distribution matrix of S. A subset S of the vertex set of a P-polynomial scheme is *completely regular* if its covering radius is one less than the number of distinct rows in its outer distribution matrix.

1.38 The *dual inner distribution* of a subset S of the vertex set X of a d-class scheme is the vector $\mathbf{b}$ in $\mathbb{R}^{d+1}$ such that $\mathbf{b} = Q^T\mathbf{a}$; that is, $b_i := \frac{|X|}{|S|}\mathbf{u}^T E_i\mathbf{u}$. The Q-transform is the *MacWilliams transform* of the inner distribution $\mathbf{a}$.

1.39 **Example** If $H(n,q)$ is the Hamming scheme with $F = \mathbb{F}_q$ as alphabet and C is a subspace of $H(n,q)$, then the dual inner distribution of C is the inner distribution of the dual code to C, scaled by $|C|$.

1.40 **Theorem** If $\mathbf{a}$ is the inner distribution of a subset of X, one has *Delsarte's inequalities*, equivalently the *linear programming bound*: $Q^T\mathbf{a} \geq 0$.

1.41 **Remark** Delsarte's inequalities are very important as they give conditions satisfied by the Q-transform of a subset of the scheme, knowing only information such as "block intersection numbers". For applications in design theory and coding theory, see [673, 1505, 2155].

1.42 **Remark** Schrijver [1856] has recently developed an extension of Delsarte's linear programming bound using a noncommutative algebra, the *Terwilliger algebra* [2018, 2019].

1.43 **Lemma** (Delsarte) In a cometric scheme $\mathcal{A}$ where the columns of Q are ordered in a manner consistent with the Q-polynomial ordering $E_0, \ldots, E_d$ of the primitive idempotents, the strength of $S \subseteq X$ with inner distribution $\mathbf{a}$ and dual inner distribution $\mathbf{b} = Q^T\mathbf{a}$ is the largest $t \geq 0$ for which $b_1 = b_2 = \cdots = b_t = 0$ where b_i is the i^{th} entry of $\mathbf{b}$.

1.44 **Theorem** (Delsarte) A subset of the Hamming scheme $H(n,q)$ is the set of columns of an orthogonal array of strength t if and only if, as a Delsarte design, it has strength at least t.

1.45 **Example** If S is a linear code, then its strength as an orthogonal array is one less than the minimum distance of its dual code.

1.46 **Theorem** (Delsarte) A subset of the Johnson scheme $J(v,k)$ is the set of blocks of a t-(v,k,λ) design if and only if, as a Delsarte design, it has strength at least t.

1.4 Parameters of Designs

1.47 **Theorem** [1783] If a t-design $\mathcal{D}$ with degree s has v points and b blocks, then $\binom{v}{t/2} \leq b \leq \binom{v}{s}$. If one of the inequalities is tight, so is the other. (See §II.4.)

1.48 Designs with $t = 2s$ are *tight t-designs*.

1.49 **Theorems**

1. The only tight 4-designs are the Witt design on 23 points and its complement (see §II.5.6 or [1992] and references therein).
2. [1732] There are no tight 6-designs.
3. [155] If $t = 2s \geq 10$, then there are at most finitely many tight t-designs.

1.50 **Remark** When $t = 2$, tight designs are equivalent to symmetric designs.

1.51 Let $\mathcal{D}$ be a design with degree set $i_1, \ldots, i_s$. Let A_r be the $\{0,1\}$-matrix with rows and columns indexed by the blocks of $\mathcal{D}$ and with $\alpha\beta$-entry equal to one if and only if $|\alpha \cap \beta| = i_r$. Let A_0 be the identity matrix. $\mathcal{D}$ is *schematic* if $A_0, \ldots, A_s$ form an association scheme, the scheme *induced* by $\mathcal{D}$. A 1-design is a *partially balanced incomplete block design* (PBIBD) if and only if its dual design is schematic.

1.52 **Theorem** [414] Let $\mathcal{D}$ be a t-design with degree s. If $t \geq 2s-2$, then $\mathcal{D}$ is schematic.

1.53 A 2-design with degree two is a *quasi-symmetric design.*

1.54 **Lemma** The degree set of a design with $t \geq 2s-1$ is determined by v, k, and the number of blocks.

1.55 **Remark** Schematic subsets in the Hamming scheme may be defined in the same way; the condition $t \geq 2s-2$ is again sufficient for a subset to be schematic and one always has $t \leq 2s$. These claims, and close analogs of the Ray-Chaudhuri and Wilson bounds, hold in any Q-polynomial association scheme as in Theorem 1.56. See [1524] for a more general model.

1.56 **Theorem** (Delsarte) Let $\mathcal{A}$ be a Q-polynomial scheme on X, and let $S \subset X$.

(1) If S is a t-design, then $|S| \geq 1 + f_1 + \cdots + f_{[t/2]}$.
(2) If S is of degree s, then $|S| \leq 1 + f_1 + \cdots f_s$.
(3) If S is a t-design with degree s, then $t \leq 2s$.
(4) If both the hypothesis and equality hold in one of (1), (2), and (3), then t is even and S satisfies the hypotheses and equalities in the other two.

See Also

§II.6	Symmetric designs are equivalent to tight designs with $t = 2$.
§VI.42	Association schemes underlie PBIBDs.
§VI.48	Quasi-symmetric designs are 2-designs of degree 2.
[137]	An introduction to association schemes as occurring in designed experiments in statistics.
[156, 912]	Gives comprehensive treatment of the subject.
[343]	Standard text on distance-regular graphs.
[673]	The most influential work, especially Delsarte's inequalities.
[1033]	Provides a list of all association schemes up to 30+ vertices.
[1173]	Adapts Delsarte's theory to coset geometries.
[2216]	Gives purely group theoretic treatment of general schemes.
[1505, 2154, 2155]	Contains Delsarte's theory and its applications.

References Cited: [137, 155, 156, 343, 414, 673, 912, 1033, 1173, 1505, 1524, 1732, 1783, 1856, 1992, 2018, 2019, 2154, 2155, 2216]

2 Balanced Ternary Designs

Spencer P. Hurd
Dinesh G. Sarvate

2.1 Definitions and Examples

2.1 A *balanced ternary design* $\mathrm{BTD}(V, B; \rho_1, \rho_2, R; K, \Lambda)$, is an arrangement of V elements into B multisets, or *blocks*, each of cardinality K ($K \leq V$), satisfying:

1. Each element appears $R = \rho_1 + 2\rho_2$ times altogether, with multiplicity one in exactly ρ_1 blocks, with multiplicity two in exactly ρ_2 blocks.
2. Every pair of distinct elements appears Λ times; that is, if m_{vb} is the multiplicity of the vth element in the bth block, then for every pair of distinct elements v and w, $\sum_{b=1}^{B} m_{vb}m_{wb} = \Lambda$.

2.2 Example The only two nonisomorphic BTDs with parameter set $(4; 8; 2, 3, 8; 4, 6)$ are given. The columns are blocks.

1 1 1 2 2 3 1 1	1 1 1 2 2 3 1 1
1 1 1 2 2 3 2 2	1 1 1 2 2 3 2 2
2 3 4 3 4 4 3 3	2 3 4 3 4 4 3 3
2 3 4 3 4 4 4 4	2 4 4 4 4 4 3 3

2.3 Remark The incidence matrix of a BTD is defined in the same manner as the incidence matrix of a BIBD: If an element i occurs in the jth block k times, then the (ij)-entry of the incidence matrix is k where $0 \leq k \leq 2$.

2.4 Remarks The term *n-ary* is used to refer to equireplicate designs in which the cells of the incidence matrices are n-valued. The incidence matrix of ternary designs are 3-valued: (0, 1, or 2) and those of binary designs such as BIBDs are 2-valued : (0 or 1). For useful surveys and historical results see [271] and [270].

2.5 Example The $\{0, 1, 2\}$-incidence matrix of a BTD on 10 points with block size 7. This design is the unique BTD with the parameter set $(10, 10; 1, 3, 7; 7, 4)$.

$$\begin{pmatrix}
2 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 \\
1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 \\
0 & 2 & 0 & 0 & 1 & 0 & 2 & 2 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 2 \\
0 & 1 & 0 & 2 & 2 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 2 & 0 & 2 & 0 & 0 & 1 & 0 & 2 \\
0 & 0 & 2 & 0 & 0 & 1 & 2 & 0 & 2 & 0 \\
0 & 0 & 1 & 2 & 0 & 2 & 0 & 2 & 0 & 0
\end{pmatrix}$$

2.6 Remarks

1. The design parameters of a BTD do not determine the number of blocks b_1 that have no doubletons and the number of blocks b_2 that have at least one doubleton, and as a consequence balanced part ternary designs (BPTDs) were introduced [1368] in order to emphasize the block configuration as a useful focus in solving the general existence problem for BTDs.
2. The design in Example 2.5 has a uniform configuration with $b_1 = 0$ whereas the designs in Example 2.2 are nonisomorphic since the first design has $b_1 = 2$ but the second design has $b_1 = 0$.
3. Table 2.11 lists unknown BTDs for small parameters.

2.7 A *balanced part ternary design* $\mathrm{BPTD}(V; b_1, b_2, B; \rho_1, \rho_2, R; K, \Lambda)$ is a BTD that also satisfies:
3. There exist exactly $b_2 = B - b_1$ blocks each containing at least one element of multiplicity two.

2.8 Remarks Every BTD is a BPTD for some choice of b_1 and b_2. BTDs are closely related to other combinatorial structures. There are constructions of BTDs, for example, using Bhaskar Rao designs and weighing designs, but BTDs are also used to construct other designs, see for example, [963]. The incidence matrix of a BTD can be used to form a ternary error-correcting code analogous to the binary codes from BIBDs [1991].

2.9 **Example** The incidence matrix of a BTD$(5, 10; 2, 4, 10; 5, 8)$ appears on the right. If each 2 in the matrix is changed to 1, it becomes the incidence matrix of a BIBD$(5, 3, 3)$ nested in the BTD. If each 1 in the incidence matrix is changed to -1 the result is a *Bhaskar Rao balanced ternary design*.

$$\begin{pmatrix} 2&0&2&0&2&0&2&0&1&1 \\ 2&0&0&2&0&2&1&1&2&0 \\ 0&2&2&0&1&1&0&2&2&0 \\ 0&2&1&1&0&2&2&0&0&2 \\ 1&1&0&2&2&0&0&2&0&2 \end{pmatrix}$$

2.10 **Theorems** The known existence results for block size 3 and 4.

1. The necessary conditions are sufficient for the existence of BTDs with block size 3 with any Λ and any ρ_i; see [270] and references therein.
2. The necessary conditions are sufficient for the existence of BTDs with block size 4 with any Λ and $\rho_2 \leq 6$; see [274] and references therein.

2.2 A BTD/BPTD List of Open Designs

2.11 **Table** The table contains a parameter list for BTD/BPTDs whose existence is unknown. The unknown but possible values of b_2 are given for each $(V; B; \rho_1, \rho_2, R; K, \Lambda)$, based on the lists in [275, 963, 1266] and personal communication from Kaski.

Column 1 shows, in parentheses, the row number of these parameters in [275]. The star $*$ in Column 9 indicates no designs have yet appeared for the parameter values for any choice of b_2.

# ([275])	V	B	ρ_1	ρ_2	R	K	Λ	Open b_2
1(43)	14	18	7	1	9	7	4	14*
3(61)	8	20	8	1	10	4	4	5
5(64)	27	30	8	1	10	9	3	27*
7(73)	10	20	6	2	10	5	4	10,11
9(76)	12	15	6	2	10	8	6	6–15*
11(91)	16	22	9	1	11	8	5	4–16*
13(94)	28	28	9	1	11	11	4	28*
15(103)	7	11	5	3	11	7	10	11
17(106)	10	22	3	4	11	5	4	20,21
19(117)	30	60	10	1	12	6	2	30*
21(119)	48	64	10	1	12	9	2	48*
23(128)	9	27	8	2	12	4	4	9–14,16,17
25(132)	15	30	8	2	12	6	4	10–29
27(135)	24	32	8	2	12	9	4	12–32*
29(137)	17	17	8	2	12	12	8	17*
31(145)	6	18	6	3	12	4	6	10,11
33(148)	7	14	6	3	12	6	9	8
35(150)	14	21	6	3	12	8	6	11–21*
37(159)	5	12	4	4	12	5	10	11
39(161)	20	30	4	4	12	8	4	20–30*
41(163)	9	12	4	4	12	9	11	10
43(171)	18	26	11	1	13	9	6	5–18*
45(179)	8	26	9	2	13	4	5	8–12,15,16
47(182)	22	26	9	2	13	11	6	9–26*
49(189)	7	13	7	3	13	7	12	11
51(192)	16	16	7	3	13	13	10	16*
53(195)	9	13	5	4	13	9	12	10
55(199)	11	13	3	5	13	11	12	12,13
57(209)	18	42	12	1	14	6	4	7–18

# ([275])	V	B	ρ_1	ρ_2	R	K	Λ	Open b_2
2(56)	7	9	3	3	9	7	8	9
4(62)	20	40	8	1	10	5	2	20*
6(65)	45	45	8	1	10	10	2	45*
8(74)	7	14	6	2	10	5	6	7
10(79)	12	20	4	3	10	6	4	12–20*
12(92)	55	55	9	1	11	11	2	55*
14(99)	20	22	7	2	11	10	5	8–22*
16(104)	27	27	5	3	11	11	4	17–27*
18(108)	9	11	3	4	11	9	10	10
20(118)	42	63	10	1	12	8	2	42*
22(121)	27	27	10	1	12	12	5	27*
24(131)	29	58	8	2	12	6	2	58*
26(133)	9	18	8	2	12	6	7	6–11,17
28(136)	33	33	8	2	12	12	4	33*
30(144)	7	21	6	3	12	4	5	11,13
32(147)	10	20	6	3	12	6	6	10–15
34(149)	7	12	6	3	12	7	11	11
36(157)	8	24	4	4	12	4	4	17
38(160)	14	28	4	4	12	6	4	19–27
40(162)	12	16	4	4	12	9	8	12–16*
42(164)	32	32	4	4	12	12	4	22–32*
44(172)	33	39	11	1	13	11	4	7–33*
46(180)	25	65	9	2	13	5	2	50*
48(183)	39	39	9	2	13	13	4	39*
50(190)	31	31	7	3	13	13	5	31*
52(194)	5	13	5	4	13	5	11	11
54(197)	12	26	3	5	13	6	5	20–26*
56(208)	10	28	12	1	14	5	6	5–7,10
58(210)	42	84	12	1	14	7	2	42*

# ([275])	V	B	ρ_1	ρ_2	R	K	Λ	Open b_2	# ([275])	V	B	ρ_1	ρ_2	R	K	Λ	Open b_2
59(214)	37	37	12	1	14	14	5	37*	60(216)	21	21	12	1	14	14	9	21*
61(223)	12	28	10	2	14	6	6	8–24*	62(224)	41	82	10	2	14	7	2	82*
63(225)	21	42	10	2	14	7	4	14–41	64(226)	17	34	10	2	14	7	5	12–23
65(227)	11	22	10	2	14	7	8	8–21	66(228)	9	18	10	2	14	7	10	6–9
67(231)	10	35	8	3	14	4	4	15-24,26-30	68(233)	9	21	8	3	14	6	8	9–15
69(234)	14	28	8	3	14	7	6	14–28*	70(235)	7	14	8	3	14	7	13	11–14
71(236)	24	42	8	3	14	8	4	18–42*	72(237)	25	35	8	3	14	10	5	15–35*
73(238)	45	45	8	3	14	14	4	45*	74(239)	23	23	8	3	14	14	8	23*
75(240)	17	17	8	3	14	14	11	17*	76(243)	5	14	6	4	14	5	12	11
77(244)	20	40	6	4	14	7	4	27–39	78(245)	16	28	6	4	14	8	6	17–28
79(246)	27	42	6	4	14	9	4	27–42*	80(247)	9	14	6	4	14	9	13	10
81(248)	30	30	6	4	14	14	6	30*	82(250)	12	21	4	5	14	8	8	15–21*
83(251)	18	28	4	5	14	9	6	23–28*	84(252)	30	42	4	5	14	10	4	30–42*
85(253)	11	14	4	5	14	11	13	12–14	86(255)	6	21	2	6	14	4	6	18–20
87(256)	4	14	2	6	14	4	10	13	88(262)	20	28	2	6	14	10	6	24–28*
89(266)	18	18	2	6	14	14	10	18*	90(271)	30	90	13	1	15	5	2	30*
91(272)	60	100	13	1	15	9	2	60*	92(273)	20	30	13	1	15	10	7	4–20*
93(281)	15	45	11	2	15	5	4	15–29	94(282)	9	27	11	2	15	5	7	10–12,17,18
95(283)	8	24	11	2	15	5	8	8–11,15	96(285)	30	50	11	2	15	9	4	15–50*
97(286)	24	30	11	2	15	12	7	8–30*	98(296)	10	30	9	3	15	5	6	15-20,28-30
99(297)	7	21	9	3	15	5	9	11,19,20	100(298)	7	15	9	3	15	7	14	11

See Also

§V.4	Bhaskar Rao designs can be constructed from BTDs.
[275]	The original BTD parameter list. Gives the necessary conditions.

References Cited: [270, 271, 274, 275, 963, 1266, 1368, 1991]

3 Balanced Tournament Designs

Esther R. Lamken

3.1 Definitions, Examples, and Existence

3.1 A *balanced tournament design* of order n, BTD(n), defined on a $2n$-set V is an arrangement of the $\binom{2n}{2}$ distinct unordered pairs of the elements of V into an $n \times (2n-1)$ array such that

1. every element of V is contained in precisely one cell of each column, and
2. every element of V is contained in at most two cells of any row.

3.2 A *factored balanced tournament design* of order n, FBTD(n), is a BTD(n) with the property that in each row there exist n cells, a *factor*, which contain all $2n$ elements of V.

3.3 **Remark** The columns of a BTD(n) provide a 1-factorization of the complete graph on $2n$ vertices, K_{2n}.

3.4 **Example** A balanced tournament design of order 3.

1 6	3 5	2 3	4 5	2 4
2 5	4 6	1 4	1 3	3 6
3 4	1 2	5 6	2 6	1 5

3.5 **Example** An FBTD(6). The factors are underlined.

α 8	<u>4 6</u>	6 2	<u>∞ 0</u>	0 3	<u>α 3</u>	<u>9 1</u>	1 7	∞ 5	<u>5 8</u>	<u>2 7</u>
<u>6 9</u>	α 9	<u>5 7</u>	7 3	<u>∞ 1</u>	1 4	<u>α 4</u>	<u>0 2</u>	2 8	∞ 6	<u>3 8</u>
∞ 7	<u>7 0</u>	α 0	<u>6 8</u>	8 4	<u>∞ 2</u>	2 5	<u>α 5</u>	<u>1 3</u>	3 9	<u>4 9</u>
4 0	∞ 8	<u>8 1</u>	α 1	<u>7 9</u>	9 5	<u>∞ 3</u>	3 6	<u>α 6</u>	<u>4 2</u>	<u>5 0</u>
<u>5 3</u>	5 1	∞ 9	<u>9 2</u>	α 2	<u>8 0</u>	0 6	<u>∞ 4</u>	4 7	<u>α 7</u>	<u>6 1</u>
<u>1 2</u>	2 3	<u>3 4</u>	4 5	<u>5 6</u>	6 7	<u>7 8</u>	8 9	<u>9 0</u>	0 1	<u>∞ α</u>

3.6 **Construction** A BTD(n) when $2n \equiv 0, 2 \pmod 3$ (see [1066]). First construct an $n \times 2n-1$ array A using the patterned starter over $\mathbb{Z}_{2n-1}$ (see Construction VI.55.7); column i of A is

$$[\{\infty, i\}, \{1+i, -1+i\}, \{2+i, -2+i\}, \ldots, \{n-1+i, -(n-1)+i\}]^T$$

for $i = 0, 1, \ldots, 2n-2$ where all arithmetic is modulo $(2n-1)$. Construct a BTD(n) from A by interchanging the pairs $\{\infty, i\}$ and $\{3i+1, -i-1\}$ in column i for $i \neq n-1$.

3.7 **Example** For $n = 4$, column i of A is $[\{\infty, i\}, \{1+i, 6+i\}, \{2+i, 5+i\}, \{3+i, 4+i\}]^T$ for $i = 0, 1, \ldots, 6$ (with all arithmetic modulo 7). A BTD(4) is constructed from A by interchanging the pairs $\{\infty, i\}$ and $\{3i+1, -i-1\}$ in column i for $i = 0, 1, 2, 4, 5, 6$:

1 6	4 5	4 0	∞ 3	6 2	1 2	0 5
∞ 0	2 0	3 1	4 2	5 3	6 4	∞ 6
2 5	3 6	∞ 2	5 1	∞ 4	0 3	1 4
3 4	∞ 1	5 6	6 0	0 1	∞ 5	2 3

3.8 **Remark** Balanced tournament designs can be used to schedule round robin tournaments: the rows represent the locations, the columns the rounds of play, and the elements the players or the teams. The properties of the array provide a schedule of play with the following properties:

1. every team plays every other team precisely once during the tournament,
2. each team plays in each round, and
3. no team plays more than twice at any location.

See §VI.51 for more on the scheduling of tournaments.

3.9 **Theorem** There exists a (factored) BTD(n) if and only if n is a positive integer, $n \neq 2$.

3.10 **Remark** BTD(n)s have been enumerated for $1 \leq n \leq 5$. If two BTD(n) have different underlying (column) 1-factorizations they are nonisomorphic. The largest number of nonisomorphic BTD(5) from a single 1-factorization of K_{10} is 103,912 (from 1-factorization #48); the smallest is 293 (from #1). Also, each of the nonisomorphic one-factorizations of K_{10} gives rise to at least one *factored* BTD(5) [711].

3.11 **Table** The number of nonisomorphic BTD(n)s and factored BTD(n)s for $1 \leq n \leq 5$ (see [711] and references therein).

n	BTD(n)	FBTD(n)
1,3	1	1
4	47	29
5	30,220,557	8,081,144

3.2 Partitioned Balanced Tournament Designs

3.12 A *partitioned balanced tournament design*, PBTD(n), is a BTD(n) that also satisfies the properties:

3. each row contains a factor in the first n columns, and
4. each row contains a factor in the last n columns.

3.13 Example A partitioned balanced tournament design of order 5.

α 4	∞ 2	1 3	5 7	0 6	2 3	4 5	∞ 7	α 1
∞ 3	α 5	4 6	0 2	1 7	∞ 4	α 2	0 5	6 3
5 6	0 3	α 7	∞ 1	4 2	6 7	0 1	α 3	∞ 5
1 2	4 7	∞ 0	α 6	5 3	α 0	∞ 6	1 4	7 2
0 7	1 6	2 5	4 3	α ∞	1 5	3 7	2 6	0 4

3.14 Theorem [1387] There exists a PBTD(n) for n a positive integer, $n \geq 5$, except possibly for $n \in \{9, 11, 15\}$.

3.15 Theorem (see [1396]) For n a positive integer, the existence of the following designs are equivalent:

1. a PBTD(n);
2. a maximum empty subarray Room square of side $2n-1$, a MESRS($2n-1$) (§VI.50.7);
3. a pair of almost disjoint $H(n, 2n)$s (Howell designs); and
4. a partitionable house of order n.

3.16 Remark In terms of tournament scheduling, a PBTD(n) represents a tournament where each team plays precisely once at each location in the first n rounds of play and each team plays precisely once at each location in the last n rounds of the tournament.

3.3 Odd and Hamiltonian Balanced Tournament Designs

3.17 An *odd balanced tournament design*, OBTD(n), defined on a $2n+1$-set V is an arrangement of the $\binom{2n+1}{2}$ distinct unordered pairs of the elements of V into an $n \times (2n+1)$ array such that

1. each column of the array contains $2n$ distinct elements of V, and
2. each element of V occurs precisely twice in each row.

3.18 If each row of the OBTD(n) corresponds to a hamiltonian cycle, then the OBTD(n) is a *Kotzig factorization* of order $2n+1$.

3.19 Example A Kotzig factorization of order 7.

1 6	2 7	3 1	4 2	5 3	6 4	7 5
2 5	3 6	4 7	5 1	6 2	7 3	1 4
3 4	4 5	5 6	6 7	7 1	1 2	2 3

3.20 Remark Starters can be used to construct OBTDs. (See §VI.55 and Remark VI.51.9.)

3.21 Theorem For n a positive integer, there exists an OBTD(n).

3.22 Theorem For each positive integer n, there exists a Kotzig factorization of order $2n+1$.

3.23 If each row of a BTD(n) gives a hamiltonian path in K_{2n}, the BTD(n) is a *hamiltonian balanced tournament design*, HBTD(n).

3.24 **Remark** An HBTD is the analogue of a Kotzig factorization.

3.25 **Example** A hamiltonian balanced tournament design of side 4.

1 2	1 3	5 8	3 7	4 7	2 8	4 6
3 4	5 7	1 4	2 6	2 5	3 6	1 8
5 6	2 4	6 7	4 8	3 8	1 7	3 5
7 8	6 8	2 3	1 5	1 6	4 5	2 7

3.26 **Theorem**

1. There exist HBTD(n) for $n = 1, 4, 5$. There do not exist HBTD(n) for $n = 2, 3$.
2. There exist HBTD(n) for all positive integers n not divisible by 2, 3, or 5. [1133]

3.4 Generalized Balanced Tournament Designs

3.27 A *generalized balanced tournament design*, GBTD(n, k), defined on a kn-set V, is an arrangement of the blocks of a BIBD($kn, k, k-1$) defined on V into an $n \times (kn-1)$ array such that

1. every element of V is contained in precisely one cell of each column, and
2. every element of V is contained in at most k cells of each row.

3.28 **Example** A GBTD(3, 3).

1 2 9	3 4 9	5 6 9	1 4 5	3 5 7	1 7 8	2 3 8	2 6 7
3 5 7	1 6 7	1 3 8	2 3 6	4 6 8	2 4 5	7 4 9	5 8 9
4 6 8	2 5 8	2 4 7	7 8 9	1 2 9	3 6 9	1 6 5	1 3 4

3.29 **Theorem** [1388] For all positive integers n, $n \neq 2$, there exists a GBTD($n, 3$). There does not exist a GBTD($2, 3$).

3.30 **Remarks**

1. A GBTD($n, 2$) is a BTD(n).
2. Factored GBTDs, partitioned GBTDs, and near GBTDs are the generalizations of FBTDs, PBTDs, and OBTDs, respectively, to larger block size k [1384, 1388].
3. Existence results have been established for factored GBTDs and partitioned GBTDs with block size 3, see [1388].
4. GBTDs are also equivalent to other combinatorial designs [1384].

3.31 **Remark** Generalized balanced tournament designs can be used to construct several other types of combinatorial designs including resolvable, near-resolvable, doubly resolvable, and doubly near-resolvable balanced incomplete block designs [1384, 1386, 1388].

See Also

§II.7	GBTDs and near GBTDs are RBIBDs and near RBIBDs.
§VI.24	Kotzig factorizations and HBTDs are graph decompositions.
§VI.29	A PBTD(n) can also be defined in terms of Howell designs.
§VI.50	A PBTD(n) is equivalent to a MESRS($2n-1$).
§VI.55	Starters can be used to construct BTDs and OBTDs.
§VI.51	Scheduling tournaments.
[1396]	A survey of balanced tournament designs.
[1384, 1388]	Further information and references on GBTDs.
[815]	Applications of tournament designs to scheduling softball leagues.

References Cited: [711, 815, 1066, 1133, 1384, 1386, 1387, 1388, 1396]

4 Bent Functions

Douglas R. Stinson

4.1 Boolean Functions and Fourier Transforms

4.1 A function $f : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ is a *boolean function* of n variables. Let $\mathcal{B}_n$ be the set of all boolean functions of n variables. For $f \in \mathcal{B}_n$, list the values $f(\mathbf{x})$, for all $\mathbf{x} \in (\mathbb{Z}_2)^n$, in a vector of length 2^n. Denote this vector by $\phi(f)$, where $\phi(f)_{\mathbf{x}} = f(\mathbf{x})$ for all $\mathbf{x} \in (\mathbb{Z}_2)^n$. Index the coordinates of $\phi(f)$ in lexicographic order.

4.2 **Theorem** $|\mathcal{B}_n| = 2^{2^n}$ (there are 2^{2^n} boolean functions of n variables).

4.3 For any $f \in \mathcal{B}_n$, define $(-1)^f$ to be the function $g : (\mathbb{Z}_2)^n \to \{-1, 1\}$ such that $g(\mathbf{x}) = (-1)^{f(\mathbf{x})}$ for all $\mathbf{x} \in (\mathbb{Z}_2)^n$.

4.4 The *inner product* of two vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n) \in (\mathbb{Z}_2)^n$ is
$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i \pmod 2.$$

4.5 Let F be any real-valued function defined on $(\mathbb{Z}_2)^n$. The *Fourier transform* of F is the function $\widehat{F} : (\mathbb{Z}_2)^n \to \mathbb{R}$ defined by the following formula. For all $\mathbf{x} \in (\mathbb{Z}_2)^n$,
$$\widehat{F}(\mathbf{x}) = \sum_{\mathbf{y} \in (\mathbb{Z}_2)^n} (-1)^{\mathbf{x} \cdot \mathbf{y}} F(\mathbf{y}).$$

4.6 Let $S_n = (s_{\mathbf{x},\mathbf{y}})$ be the $2^n \times 2^n$ matrix in which the rows and columns are indexed by $(\mathbb{Z}_2)^n$ (in lexicographic order) and $s_{\mathbf{x},\mathbf{y}} = (-1)^{\mathbf{x} \cdot \mathbf{y}}$ for all $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}_2)^n$.

4.7 **Lemma** S_n is a Hadamard matrix.

4.8 For any function $F : \{0, 1\}^n \to \mathbb{R}$, define $\phi(F)$ in the same way that $\phi(f)$ was defined from f, so that $\phi(F)$ is the vector of values $F(\mathbf{x})$.

4.9 **Lemma** Suppose that $F : \{0, 1\}^n \to \mathbb{R}$. Then $\phi(\widehat{F}) = \phi(F) S_n$.

4.10 **Corollary** Suppose that $F : \{0, 1\}^n \to \mathbb{R}$. Then $\widehat{\widehat{F}} = 2^n F$.

4.11 **Theorem** Suppose that $f \in \mathcal{B}_n$ and $F = (-1)^f$. Let $\mathbf{y} \in (\mathbb{Z}_2)^n$. Then it holds that
$$\sum_{\mathbf{x} \in (\mathbb{Z}_2)^n} \widehat{F}(\mathbf{x}) \widehat{F}(\mathbf{x} + \mathbf{y}) = \begin{cases} 2^{2n} & \text{if } \mathbf{y} = (0, \ldots, 0) \\ 0 & \text{if } \mathbf{y} \neq (0, \ldots, 0). \end{cases}$$

4.12 **Corollary** (Parseval's Equation) Suppose that $f \in \mathcal{B}_n$ and $F = (-1)^f$. Then
$$\sum_{\mathbf{x} \in (\mathbb{Z}_2)^n} (\widehat{F}(\mathbf{x}))^2 = 2^{2n}.$$

4.13 **Theorem** Suppose that $F : (\mathbb{Z}_2)^n \to \mathbb{R}$ and let $\mathbf{y} \in (\mathbb{Z}_2)^n$. Then it holds that
$$\sum_{\mathbf{x} \in (\mathbb{Z}_2)^n} \widehat{F}(\mathbf{x}) \widehat{F}(\mathbf{x} + \mathbf{y}) = 2^n \sum_{\mathbf{u} \in (\mathbb{Z}_2)^n} (-1)^{\mathbf{y} \cdot \mathbf{u}} (F(\mathbf{u}))^2.$$

4.2 Linear, Affine, and Bent Functions

4.14 Suppose that $f, g \in \mathcal{B}_n$. The *distance* between f and g is the quantity

$$\mathsf{d}(f,g) = |\{\mathbf{x} \in (\mathbb{Z}_2)^n : f(\mathbf{x}) \neq g(\mathbf{x})\}|.$$

Equivalently, $\mathsf{d}(f,g)$ is the Hamming distance between the vectors $\phi(f)$ and $\phi(g)$.

4.15 A function $f \in \mathcal{B}_n$ is a *linear function* if f has the form $f(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x}$, where $\mathbf{a} \in (\mathbb{Z}_2)^n$. For brevity, denote the function $\mathbf{a}\cdot\mathbf{x}$ by $L_{\mathbf{a}}$. Then $L_{\mathbf{a}} + 1$ is the function taking on the value $L_{\mathbf{a}}(\mathbf{x}) + 1 \bmod 2$ for all $\mathbf{x}$. A function $f \in \mathcal{B}_n$ is an *affine function* if $f = L_{\mathbf{a}}$ or $f = L_{\mathbf{a}} + 1$ for some $\mathbf{a} \in (\mathbb{Z}_2)^n$. Define $\mathcal{A}_n$ to be the set of all affine functions on n boolean variables.

4.16 Theorem Suppose that $f \in \mathcal{B}_n$ and $F = (-1)^f$. Let $\mathbf{a} \in (\mathbb{Z}_2)^n$. Then

$$\mathsf{d}(f, L_{\mathbf{a}}) = 2^{n-1} - \frac{1}{2}\widehat{F}(\mathbf{a}) \quad \text{and} \quad \mathsf{d}(f, L_{\mathbf{a}}+1) = 2^{n-1} + \frac{1}{2}\widehat{F}(\mathbf{a}).$$

4.17 The *nonlinearity* of f, denoted N_f, is the quantity $N_f = \min\{\mathsf{d}(f,g) : g \in \mathcal{A}_n\}$.

4.18 Theorem Let $F = (-1)^f$. Then $N_f = 2^{n-1} - \frac{1}{2}\max\{|\widehat{F}(\mathbf{a})| : \mathbf{a} \in (\mathbb{Z}_2)^n\}$.

4.19 A function $f \in \mathcal{B}_n$ is a *bent function* if $|\widehat{F}(\mathbf{x})| = 2^{n/2}$ for all $\mathbf{x} \in (\mathbb{Z}_2)^n$, where $F = (-1)^f$.

4.20 Theorem A bent function can exist in $\mathcal{B}_n$ only when n is even.

4.21 Example Suppose that n is even, then following is a bent function:

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n \bmod 2.$$

4.22 Theorem For any $f \in \mathcal{B}_n$, it holds that $N_f \leq 2^{n-1} - 2^{n/2-1}$. Furthermore, equality holds if and only if f is a bent function.

4.23 Remark Theorem 4.22 shows that bent functions are the functions having maximum possible nonlinearity.

4.24 Corollary For even n, the covering radius of the Reed–Muller code $\mathrm{RM}(1,n)$ is equal to $2^{n-1} - 2^{n/2-1}$.

4.25 Theorem Suppose that $f \in \mathcal{B}_n$ and $F = (-1)^f$. Define the matrix $H_f = (h_{\mathbf{x},\mathbf{y}})$, where $h_{\mathbf{x},\mathbf{y}} = F(\mathbf{x}+\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}_2)^n$. Then f is a bent function if and only if H_f is a Hadamard matrix.

4.26 Theorem [704] There exists a bent function $f : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ if and only if there exists a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$-difference set in $(\mathbb{Z}_2)^n$.

4.27 Remark Suppose that $f \in \mathcal{B}_n$ is a bent function. Let $i = 0$ or 1 and

$$D_i = \{\mathbf{x} \in (\mathbb{Z}_2)^n : f(\mathbf{x}) = i\}.$$

Then D_i is a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$-difference set in $(\mathbb{Z}_2)^n$. Conversely, suppose that $D \subseteq (\mathbb{Z}_2)^n$ is a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$-difference set. Define $f \in \mathcal{B}_n$ by $f(\mathbf{x}) = 0$ if and only if $\mathbf{x} \in D$. Then f is a bent function.

4.28 Example Suppose that $n = 4$ and $f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4 \pmod 2$. Then $\phi(f) = (0,0,0,1,0,0,0,1,0,0,0,1,1,1,1,0)$. Further, $D = \{\mathbf{x} : f(\mathbf{x}) = 1\} = \{(0,0,1,1)$ $(0,1,1,1)$, $(1,0,1,1)$, $(1,1,0,0)$, $(1,1,0,1)$, $(1,1,1,0)\}$ is a $(16,6,2)$-difference set in the group $((\mathbb{Z}_2)^4, +)$.

4.29 Remark Bent functions were used in the design of S-boxes in the block cipher CAST. [54].

4.3 Generalized Bent Functions

4.30 Suppose $F : (\mathbb{Z}_q)^n \to \mathbb{C}$ and let $\omega = e^{2i\pi/q}$. The *Fourier transform* of F is the function $\widehat{F} : (\mathbb{Z}_q)^n \to \mathbb{C}$ defined for all $\mathbf{x} \in (\mathbb{Z}_q)^n$ by the formula:

$$\widehat{F}(\mathbf{x}) = \sum_{\mathbf{y} \in (\mathbb{Z}_q)^n} \omega^{\mathbf{x}\cdot\mathbf{y}} F(\mathbf{y}).$$

4.31 Suppose $f : (\mathbb{Z}_q)^n \to \mathbb{Z}_q$ and define $F : (\mathbb{Z}_q)^n \to \mathbb{C}$ by the rule $F(\mathbf{x}) = \omega^{f(\mathbf{x})}$ for all $\mathbf{x} \in (\mathbb{Z}_q)^n$,where $\omega = e^{2i\pi/q}$. Then f is a *generalized bent function* if $|\widehat{F}(\mathbf{x})| = q^{n/2}$ for all $\mathbf{x} \in (\mathbb{Z}_q)^n$.

4.32 Theorem Suppose f and F are defined as above. Define the matrix $H_f = (h_{\mathbf{x},\mathbf{y}})$, where $h_{\mathbf{x},\mathbf{y}} = F(\mathbf{x} - \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}_q)^n$. Then f is a generalized bent function if and only if $H_f {H_f}^* = nI$, where ${H_f}^*$ is the adjoint matrix of H_f.

4.33 Remark When q is prime, an n by n matrix of complex qth roots of unity which satisfies $H_f {H_f}^* = nI$ is equivalent to a generalized Hadamard matrix $\mathrm{GH}(n, 1)$ with entries from $\mathbb{Z}_q$.

4.34 Theorem Suppose that n is even or $q \not\equiv 2 \bmod 4$. Then there exists a generalized bent function $f : (\mathbb{Z}_q)^n \to \mathbb{Z}_q$.

See Also

§V.1	Hadamard matrices and designs.
§VII.1	Codes and orthogonal arrays.
[1829]	The paper that introduced bent functions.
[704]	Dillon's Ph.D. thesis, where Theorem 4.26 was first proved.
[436]	Recent results on bent functions.
[1366]	Results on generalized bent functions.

References Cited: [54, 436, 704, 1366, 1829]

5 Block-Transitive Designs

Anne Delandtsheer

5.1 Point-, Block-, and Flag-transitivity

5.1 Remark In this chapter, all t-(v, k, λ) designs $\mathcal{D} = (X, \mathcal{B})$ are assumed to be simple and nontrivial with $1 < t < k < v$, and q always denotes a prime power.

5.2 Theorem [2075] Let t be a natural number and G a finite (abstract) group. Then there is a t-design $\mathcal{D}$ such that Aut $\mathcal{D}$ has a subgroup isomorphic to G.

5.3 Theorem (Block's Lemma) [283] Let G be any automorphism group of a t-(v, k, λ) design having exactly m orbits on the v points and n orbits on the b blocks. Then $m \leq n \leq m + b - v$. These inequalities also hold for PBDs. Moreover, the first inequality is best possible for PBDs with $\lambda = 1$ [285].

5.4 Corollary Any block-transitive automorphism group of a t-design is point-transitive. This is also a consequence of Theorem 5.8.

5.5 A *flag* of a design is an incident (point, block) pair.

5.6 A subgroup G of the automorphism group Aut $\mathcal{D}$ of a t-design $\mathcal{D} = (X, \mathcal{B})$ is *flag-transitive* if G acts transitively on the set of flags of $\mathcal{D}$. The pair $(\mathcal{D}, G)$ as well as the design $\mathcal{D}$ are *flag-transitive*. *Block-transitivity, point-transitivity,* and *point-primitivity* are defined similarly.

5.7 **Remark** For $1 \leq s < t$, any block (resp. flag)-transitive $t-(v,k,\lambda)$ design is also a block (resp. flag)-transitive $s-(v,k,\lambda')$ design, with $\lambda' > \lambda$.
The complementary design $\mathcal{D}^c$ of a block-transitive t-design $\mathcal{D}$ is also a block-transitive t-design if $k+t \leq v$, but $\mathcal{D}^c$ is not necessarily flag-transitive if $\mathcal{D}$ is.

5.8 **Theorem** (Cameron–Praeger, Camina) [423, 427]
1. If $(\mathcal{D}, G)$ is block-transitive, then $t \leq 7$ and G is $\lfloor t/2 \rfloor$-homogeneous on X.
2. If $(\mathcal{D}, G)$ is flag-transitive, then $t \leq 6$ and G is $\lfloor (t+1)/2 \rfloor$-homogeneous on X.
3. If $(\mathcal{D}, G)$ is flag-transitive, $t = 2$ and $gcd(r, \lambda) = 1$, then G is primitive on X.

5.9 **Conjecture** [423] There is no nontrivial block-transitive 6-design.

5.10 **Theorem** [1147] There is no nontrivial flag-transitive $6-(v,k,1)$ design. The only nontrivial flag-transitive pairs $(\mathcal{D}, G)$ with $t \geq 4$ and $\lambda = 1$ are the Witt 4-(11,5,1), 5-(12,6,1), 4-(23,7,1), and 5-(24,8,1) designs with $G = \mathcal{M}_v$ (or $v = 24$ and $G = PSL(2,23)$).

5.2 2-homogeneity on Blocks

5.11 **Theorem** [427] If $\mathcal{D}$ is a t-design with an automorphism group G that is 2-homogeneous on $\mathcal{B}$, then $\mathcal{D}$ is symmetric, G is 2-homogeneous on X, and $\mathcal{D}$ or $\mathcal{D}^c$ is one of the following:

Case	Parameters	Name or Reference
1.	$2\text{-}(q, (q-1)/2, (q-3)/4), q \equiv 3 \pmod 4$	Paley design
2.	$2-\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)(d \geq 2)$	$\mathrm{PG}_{d-1}(d,q)$
3.	$2\text{-}(11,5,2)$	biplane on 11 points
4.	$2\text{-}(176,50,14)$	Higman design (See II.6.8)
5.	$2\text{-}(2^{2m}, 2^{m-1}(2^m-1), 2^{m-1}(2^{m-1}-1))$	Kantor (See II.6.8)

5.12 **Remark** The 2-transitive symmetric designs are given in Theorem II.6.20.

5.3 Flag-transitive Steiner 3-designs

5.13 **Theorem** [1148] The 3-$(v,k,1)$ designs $\mathcal{D}$ with a flag-transitive automorphism group G are necessarily 2-transitive on points. They are listed here, where $\mathcal{D}_x$ denotes any point-residue of $\mathcal{D}$ and $AG_2(d,2)$ is the design of points and planes of the d-dimensional affine space over $\mathbb{F}_2$.

Case	v	k	$\mathcal{D}$ or $\mathcal{D}_x$	G
1.a	$2^d (d \geq 3)$	4	$\mathcal{D} = AG_2(d,2)$	$AGL(d,2)$
1.b	8	4	$\mathcal{D} = AG_2(3,2)$	$AGL(1,8)$ or $A\Gamma L(1,8)$
1.c	16	4	$\mathcal{D} = AG_2(4,2)$	$G_0 \cong \mathcal{A}_7$
1.d	32	4	$\mathcal{D} = AG_2(5,2)$	$A\Gamma L(1,32)$
2.	q^e+1 $(q \geq 3, e \geq 2)$	$q+1$	$\mathcal{D}_x = AG_1(e,q)$	$PSL(2,q^e) \leq G \leq P\Gamma L(2,q^e)$
3.	$q+1$ $(q \equiv 7 (\mathrm{mod}\ 12))$	4	$\mathcal{D}_x = N(3,q)$	$PSL(2,q) \leq G \leq P\Sigma L(2,q)$
4.	22	6	$\mathcal{D}_x = PG_1(2,4)$	$\mathcal{M}_{22} \trianglelefteq G$

In Case 2, $\mathcal{D}$ is the *inversive space* with $X = \mathbb{F}_{q^e} \cup \{\infty\}$ and $\mathcal{B}$ is the orbit of $\mathbb{F}_q \cup \{\infty\}$ under G. In Case 3, $X = \mathbb{F}_q \cup \{\infty\}$, $\mathcal{B}$ is the orbit of $\{0, 1, \epsilon, \infty\}$ under G, where ϵ is a primitive sixth root of unity in $\mathbb{F}_q$, and $\mathcal{D}_x$ is the Netto triple system defined in Construction 5.16.

5.4 Flag-transitive Steiner 2-designs

5.14 Remark The Steiner 2-designs (or 2-$(v, k, 1)$ designs) are linear spaces and their blocks are lines. See §IV.6 and §VI.31.

5.15 An automorphism group G of a t-design $\mathcal{D} = (X, \mathcal{B})$ is *affine* if $(\mathbb{Z}_p)^d \trianglelefteq G \leq AGL(d, p)$, where $(\mathbb{Z}_p)^d$ is point-regular, so that $|X| = p^d$ for some prime p. G is *1-dimensional affine* if G is a subgroup of $A\Gamma L(1, p^d)$.

5.16 Construction There are many examples of linear spaces $\mathcal{D}$ with a flag-transitive 1-dimensional affine group, but they have not been classified. If k divides v, then the lines of $\mathcal{D}$ are subspaces of $AG(d, p)$ and the lines through 0 induce a spread in the projective space $PG(d-1, p)$ at infinity of ${\mathbb{F}_p}^d$. Examples are given in [1259, 1658] such as 2-$(q^n, \sqrt{q}, 1)$ designs with a flag-transitive automorphism group $AG^mL(1, q^n)$ where $gcd(m, (q^n - 1)/(q - 1)) = 1$.

If k does not divide v, then k and v are coprime [667]. If $X = \mathbb{F}_q$ and if $\mathcal{B}$ is the orbit of the set of kth roots of unity in $\mathbb{F}_q$ under the group $AG^{k-1}L(1, q)$,then $(X, \mathcal{B})$ is a flag-transitive linear space if and only if, for any primitive kth root of unity ϵ in $\mathbb{F}_q$, the elements $\epsilon - 1, \epsilon^2 - 1, \cdots, \epsilon^{k-1} - 1$ are in distinct cosets of the multiplicative group consisting of all $(k-1)$th powers of nonzero elements of $\mathbb{F}_q$. For $k = 3$ and $q \equiv 7 \pmod{12}$, one gets the *Netto triple systems* $N(3, q)$, which can also be defined by taking for $\mathcal{B}$ the orbit of $\{0, 1, \epsilon\}$ under $AG^2L(1, q)$ where ϵ is a primitive sixth root of unity. For $k = 5$, the only feasible values of $q \leq 800$ are $61, 421, 661, 701$. For $(k, q) = (3, 7)$ and $(9, 73)$, one gets $PG(2, 2)$ and $PG(2, 8)$, respectively.

5.17 Theorem [373, 1449, 1845] If $\mathcal{D} = (X, \mathcal{B})$ is a 2-$(v, k, 1)$ design with a flag-transitive automorphism group G, then G is primitive on X and either G is 1-dimensional affine or $\mathcal{D}$ and G are as in the table, where soc $G = T$ means that $T \trianglelefteq G \leq$ Aut T and G_0 is the stabilizer of a point if G is affine. In each case (except Case 5), for each parameter k, $\mathcal{D}$ is unique, while Aut $\mathcal{D}$ has usually several flag-transitive subgroups. A complete description of the designs is given in [372]. $U_H(q)$ (resp. $U_R(q)$) is the hermitian (resp. Ree) unital. $W(2^n)$ is the Witt–Bose–Shrikhande design. $H_1(9)$ and $H_2(9)$ are Hering's designs. The groups in Case 6 are given in [1449]: G is affine, 2-transitive on X and nonsolvable (except for $(d, q) = (4, 3)$ or $(2, q)$ where $q = 3, 5, 7, 9, 11, 19, 23, 29,$ and 59).

Case	v	k	$\mathcal{D}$	G, soc G or G_0
1.a	$\frac{q^{d+1}-1}{q-1}$	$q+1$	$PG_1(d, q)$	soc $G = PSL(d+1, q)$
1.b	15	3	$PG_1(3, 2)$	$\mathcal{A}_7$
2	$q^3 + 1$	$q+1$	$U_H(q)$	soc $G = PSU(3, q)$
3	$q^3 + 1$	$q+1$ $(q = 3^{2e+1} > 3)$	$U_R(q)$	soc $G = {}^2G_2(q)$
4	$2^{n-1}(2^n - 1)$	$2^{n-1}(n \geq 3)$	$W(2^n)$	soc $G = PSL(2, 2^n)$
5	9^3	9	$H_1(9)$ or $H_2(9)$	$G = 3^6 \cdot SL(2, 13)$
6	q^d	q	$AG_1(d, q)$	G 2-tra (+ exceptions)
7.a	q^4	$q^2(q = 2^{2e+1} > 2)$	Lü (q^2)	$Sz(q) \trianglelefteq G_0 \leq$ Aut $Sz(q)$
7.b	27^2	27	A_{27}	$G_0 \cong SL(2, 13)$
7.c	9^2	9	A_9	Aut $A_9 \cong 3^4 \cdot \mathcal{S}_5 \cdot 2^4 \cdot 2$

In Case 7, $\mathcal{D}$ is an affine translation plane: Lü (q^2) is the Lüneburg–Tits plane related to the Suzuki group $Sz(q)$, A_{27} is Hering's plane and A_9 the nearfield plane of order 9. Except for $W(2^n)$ and Lü (q^2), Aut $\mathcal{D}$ is 2-transitive on X. In all cases $gcd(k, v) = 1$ or k.

The pairs $(\mathcal{D}, G)$ with G 2-transitive on X (including the 1-dimensional affine case) are classified in [1257].

5.18 **Theorem** [670] If $\mathcal{D} = (X, \mathcal{B})$ is a 2-$(v, k, 1)$ design with an automorphism group G that is 2-homogeneous but not 2-transitive on X, then $G \leq A\Gamma^2 L(1, p^d)$ is 1-dimensional affine with $p \equiv 3 \pmod 4$, d is odd and $\mathcal{D} = N(3, q)$ as in Construction 5.16 or $\mathcal{D} = AG_1\left(\frac{d}{m}, p^m\right)$ with $m|d$.

5.5 Block-transitive Steiner 2-designs

5.19 Since $gcd(v, r) = 1$ in any 2-$(v, k, 1)$ design, it is natural to define $k^{(v)} = gcd(k, v), k^{(r)} = gcd(k, r), b^{(v)} = gcd(b, v), b^{(r)} = gcd(b, r)$, so that $k = k^{(v)}k^{(r)}, b = b^{(v)}b^{(r)}, v = b^{(v)}k^{(v)}$, and $r = b^{(r)}k^{(r)}$.

5.20 **Theorem** [806] If G is block-transitive on a 2-$(v, k, 1)$ design, then G has at most $k^{(r)}$ orbits on flags. In particular if G is block-transitive and $k|v$, then G is flag-transitive.

5.21 **Theorem** [430, 431, 1475, 429, 1476] If G is block-transitive on a 2-$(v, k, 1)$ design $\mathcal{D}$, then one of the following holds:

1. G has a simple nonabelian point-transitive subgroup T and $T \trianglelefteq G \leq$ Aut T,
2. G is point-primitive and affine, or
3. G has a nontrivial normal subgroup K that is point-intransitive and acts faithfully on each of its point-orbits (regularly if K is abelian).

In Case 1, T cannot be a sporadic simple group nor a Suzuki group $Sz(q)$; if T is an alternating group $\mathcal{A}_n (n \geq 5)$, then $n = 7$ or 8 and $\mathcal{D} = PG_1(3, 2)$; if $G = {}^2G_2(q)$ with $q > 3$, then $\mathcal{D} = U_R(q)$. If T is a group of Lie type of characteristic p dividing $b^{(r)}$, then G is flag-transitive and $\mathcal{D}$ is a unital [907].

5.22 **Remark** If $\mathcal{D}$ is a finite projective plane, any point-transitive automorphism group is block-transitive and conversely. Also, any point-primitive automorphism group of $\mathcal{D}$ is line-primitive and conversely [1258].

5.23 **Theorem** [428] If G is a line-transitive automorphism group of a projective plane of order n and if M is a minimal normal subgroup of G, then M is simple, or M is abelian, or $n \in \{3, 9, 16, 25\}$. Moreover, there is a function $f(n)$ such that if G is a classical simple group of rank d over $\mathbb{F}_q$, then $d < f(n)$.

5.24 **Theorem** [1112] If a finite projective plane $\mathcal{D}$ has more than one cyclic transitive automorphism group, then $\mathcal{D}$ is desarguesian.

5.6 Point-imprimitive Flag-transitive 2-designs

5.25 **Remark** By Theorem 5.8, any flag-transitive t-(v, k, λ) design is point-primitive as soon as $t \geq 3$, or $t = 2$ and $gcd(r, \lambda) = 1$. In any case, most flag-transitive 2-designs are point-primitive according to Theorem 5.26.

5.26 **Theorem** [422, 632] For any given λ (resp. for any given k), there are only finitely many 2-(v, k, λ) designs with a flag-transitive point-imprimitive automorphism group.

5.27 Theorem [422] In any flag-transitive point-imprimitive 2-(v, k, λ) design, $v \leq (k-2)^2$. This bound is attained for every even $k > 4$ by some Cameron–Praeger 2-design (see Construction 5.35).

5.28 Theorem [1758] If $(X, \mathcal{B})$ is a symmetric 2-(v, k, λ) design with a flag-transitive point-imprimitive automorphism group preserving a nontrivial partition of X into d classes of size c (so that $v = cd$), then $\lambda \geq 2$ and there is a constant l such that any block intersects any class in 0 or l points, and either $k \leq \lambda(\lambda-3)/2$ or one of

Case	k	c	d	l	λ
1.a	$\lambda(\lambda+1)$	λ^2	$\lambda+2$	λ	
1.b	$\lambda(\lambda+1)$	$\lambda+2$	λ^2	2	
2.a	$\lambda^2/2$	$(\lambda+2)/2$	$(\lambda^2-2\lambda+2)/2$	2	$\lambda \equiv 0 \pmod 4$
2.b	$\lambda^2/2$	$(\lambda+2)/2$	$(\lambda^2-2\lambda+2)/2$	2	$\lambda = 2u^2$, $3 \leq u$ is odd and $2(u^2-1)$ is a square
3.	$\lambda(\lambda+5)/2$	$\lambda+6$	$(\lambda^2+4\lambda-1)/4$	3	$\lambda \equiv 1$ or $3 \pmod 6$

If $\lambda \leq 10$, then v, k, c, d, l, λ are explicitly listed in [1758]. This table lists all possibilities for $\lambda \leq 4$:

No.	v	k	λ	c	d	l	total number of designs
1.	16	6	2	4	4	2	2
2.	45	12	3	9	5	3	1
3.	15	8	4	3	5	2	1
4.	96	20	4	16	6	4	≥ 4
5.	96	20	4	6	16	2	≥ 3

5.29 Remark The designs of Case 5 of Theorem 5.11 also have a flag-transitive but point-imprimitive automorphism group.

5.7 Point-imprimitive Block-transitive t-designs

5.30 Remark By Theorem 5.8, any block-transitive automorphism group of a t-design with $t \geq 4$ is 2-homogeneous on X, hence, point-primitive.

5.31 Theorem [669] In a 2-(v, k, λ) design $(X, \mathcal{B})$ with a block-transitive group preserving a nontrivial partition $\mathcal{P}$ of X into d classes of size c, let x be the number of pairs $\{p, p'\}$ of points in a given block such that p and p' are in the same class. Then $x = \binom{k}{2}(c-1)/(cd-1)$ and there is an integer $y = \binom{k}{2}(d-1)/(cd-1)$, so that $c = \left(\binom{k}{2} - x\right)/y$ and $d = \left(\binom{k}{2} - y\right)/x$.

5.32 Corollary Since $x, y \geq 1$ and $v = cd$, any block-transitive point-imprimitive 2-(v, k, λ) design satisfies $v \leq (k^2-k-2)^2/4 = \left(\binom{k}{2} - 1\right)^2$.

5.33 Theorem [1519] If $\mathcal{D}$ is a block-transitive point-imprimitive 3-(v, k, λ) design, then

1. $\lambda \geq 2$ and $v \leq (k^2-k+2)/2$
2. If $\lambda = 2$, $\mathcal{D}$ is symmetric and $v = (k^2-k+2)/2 = b$

5.34 Corollary Any block-transitive 3-$(v, k, 1)$ design is point-primitive.

5.35 Construction [422] Let $\mathcal{P}$ be a nontrivial partition of X into d classes $\Delta_1, \cdots, \Delta_d$ of size c. Let $\overline{x} = (x_1, \cdots, x_d)$ be a d-tuple such that $c \geq x_i \geq x_j \geq 0$ for any $i < j$ and $\sum_{i=1}^{d} x_i = k$. The *Cameron–Praeger design* $CP(c, d, \overline{x})$ is $(X, \tilde{\mathcal{B}})$, where $\tilde{\mathcal{B}}$ is the set of k-subsets B of X such that $(|B \cap \Delta_1|, \cdots, |B \cap \Delta_d|)$ is any rearrangement of

$\overline{x}$. This 1-design admits the wreath product $\tilde{G} = S_c \wr S_d$ as a block-transitive point-imprimitive group, it is a 2-design if and only if $\sum_{i=1}^{d} \binom{x_i}{2} = \binom{k}{2}\frac{c-1}{cd-1}$ and a 3-design if and only if $\sum_{i=1}^{d} \binom{x_i}{3} = \binom{k}{3}\frac{(c-1)(c-2)}{(cd-1)(cd-2)}$. If a block-transitive automorphism group G of a t-(v,k,λ) design $\mathcal{D} = (X, \mathcal{B})$ preserves the partition $\mathcal{P}$, then $G \le \tilde{G}$ and the orbit under $\tilde{G}$ of any block $B \in \mathcal{B}$ is precisely $\tilde{\mathcal{B}}$, so that $(X, \tilde{\mathcal{B}})$ is a t-$(v,k,\tilde{\lambda})$ design with $\tilde{\lambda} \ge \lambda$.

5.36 **Example** [2076] There are infinitely many infinite families of Cameron–Praeger 3-designs attaining the bound $v = (k^2 - k + 2)/2$ of Theorem 5.33.

5.37 **Examples** Block-transitive point-imprimitive 2-designs $\mathcal{D}$ with an automorphism group $\mathcal{S}_c \times \mathcal{S}_d$ are constructed in [422] from a complete bipartite graph. In order to reach the bound $v = \left(\binom{k}{2} - 1\right)^2$ of Corollary 5.32, take two disjoint sets of size $c = \binom{k}{2} - 1$, let $\mathcal{G}$ be the complete bipartite graph with those two sets as cocliques and let $G = \mathcal{S}_c \times \mathcal{S}_c$ act as an automorphism group of $\mathcal{G}$. Let X consist of the c^2 edges of $\mathcal{G}$ and let B_1 be a subgraph consisting of $k-3$ isolated edges and 3 edges forming a path. If $\mathcal{B}$ is the G-orbit of B_1, then $(X, \mathcal{B})$ is a 2-design attaining the bound. Other designs of this type are obtained by replacing B_1 by a subgraph B_2 consisting of $k-4$ isolated edges and two pairs of edges forming a path of length 2.

5.38 **Theorem** [422] For every $k \ge 6$ (with $k \ne 8$) such that the only 2-transitive groups of degree $c = \binom{k}{2} - 1$ are $\mathcal{S}_c$ and $\mathcal{A}_c$, there are just 3 nonisomorphic 2-(c^2, k, λ) designs having a block-transitive point-imprimitive group, namely, the unique Cameron–Praeger 2-design with these parameters and the two designs in Example 5.37.

5.8 Point-imprimitive Block-transitive Steiner 2-designs

5.39 **Examples** If an automorphism group G of a finite projective plane $\mathcal{D}$ is transitive but imprimitive on points, then $(\mathcal{D}, G)$ is a line-transitive point-imprimitive pair. This happens for any desarguesian plane $\mathcal{D}$ of order n such that $v = n^2 + n + 1$ is not a prime and G is generated by a Singer cycle.

5.40 **Examples** [1757] The only known 2-$(v,k,1)$ designs that are not projective planes and have a line-transitive group G preserving a nontrivial partition $\mathcal{P}$ of X into d classes of size c are listed here, together with the number of nonisomorphic designs. In all cases G has a normal subgroup whose point-orbits are the classes of $\mathcal{P}$.

v	c	d	k	x	y	discovered by	number
91	13	7	6	2	1	Colbourn [533]	1
91	7	13	6	1	2	Colbourn [533] and Mills [1607]	2
729	27	27	8	1	1	NNOPP [1676]	467

5.41 **Theorem** [671, 1676] Table 5.40 contains all block-transitive point-imprimitive 2-$(v,k,1)$ designs with $x = 1$ and $y \le 2$, and in particular those attaining the bound of Corollary 5.32 (that is, $x = y = 1$).

5.42 **Theorem** [234, 806] Given an integer n, there are only finitely many block-transitive point-imprimitive 2-$(v,k,1)$ designs with $gcd(k,r) \le n$. For $n = 8$, the only examples are those in Table 5.40 and the projective planes $PG(2,4)$ and $PG(2,7)$.

See Also

§II.1	Existence of BIBDs.
§II.4	Constructions and tables of t-designs.
§II.5	Steiner systems.
§VII.9	Groups acting on designs.

References Cited: [234, 283, 285, 372, 373, 422, 423, 427, 428, 429, 430, 431, 533, 632, 667, 669, 670, 671, 806, 907, 1112, 1147, 1148, 1257, 1258, 1259, 1449, 1475, 1476, 1519, 1607, 1658, 1676, 1757, 1758, 1845, 2075, 2076]

6 Complete Mappings and Sequencings of Finite Groups

Anthony B. Evans

6.1 Complete Mappings and Orthomorphisms

6.1 For a group G with identity e, a bijection $\theta : G \to G$ is a *complete mapping* of G if the mapping $\sigma : x \mapsto x\theta(x)$ is a bijection, and an *orthomorphism* of G if the mapping $\eta : x \mapsto x^{-1}\theta(x)$ is a bijection. θ is *normalized* if $\theta(e) = e$.

6.2 **Remark** A bijection $\theta : G \to G$ is a complete mapping of G if and only if σ is an orthomorphism of G, and an orthomorphism of G if and only if η is a complete mapping of G.

6.3 Two mappings $\theta, \phi : G \to G$ are *orthogonal*, written $\theta \perp \phi$, if the mapping $\delta : x \mapsto \theta(x)^{-1}\phi(x)$ is a bijection. $\omega(G)$ denotes the largest number r for which there is a set of r pairwise orthogonal orthomorphisms of G. $\phi \perp \theta$.

6.4 **Examples**

1. If $\{(x_i, y_i) \mid i = 1, \ldots, n\}$ is a starter of G, $|G| = 2n + 1$, then θ defined by $\theta(e) = e$, $\theta(x_i) = y_i$, and $\theta(y_i) = x_i$ is an involutory orthomorphism of G. Starters and involutory orthomorphisms are equivalent. (See §VI.55.)
2. $\phi_i : x \mapsto x^i$ is a bijection if $(i, |G|) = 1$, a complete mapping if $(i + 1, |G|) = (i, |G|) = 1$, and an orthomorphism if $(i - 1, |G|) = (i, |G|) = 1$. $\phi_i \perp \phi_j$ if and only if $(i - j, |G|) = 1$.
3. For $\alpha, \beta \in Aut(G)$, α is an orthomorphism if and only if α is fixed-point-free (fixes only e), and $\alpha \perp \beta$ if and only if $\alpha\beta^{-1}$ is fixed-point-free.

6.5 **Remarks** The Cayley table M of the group $G = \{g_1, \ldots, g_n\}$ is the latin square with ijth entry $g_i g_j$. For a bijection $\theta : G \to G$, M_θ is the latin square with ijth entry $g_i\theta(g_j)$.

1. The cells $\{(g_i, \theta(g_i)) \mid i = 1, \ldots, n\}$ form a transversal of M if and only if θ is a complete mapping of G. There is a one-to-one correspondence between transversals of M and complete mappings of G.
2. M_θ is orthogonal to M if and only if θ is an orthomorphism of G.
3. If θ, ϕ are orthomorphisms of G then M_θ is orthogonal to M_ϕ if and only if $\theta \perp \phi$.

6.6 **Example** $F_4^+ = \{0, 1, g, g^2\}$, $1+g = g^2$. Let $\theta(x) = gx$, $\phi(x) = g^2x$, and $\gamma(x) = gx+1$. Then θ and ϕ are orthogonal orthomorphisms of F_4^+, and γ is a complete mapping of F_4^+. Then

$$M = \begin{bmatrix} 0 & \mathbf{1} & g & g^2 \\ 1 & 0 & g^2 & \mathbf{g} \\ g & g^2 & \mathbf{0} & 1 \\ \mathbf{g^2} & g & 1 & 0 \end{bmatrix}, \quad M_\theta = \begin{bmatrix} 0 & g & g^2 & 1 \\ 1 & g^2 & g & 0 \\ g & 0 & 1 & g^2 \\ g^2 & 1 & 0 & g \end{bmatrix}, \text{ and } M_\phi = \begin{bmatrix} 0 & g^2 & 1 & g \\ 1 & g & 0 & g^2 \\ g & 1 & g^2 & 0 \\ g^2 & 0 & g & 1 \end{bmatrix}.$$

From Remarks 6.5, M, M_θ, and M_ϕ form a set of 3 MOLS of order 4. The bold face entries in M form the transversal of M determined by γ.

6.7 **Theorem** (Hall–Paige) If the Sylow 2-subgroup of G is nontrivial and cyclic, then G admits no complete mappings.

6.8 **Conjecture** (Hall–Paige) If the Sylow 2-subgroup of G is trivial or noncyclic, then G admits complete mappings.

6.9 **Remark** Conjecture 6.8 has been proved for abelian groups, groups of odd order, 2-groups, and more generally solvable groups. It has also been proved for the groups A_n, S_n, and $Sz(2^{2n+1})$; $SU(3, q^2)$ and $PSU(3, q^2)$ for q even; $GL(2, q)$, $SL(2, q)$, $PGL(2, q)$, and $PSL(2, q)$; $GL(n, q)$, $SL(n, q)$, $PGL(n, q)$, and $PSL(n, q)$ for q even; $GL(n, q)$ and $PGL(n, q)$ for q odd; and many classes of almost simple groups.

6.10 **Theorem** (Aschbacher) If G is a minimal counterexample to Conjecture 6.8 then G has a quasi-simple normal subgroup L such that $C_G(L)$ and G/L are cyclic 2-groups.

6.11 **Theorem**

1. If $G \neq \{e\}$ and p is the smallest prime divisor of $|G|$, then $p-2 \leq \omega(G) \leq |G|-2$: $\{x \mapsto x^r \mid r = 2, \ldots, p-1\}$ is a set of $p-2$ pairwise orthogonal orthomorphisms of G.
2. $\omega(F_q^+) = q - 2$: $\{x \mapsto ax \mid a \neq 0, 1\}$ is a set of $q-2$ pairwise orthogonal orthomorphisms of F_q.

6.12 **Theorem** If $n \geq 5$ is odd then $\omega(\mathbb{Z}_n) \geq 3$, with the possible exception of some values of n of the form $9m$ with $\gcd(3, m) = 1$. The smallest unsettled cases are $n = 171$, 333, 369, 387, 423, and 477. See [32, 799].

6.13 **Table** Data for small groups. $Orth(G)$ is the set of normalized orthomorphisms of G. The actual number of orthomorphisms of a group G is $|G|$ times $|Orth(G)|$. Values for $|Orth(\mathbb{Z}_n)|$ can be found in [1139] and values for $|Orth(F_q^+)|$ can be found in [1417].

G	$\lvert G\rvert$	$\lvert Orth(G)\rvert$	$\omega(G)$	G	$\lvert G\rvert$	$\lvert Orth(G)\rvert$	$\omega(G)$
$\mathbb{Z}_3$	3	1	1	$\mathbb{Z}_2 \times \mathbb{Z}_6$	12	16,512	4
$\mathbb{Z}_2 \times \mathbb{Z}_2$	4	2	2	D_6	12	6,336	2
$\mathbb{Z}_5$	5	3	3	A_4	12	3,840	1
$\mathbb{Z}_7$	7	19	5	$\mathbb{Z}_{13}$	13	79,259	11
$\mathbb{Z}_4 \times \mathbb{Z}_2$	8	48	2	$\mathbb{Z}_{15}$	15	2,424,195	3
D_4	8	48	1	F_{16}^+	16	15,296,512	14
Q_4	8	48	1	$\mathbb{Z}_{17}$	17	94,417,089	15
F_8^+	8	48	6	$\mathbb{Z}_{19}$	19	4,613,520,889	17
$\mathbb{Z}_9$	9	225	1	$\mathbb{Z}_{21}$	21	275,148,653,115	≥ 4
F_9^+	9	249	7	$\mathbb{Z}_{23}$	23	19,686,730,313,955	21
$\mathbb{Z}_{11}$	11	3441	9				

6.14 **Remark** Of all groups of a given order the largest lower bounds for $\omega(G)$ have been found when G is a direct product of elementary abelian groups.

6.15 Table Lower bounds on $\omega(G)$, G a direct product of elementary abelian groups.

G	$\|G\|$	Bound	G	$\|G\|$	Bound	G	$\|G\|$	Bound
$F_3^+ \times F_8^+$	24	6	$F_3^+ \times F_{13}^+$	39	4	$F_3^+ \times F_{17}^+$	51	4
$F_4^+ \times F_7^+$	28	4	$F_5^+ \times F_8^+$	40	6	$F_4^+ \times F_{13}^+$	52	4
$F_3^+ \times F_{11}^+$	33	4	$F_4^+ \times F_{11}^+$	44	4	$F_5^+ \times F_{11}^+$	55	5
$F_5^+ \times F_7^+$	35	4	$F_5^+ \times F_9^+$	45	5	$F_7^+ \times F_8^+$	56	6
$F_4^+ \times F_9^+$	36	7	$F_3^+ \times F_{16}^+$	48	6			

6.16 Remarks

1. A set of r pairwise orthogonal orthomorphisms of G is equivalent to an $(|G|, r+2; 1)$-difference matrix, from which one can construct $r+1$ MOLS of order $|G|$.
2. A maximal set of r pairwise orthogonal orthomorphisms of G is equivalent to a maximal $(|G|, r+2; 1)$-difference matrix, from which one can construct an $r+1$ Max MOLS($|G|$). (See §VI.17.)
3. A set of $|G|-2$ pairwise orthogonal orthomorphisms of G is equivalent to a GH($|G|, 1$) over G and to a Cartesian projective plane of order $|G|$, with Cartesian group G.
4. From a Z-cyclic $TWh(4n+1)$ or $DWh(4n+1)$ one can construct a set of 3 pairwise orthogonal orthomorphisms of $\mathbb{Z}_{4n+1}$. (See §VI.64.)

6.17 Examples Complete mappings and orthomorphisms of F_q^+ can be represented by permutation polynomials (§VI.45). A permutation polynomial f of F_q is a *complete mapping (orthomorphism) polynomial* if $f(x)+x$ (resp. $f(x)-x$) is a permutation polynomial. $f \perp g$ if and only if $f(x)-g(x)$ is a permutation polynomial. f is *normalized* if $f(0)=0$.

1. For any q, the polynomial ax is an orthomorphism polynomial if and only if $a \neq 0, 1$ and a complete mapping polynomial if and only if $a \neq 0, -1$, and $ax \perp bx$ if and only if $a \neq b$.
2. For q odd, $ax^{\frac{q+1}{2}}+bx$ is a complete mapping polynomial if and only if $(b+a)(b-a)$ and $(b+a+1)(b-a+1)$ are nonzero squares, an orthomorphism polynomial if and only if $(b+a)(b-a)$ and $(b+a-1)(b-a-1)$ are nonzero squares, and $ax^{\frac{q+1}{2}}+bx \perp cx^{\frac{q+1}{2}}+dx$ if and only if $(b+a-d-c)(b-a-d+c)$ is a nonzero square.

6.18 Table Some examples of normalized orthomorphism polynomials.

q	Orthomorphism Polynomial
3	$2x$
4	ax, $a \neq 0, 1$
5	ax, $a \neq 0, 1$
7	ax, $a \neq 0, 1$ ax^4+4x, $a = 1, 6$
8	ax, $a \neq 0$, ax^4+bx^2+cx, $a \neq 0$, ax^3+bx+d irreducible for $d = c, c-1$
9	ax, $a \neq 0, 1$ ax^5, $a^2 = -1$ ax^5+bx, $a^2 = -1$, $b = \pm 1$ ax^3, a a nonsquare ax^3+x, a a nonsquare ax^3+bx, ab and $a(b-1)$ nonsquares
11	ax, $a \neq 0, 1$ ax^6+bx, $(a,b) = (2,4), (9,4), (4,6), (7,6), (3,6), (8,6), (6,10),$ $(5,10), (2,8), (9,8), (6,2)$, or $(5,2)$ $6x^7+x^5+10x^3+4x$, $4x^7+8x^5+3x^3+3x$, and $x^7+2x^5+9x^3+9x$

6.19 Remark Other orthomorphism polynomials can be obtained from those in Table 6.18, as if $f(x)$ is a normalized orthomorphism polynomial of F_q, then so are $f(x+b)-f(b)$, $f(bx)b^{-1}$ for $b \neq 0$, $x + f(-x)$, and $f^{-1}(x)$.

6.2 Variants of Complete Mappings

6.20 For a group G with identity e, a bijection $\theta : G \setminus \{h\} \to G \setminus \{e\}$, $h \neq e$, is a *near-complete mapping* of G if the mapping $\sigma : x \mapsto x\theta(x)$ is a bijection $G\setminus\{h\} \to G\setminus\{k\}$, for some $k \neq h$, and a *near-orthomorphism* of G if the mapping $\eta : x \mapsto x^{-1}\theta(x)$ is a bijection $G \setminus \{h\} \to G \setminus \{k\}$, for some $k \neq h^{-1}$. If $k = e$, then θ is in *canonical form*, in which case h is the *exdomain element* of θ.

6.21 Remark Let M be the Cayley table (see Remarks 6.5) of the group $G = \{g_1, \ldots, g_n\}$. An *almost-transversal* of M is a set of $n - 1$ cells of M, from distinct rows, distinct columns, and containing distinct entries. If $\theta : G \setminus \{h\} \to G \setminus \{e\}$ is a near-complete mapping of G then $\{(g_i, \theta(g_i)) \mid g_i \neq h\}$ is an almost-transversal of M.

6.22 Example $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 0 & 2 & 5 & . \end{pmatrix}$ is a near-complete mapping of $\mathbb{Z}_6$. The Cayley table of $\mathbb{Z}_6$ is shown on the right with the corresponding almost-transversal in bold. By Remarks 6.5.1 and Theorem 6.7, Cayley tables of cyclic groups of even order do not possess transversals.

0	**1**	2	3	4	5
1	2	3	**4**	5	0
2	3	4	5	0	1
3	4	**5**	0	1	2
4	5	0	1	2	**3**
5	0	1	2	3	4

6.23 Theorem An abelian group admits near-complete mappings if and only if it has a unique element of order 2.

6.24 Table The number N, of near-complete mappings in canonical form for groups with 12 or fewer elements.

G	$\lvert G\rvert$	N	G	$\lvert G\rvert$	N	G	$\lvert G\rvert$	N
$\mathbb{Z}_2$	2	1	D_4	8	16	D_6	12	10,944
$\mathbb{Z}_4$	4	2	Q_4	8	16	A_4	12	12,864
$\mathbb{Z}_6$	6	8	$\mathbb{Z}_{10}$	10	928	Q_6	12	17,280
D_3	6	6	D_5	10	820			
$\mathbb{Z}_8$	8	64	$\mathbb{Z}_{12}$	12	17,536			

6.25 A *left neofield* is a set N, with two binary operations, addition and multiplication, such that N is a loop with identity 0 under addition, the nonzero elements of N form a group N^* with identity 1 under multiplication, and the left distributive law holds. A *neofield* is a left neofield in which the right distributive law holds.

6.26 Theorems

1. A (left) neofield is completely determined by its *presentation function* $x \mapsto 1+x$. There is a unique element $h \in N$ satisfying $1 + h = 0$.
2. If $h \neq 1$, then the mapping $x \mapsto 1 + x$, $x \neq 0, h$, is a near-orthomorphism in canonical form of N^*, with exdomain element h.
3. If $h = 1$, then the mapping $x \mapsto 1 + x$, $x \neq 0, 1$, and $1 \mapsto 1$ is a normalized orthomorphism of N^*.
4. There is a one to one correspondence between near-orthomorphisms in canonical form of a group G and left neofields, in which $1 + 1 \neq 0$, with multiplicative group G.
5. There is a one to one correspondence between normalized orthomorphisms of a group G and left neofields, in which $1 + 1 = 0$, with multiplicative group G.

6. A left neofield N is a neofield if and only if the associated (near) orthomorphism commutes with all inner automorphisms of N^*.

6.27 **Remark** In [1140] cyclic neofields (neofields whose multiplicative group is cyclic) are classified and many constructions of cyclic neofields are given.

6.28 A *strong complete mapping* of a group G is a complete mapping of G that is also an orthomorphism of G.

6.29 **Theorem** $\mathbb{Z}_n$ admits strong complete mappings if and only if $(n, 6) = 1$.

6.30 **Theorem**

1. $x \mapsto x^i$ is a strong complete mapping of a group G if and only if $(i+1, |G|) = (i-1, |G|) = (i, |G|) = 1$.
2. Let $\theta : \mathbb{Z}_n \to \mathbb{Z}_n$ be a bijection. M_θ as defined in Remark 6.5 is a Knut Vik design (see §III.1.10) if and only if θ is a strong complete mapping of $\mathbb{Z}_n$.

6.31 **Theorem** Let θ be a strong complete mapping of the cyclic group $(\mathbb{Z}_n, +)$. Then the square matrix whose (i, j)th cell contains $i+\theta(j)$ is a Knut Vik design (§III.1.10). Conversely, any Knut Vik design $A = (a_{ij})$ on the n symbols $0, 1, \ldots, n-1$ defines a strong complete mapping $g \mapsto \theta(g)$ of $(\mathbb{Z}_n, +)$ such that $\phi(j) = a_{ij} - i$.

6.32 **Example** The mapping $h \mapsto 2h$ is a strong complete mapping of $((Z)_7, +)$. This defines the Knut Vik design on the right.

0	2	4	6	1	3	5
1	3	5	0	2	4	6
2	4	6	1	3	5	0
3	5	0	2	4	6	1
4	6	1	3	5	0	2
5	0	2	4	6	1	3
6	1	3	5	0	2	4

6.3 Sequencings of Groups

6.33 A *sequencing* of a group G of order n is an ordering $a_0 = e, a_1, a_2, \ldots, a_{n-1}$ of the elements of G such that all of the partial products $b_0 = a_0 = e,\ b_1 = a_0a_1,\ b_2 = a_0a_1a_2\ , \ldots, b_{n-1} = a_0a_1a_2 \cdots a_{n-1}$ are distinct. A group is *sequenceable* if it possesses a sequencing. The sequence $(b_0, b_1, \ldots, b_{n-1})$ is a *basic directed terrace*.

6.34 **Theorem** If $a_0, a_1, a_2, \ldots, a_{n-1}$ is a sequencing of a group of order n and $b_0, b_1, \ldots, b_{n-1}$ is the corresponding sequence of partial products, then $\theta(b_i) = a_{i+1}$, $i = 0, \ldots, n-2$ is a near-complete mapping of G with exdomain element b_{n-1}.

6.35 **Example** $0, 1, 2, 3, 4, 5, 6, 7$ is a sequencing of $\mathbb{Z}_8$ with partial sums $0, 1, 3, 6, 2, 7, 5, 4$. The associated near-complete mapping is $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 3 & . & 7 & 4 & 6 \end{pmatrix}$.

6.36 **Theorem** If $a_0, a_1, a_2, \ldots, a_{n-1}$ is a sequencing of a group G and $b_0, b_1, b_2, \ldots, b_{n-1}$ is the corresponding sequence of partial products, then $L = \{b_i^{-1}b_j\}$ is a complete latin square of order n. (See §VI.62.)

6.37 **Example** $0, 2, 5, 3, 1, 4$ is a sequencing of $\mathbb{Z}_6$ and $0, 2, 1, 4, 5, 3$ is the corresponding sequence of partial sums. The associated complete latin square is on the right.

0	2	1	4	5	3
4	0	5	2	3	1
5	1	0	3	4	2
2	4	3	0	1	5
1	3	2	5	0	4
3	5	4	1	2	0

6.38 **Theorem** An abelian group is sequenceable if and only if it has a unique element of order 2.

6.39 **Construction** $0, 1, -2, 3, -4, \ldots, 2n-3, -(2n-2), 2n-1$ is a sequencing of $\mathbb{Z}_{2n}$.

6.40 **Theorem** No nonabelian group of order less than 10 is sequenceable.

6.41 **Conjecture** (Keedwell) All nonabelian groups of order at least 10 are sequenceable.

6.42 **Remark** Conjecture 6.41 has been proved true for the following classes of groups:

1. All nonabelian groups of order n, $10 \le n \le 32$.
2. A_5, S_5, and all dihedral groups D_n of order at least 10.
3. Solvable groups with a unique element of order 2.
4. Some nonsolvable groups with a unique element of order 2.
5. Some groups of order pq, p, and q odd primes.

6.43 **Table** All sequencings of groups with 4, 6, or 8 elements.

$\mathbb{Z}_n$	Sequencing	$\mathbb{Z}_n$	Sequencing
$\mathbb{Z}_4$	0, 1, 2, 3	$\mathbb{Z}_8$ (cont.)	0, 3, 2, 4, 1, 5, 7, 6
	0, 3, 2, 1		0, 3, 6, 1, 4, 7, 2, 5
$\mathbb{Z}_6$	0, 1, 4, 3, 2, 5		0, 3, 7, 5, 2, 4, 1, 6
	0, 2, 5, 3, 1, 4		0, 5, 1, 3, 6, 4, 7, 2
	0, 4, 1, 3, 5, 2		0, 5, 2, 7, 4, 1, 6, 3
	0, 5, 2, 3, 4, 1		0, 5, 6, 4, 7, 3, 1, 2
$\mathbb{Z}_8$	0, 1, 2, 3, 4, 5, 6, 7		0, 5, 6, 7, 4, 1, 2, 3
	0, 1, 5, 7, 6, 4, 3, 2		0, 6, 1, 4, 2, 5, 7, 3
	0, 1, 6, 3, 4, 5, 2, 7		0, 6, 3, 1, 5, 4, 2, 7
	0, 1, 6, 4, 3, 7, 5, 2		0, 6, 5, 4, 2, 1, 3, 7
	0, 2, 1, 3, 7, 4, 6, 5		0, 6, 7, 5, 1, 4, 2, 3
	0, 2, 3, 4, 6, 7, 5, 1		0, 7, 2, 4, 5, 1, 3, 6
	0, 2, 5, 7, 3, 4, 6, 1		0, 7, 2, 5, 4, 3, 6, 1
	0, 2, 7, 4, 6, 3, 1, 5		0, 7, 3, 1, 2, 4, 5, 6
	0, 3, 2, 1, 4, 7, 6, 5		0, 7, 6, 5, 4, 3, 2, 1

6.44 **Table** Some sequencings of nonabelian groups of order 10, 12, and 14. $D_n = \langle a, b \mid a^n = b^2 = e, ab = ba^{-1} \rangle$, $A_4 = \langle a, b, c \mid a^2 = b^2 = c^3 = e, ab = ba, ca = abc, cb = ac \rangle$, and $Q_6 = \langle a, b \mid a^6 = e, b^2 = a^3, ab = ba^{-1} \rangle$.

Group	Sequencing
D_5	$e, ba, a^4, ba^2, b, ba^4, a^2, a, ba^3, a^3$
A_4	$e, abc, a, bc^2, ac^2, ac, c, bc, ab, b, c^2, abc^2$
D_6	$e, ba^2, a, b, a^2, ba^4, ba, ba^3, a^5, a^4, ba^5, a^3$
Q_6	$e, a^4, a, b, a^5, a^2, a^3, ba^4, ba^5, ba^3, ba, ba^2$
D_7	$e, b, a, ba^5, a^6, a^5, ba^6, a^4, ba^4, a^3, ba, ba^2, ba^3, a^2$

6.4 Variants on Sequencing

6.45 An *R-sequencing* of a group G of order n is an ordering $a_0 = e, a_1, a_2, \ldots, a_{n-1}$ of the elements of G such that the partial products $b_0 = a_0 = e$, $b_1 = a_0a_1$, $b_2 = a_0a_1a_2$, $\ldots, b_{n-2} = a_0a_1a_2 \cdots a_{n-2}$ are distinct and $a_0a_1a_2 \cdots a_{n-1} = e$. A group is *R-sequenceable* if it possesses an R-sequencing.

6.46 **Theorem** If $a_0, a_1, a_2, \ldots, a_{n-1}$ is an R-sequencing of a group G, $b_0, b_1, b_2, \ldots, b_{n-2}$ the corresponding sequence of partial products, and c the element of G that is not in the list of partial products, then the mapping $\theta : b_i \mapsto b_{i+1}$, $i = 0, 1, \ldots, n-3$, $\theta(b_{n-2}) = b_0$, $\theta(c) = c$ is an orthomorphism of G.

6.47 **Example** $0, 12, 2, 10, 4, 8, 6, 5, 9, 3, 11, 1, 7$ is an R-sequencing of $\mathbb{Z}_{13}$. The partial sums are $0, 12, 1, 11, 2, 10, 3, 8, 4, 7, 5, 6$, missing 9. The associated orthomorphism is

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 11 & 10 & 8 & 7 & 6 & 0 & 5 & 4 & 9 & 3 & 2 & 1 \end{pmatrix}.$$

6.48 Theorem If G is an R-sequenceable group, then its Sylow 2 subgroup is either trivial or noncyclic.

6.49 Theorem The following groups are R-sequenceable.

1. $\mathbb{Z}_n$, n odd.
2. Abelian groups of order n with $gcd(n, 6) = 1$.
3. D_n, n even.
4. Q_{2n} if $n + 1$ is a prime of the form $4k + 1$, for which -2 is a primitive root.
5. Nonabelian groups of order pq, $p < q$ odd primes, with 2 a primitive root of p.

6.50 Construction

1. $0,-1,2,-3,4,\ldots,-(2n-1),2n,2n-1,-(2n-2),2n-3,-(2n-4),\ldots,3,-2,1,-2n$ is an R-sequencing of $\mathbb{Z}_{4n+1}$.
2. $0,-1,2,-3,4,\ldots,-(2n-1),2n,-(2n+2),2n+3,-(2n+4),\ldots,-4n,4n+1,-(4n+2),2n+2$ is an R-sequencing of $\mathbb{Z}_{4n+3}$.

6.51 A *harmonious ordering* of a group G of order n is an ordering $a_0 = e, a_1, a_2, \ldots, a_{n-1}$ of the elements of G such that the products $a_0a_1,\ a_1a_2,\ a_2a_3, \ldots,\ a_{n-1}a_0$ are distinct. G is a *harmonious* group if it possesses a harmonious ordering.

6.52 Theorem If $a_0 = e, a_1, a_2, \ldots, a_{n-1}$ is a harmonious ordering of a group G, of order n, then the mapping $a_i \mapsto a_ia_{i+1}$, indices added modulo n, is an orthomorphism of G.

6.53 Example $0, 1, 2, \ldots, n-1$ is a harmonious ordering of $\mathbb{Z}_n$ if n is odd. The associated orthomorphism is $x \mapsto 2x + 1$.

6.54 Theorem The following groups are harmonious.

1. Groups of odd order.
2. Abelian groups with noncyclic 2-groups, except $F_{2^r}^+$.
3. D_n if 4 or 6 divides n.
4. Q_{2n} if 4 or 6 divides n.

6.55 Theorem The following groups are not harmonious.

1. Groups with nontrivial cyclic 2-groups.
2. $F_{2^r}^+$.

6.56 Remark See [173] for more on harmonious groups.

6.57 A group G of order $2n+1$ is *symmetrically harmonious* if it possesses a harmonious ordering $a_0 = e, a_1, a_2, \ldots, a_{2n}$ satisfying $a_{n-i+1} = a_{n+i}^{-1}$, $i = 1, 2, \ldots, n$.

6.58 An R^**-sequencing* of a group G of order n is an R-sequencing $a_0 = e, a_1, a_2, \ldots, a_{n-1}$ of G for which $a_i = a_{i-1}a_{i+1} = a_{i+1}a_{i-1}$, for some i. A group is R^**-sequenceable* if it possesses an R^*-sequencing.

6.59 A *symmetric sequencing* of a group G of order $2n$, with a unique element u of order 2, is a sequencing $a_0 = e, a_1, a_2, \ldots, a_{2n-1}$ of G for which $a_n = u$ and $a_{n-i} = a_{n+i}^{-1}$, $i = 1, 2, \ldots, n-1$. A group is *symmetrically sequenceable* if it possesses a symmetric sequencing.

6.60 **Table** Some direct product constructions. If G has the property in the first column and H the property in the second, then $G \times H$ has the property in the third column.

G	H	$G \times H$
harmonious	harmonious, of odd order	harmonious
sym. harmonious, of odd order	symmetrically harmonious, of odd order	symmetrically harmonious
R^*-sequenceable	symmetrically harmonious	R^*-sequenceable, with the possible exception of $\|G\|$ odd and $3\|\|H\|$
R^*-sequenceable, of even order	abelian, $\|H\|$ odd	R^*-sequenceable
sym. sequenceable	abelian, $(\|G\|, \|H\|) = 1$	symmetrically sequenceable

6.61 A 2-*sequencing* of a group G of order n is a sequence $a_0 = e, a_1, a_2, \ldots, a_{n-1}$ of elements of G in which $g \in G$ appears exactly once if $g = g^{-1}$, and $|\{i \mid a_i \in \{g, g^{-1}\}, i = 0, \ldots, n-1\}| = 2$ if $g \neq g^{-1}$, such that all of the partial products $b_0 = a_0 = e,\ b_1 = a_0a_1,\ b_2 = a_0a_1a_2\ , \ldots, b_{n-1} = a_0a_1a_2 \cdots a_{n-1}$ are distinct. A group is 2-*sequenceable* if it possesses a 2-sequencing.

6.62 **Example** $0, 1, -2, 3, -4, \ldots, (-1)^n(n-1)$ is a 2-sequencing of $\mathbb{Z}_n$. Thus, $0, 1, 1$ is a 2-sequencing of $\mathbb{Z}_3$; $0, 1, 2, 3$ is both a sequencing and a 2-sequencing of $\mathbb{Z}_4$, $0, 1, 3, 3, 1$ is a 2-sequencing of $\mathbb{Z}_5$; $0, 1, 4, 3, 2, 5$ is a sequencing and a 2-sequencing of $\mathbb{Z}_6$; and $0, 1, 5, 3, 3, 5, 1$ is a 2-sequencing of $\mathbb{Z}_7$.

6.63 **Theorem** For $r > 1$, the group $F_{2^r}^+$ is not 2-sequenceable.

6.64 **Theorem** The following groups are 2-sequenceable.

1. All sequenceable groups and all groups of odd order.
2. $G \times \mathbb{Z}_n$, G sequenceable and n odd.
3. $G \times \mathbb{Z}_2$, G solvable with a unique element of order 2 and $G \neq \mathbb{Z}_2$.
4. Groups of order at most 86, with the possible exception of 64, other than $F_{2^r}^+$.

6.65 **Conjecture** All groups of order at least 4, except $F_{2^r}^+$, are 2-sequenceable.

See Also

§VI.17	Many of the bounds in Tables 6.13 and 6.15 are derived from difference matrix constructions.
§VI.45	Permutation polynomials are useful in the construction and study of orthomorphisms of F_q^+ (Examples 6.17 and Table 6.18).
§VI.55	Self-inverse orthomorphisms are equivalent to starters (Example 6.4.1).
§VI.64	Some constructions of orthogonal sets of orthomorphisms of cyclic groups are derived from Z-cyclic triple whist and directed whist tournaments (Remarks 6.16.4).
[178]	A survey of orthomorphisms and near-orthomorphisms of groups.
[800]	A monograph on orthomorphisms and complete mappings of groups.
[684, 685]	These books contain material on complete mappings and sequencings of groups.
[1274]	A survey of group sequencings, updated in [685].
[1697]	A dynamic survey of group sequencings. Much of the material on group sequencings can be found here.

References Cited: [32, 173, 178, 684, 685, 799, 800, 1139, 1140, 1274, 1417, 1697]

7 Configurations

Harald Gropp

7.1 Definitions and Examples

7.1 A *configuration* (v_r, b_k) (abbreviation : cfz. (v_r, b_k)) is an incidence structure of v points and b lines such that
1. each line contains k points,
2. each point lies on r lines, and
3. two different points are connected by at most one line.

7.2 If $v = b$ and, hence, $r = k$, the configuration is *symmetric*, denoted by v_k.

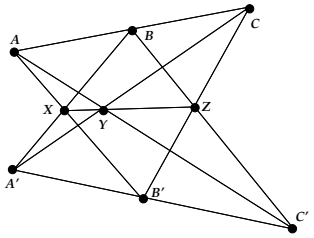
7.3 A configuration (v_r, b_k) can be described by 3 parameters *deficiency* d, *order* m, and *index* t, where $d = v - r(k-1) - 1, m = k - 1, t = r/k$.

7.4 The *configuration graph* of a configuration (v_r, b_k) has the v points as vertices, two vertices are joined by an edge iff the points are not collinear in the configuration. It is the *Martinetti graph* of the configuration and is d-regular.

7.5 **Example** The Fano configuration 7_3. (See also §I.1.)

{1,2,4}, {2,3,5}, {3,4,6}, {4,5,7}, {1,5,6}, {2,6,7}, {1,3,7}.

7.6 **Example** The Pappus configuration 9_3 (see §VII.2.14).



7.7 **Example** The Desargues configuration 10_3 is given in Example VII.2.151.

7.8 **Example** A configuration $(12_4, 16_3)$.

{1,5,12}, {1,6,8}, {1,7,10}, {1,9,11}, {2,4,9}, {2,6,7}, {2,8,11}, {2,10,12}, {3,4,10}, {3,5,11}, {3,7,12}, {3,8,9}, {4,5,6}, {4,11,12}, {5,7,8}, {6,9,10}.

7.2 Equivalent Combinatorial Objects

7.9 **Remarks**
1. A configuration (v_r, b_k) is a k-uniform r-regular linear hypergraph with v vertices and b hyperedges.
2. Steiner systems are configurations with $d = 0$.
3. A configuration corresponds to a bipartite semiregular graph with $v + b$ vertices, degrees r and k, and girth at least 6. This graph is the *Levi graph* of the configuration.

7.3 Existence and Enumeration

7.10 **Remarks** The necessary conditions for the existence of a configuration (v_r, b_k) are $vr = bk$ and $v \geq r(k-1)+1$. Without loss of generality, $v \leq b$. (If not, take the dual configuration by interchanging the role of points and lines).

7.11 **Theorem** The necessary conditions are also sufficient for $k = 3$ [984].

7.12 **Remarks**

1. For $k = 4$, no nonexistence result of a (v_r, b_k) configuration is known. All symmetric configurations $v_4, v \geq 13$ exist.
2. For $k = 5$, the necessary conditions are not sufficient. No configuration 22_5 exists.

7.13 **Table** Existence of configurations v_k for $5 \leq k \leq 12, d \leq 7$ [982]. (v_k means configuration exists, $-$ means configuration does not exist, no entry means existence unknown.)

$d=$	0	1	2	3	4	5	6	7
$k=5$	21_5	$-$	23_5	24_5	25_5	26_5	27_5	28_5
6	31_6	$-$	$-$	34_6	35_6	36_6	37_6	38_6
7	$-$	$-$	45_7			48_7	49_7	50_7
8	57_8	$-$					63_8	64_8
9	73_9	$-$				78_9		80_9
10	91_{10}	$-$						98_{10}
11	$-$							
12	133_{12}	$-$	135_{12}					

7.14 **Remarks** A configuration 98_{10} was constructed by M. Funk et al. It has recently been shown by P. Kaski and P. Östergård [1272] that there exists no configuration 33_6.

7.15 **Example** [1348] A configuration 34_6.

{1,6,10,15,23,27}, {19,25,27,29,30,33}, {9,13,14,22,23,29}, {7,8,17,19,23,32}, {11,14,17,20,27,31}, {10,12,13,19,20,26}, {3,4,5,14,15,19}, {4,8,9,16,18,27}, {2,11,13,15,18,33}, {4,6,13,17,21,30}, {1,2,4,12,25,32}, {6,8,14,25,26,34}, {4,7,10,11,29,34}, {2,6,9,19,24,31}, {1,18,19,21,28,34}, {1,5,9,11,26,30}, {6,11,12,16,22,28}, {2,7,21,22,26,27}, {5,10,17,18,22,25}, {1,8,20,22,24,33}, {15,16,17,24,26,29}, {2,3,8,10,28,30}, {7,12,14,18,24,30}, {15,22,30,31,32,34}, {3,6,18,20,29,32}, {1,3,7,13,16,31}, {2,5,16,20,23,34}, {5,8,12,21,29,31}, {10,14,16,21,32,33}, {7,9,15,20,25,28}, {3,9,12,17,33,34}, {5,13,24,27,28,32}, {3,11,21,23,24,25}, {4,23,26,28,31,33}.

7.16 **Table** The number n of nonisomorphic configurations v_3 for $v \leq 19$ [233, 982].

v	7	8	9	10	11	12	13	14	15	16	17	18	19
n	1	1	3	10	31	229	2036	21399	245342	3004881	38904499	530452205	7640941062

7.17 **Table** The number n of nonisomorphic configurations v_4 for $v \leq 18$ [229].

v	13	14	15	16	17	18
n	1	1	4	19	1972	971171

7.18 **Table** The number n of nonisomorphic configurations (v_r, b_k). For the first entry see [981], otherwise see [987].

(v_r, b_k)	$(12_4, 16_3)$	$(12_5, 20_3)$	$(14_6, 28_3)$	$(15_6, 30_3)$	$(18_8, 48_3)$
n	574	5	787	10177328	210611385743

7.4 Blocking Set Free Configurations and λ-Configurations

7.19 A subset of the point set of a configuration is a *blocking set* if it intersects all lines in at least 1 and at most $k-1$ points. A configuration is *blocking set free* if it does not contain a blocking set.

7.20 Remarks

1. There is a blocking set free configuration v_3 only for $v = 7, 13, 19, 21, 22, 25$ and for $v \geq 27$.
2. All symmetric configurations v_k with $k \geq 4$ have a blocking set [986].

7.21 A λ-*configuration* $(v_r, b_k)_\lambda$ is an incidence structure of v points and b lines such that

1. each line contains k points,
2. each point lies on r lines, and
3. two different points are connected by at most λ lines.

7.22 A 2-configuration $(v_r, b_k)_2$ is also a *spatial* configuration.

7.23 Remarks 1. All 2-configurations $(v_k)_2$, $3 \leq k \leq 6$ exist for $v \geq (k(k-1)/2) + 1$ [985].
2. $(v_7)_2$ exist for $v \geq 24$. Neither a $(22_7)_2$ nor a $(23_7)_2$ exists.

See Also

§IV.6	Regular linear spaces give configurations for each block size. Existence and enumeration results on some configurations.
§VI.42	Partially balanced incomplete block designs.
§VI.49	Configurations are special $(r, 1)$-designs (see [983]).
[980]	A survey on the history of configurations.
[987]	A more detailed survey on configurations.

References Cited: [229, 233, 980, 981, 982, 983, 984, 985, 986, 987, 1272, 1348]

8 Correlation-immune and Resilient Functions

K. Gopalakrishnan
Douglas R. Stinson

8.1 Let S be a set, $|S| = q$. Let $n \geq m \geq 1$ be integers and suppose $f : S^n \longrightarrow S^m$ is a function.

1. f has *balanced input* if every possible input vector is chosen with probability $1/q^n$.
2. f is an (n, m, t, q)-*correlation-immune* function if the probability of obtaining an output m-tuple $(y_1, \ldots, y_m)$ is exactly the same when the input is balanced as it is when the values of t inputs are fixed and the remaining $n - t$ inputs are chosen independently and uniformly at random.
3. f has *balanced output* if every possible output m-tuple occurs with equal probability $1/q^m$ whenever f has balanced input.
4. f is an (n, m, t, q)-*resilient function* if it is a (n, m, t, q)-correlation-immune function and it has balanced output.

8.2 Example Some resilient functions (all arithmetic performed in $\mathbb{F}_q$).

1. $m = 1$, $t = n - 1$. Define $f(x_1, \ldots, x_n) = x_1 + \ldots + x_n$.

2. $m = n - 1$, $t = 1$. Define $f(x_1, \ldots, x_n) = (x_1 + x_2, x_2 + x_3, \ldots, x_{n-1} + x_n)$.
3. $m = 2$, $n = 3h$, $t = 2h - 1$. Define
$$f(x_1, \ldots, x_{3h}) = (x_1 + \ldots + x_{2h}, x_{h+1} + \ldots + x_{3h}).$$

8.3 **Theorem** A $(2, 1, 1, q)$-resilient function is equivalent to a latin square of order q.

8.4 A *generalized large set of orthogonal arrays* $\mathrm{GLOA}[q^m]_{\lambda_1,\ldots,\lambda_{q^m}}(t, n, q)$ consists of q^m simple arrays $\mathrm{OA}_{\lambda_i}(t, n, q)$ such that every n-tuple occurs in exactly one of the q^m OAs. It holds that
$$\textstyle\sum_{i=1}^{q^m} \lambda_i = q^{n-t}.$$
When $\lambda_1 = \lambda_2 = \ldots = \lambda_{q^m} = q^{n-t-m}$ a GLOA is simply a *large set of orthogonal arrays* and is denoted $\mathrm{LOA}_{q^{n-t-m}}(t, n, q)$.

8.5 **Theorem** An (n, m, t, q)-resilient function is equivalent to a large set of orthogonal arrays $\mathrm{LOA}_{q^{n-m-t}}(t, n, q)$.

8.6 **Remark** An outline of the proof of Theorem 8.5: Start with an (n, m, t, q)-resilient function. For any $y \in \mathbb{F}_q^m$, the inverse image $f^{-1}(y)$ yields an $\mathrm{OA}_{q^{n-m-t}}(t, n, q)$ and the q^m orthogonal arrays thus obtained form a large set of orthogonal arrays $\mathrm{LOA}_{q^{n-m-t}}(t, n, q)$. The converse is also straightforward.

8.7 **Example** As an illustration, consider the following binary resilient function:
$$f(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1 + x_2 + x_3 + x_4, x_3 + x_4 + x_5 + x_6),$$
where addition is modulo 2. This is a $(6, 2, 3, 2)$-resilient function, and by Theorem 8.5, it is equivalent to a large set of $\mathrm{OA}_2(3, 6, 2)$. There are four orthogonal arrays in the large set; the one obtained from $f^{-1}(0, 0)$ is:
$$\begin{pmatrix}
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}$$

8.8 **Theorem** An (n, m, t, q)-correlation-immune function is equivalent to a generalized large set of orthogonal arrays $\mathrm{GLOA}[q^m]_{\lambda_1,\ldots,\lambda_{q^m}}(t, n, q)$.

8.9 **Theorem** If there is a linear m-dimensional code of length n over $\mathbb{F}_q$ having minimum Hamming distance d, then there is a $(n, m, d - 1, q)$-resilient function.

8.10 **Remark** The construction of the desired resilient function for Theorem 8.9 is straightforward. Let G be a m by n generating matrix for the hypothesized code. Then define $f : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^m$ to be $f(x) = x\,G^T$ for all $x \in (\mathbb{F}_q)^n$.

8.11 A resilient function of the form $x \mapsto x\,G^T$ is a *linear* resilient function.

8.12 **Remark** It was conjectured by Bennett, Brassard and Robert [188] that, if there exists an $(n, m, t, 2)$-resilient function, then there exists a linear $(n, m, t, 2)$-resilient function. Stinson and Massey [1973] disproved the conjecture by exhibiting an infinite class of counterexamples derived from the nonlinear Kerdock codes.

8.13 **Example** There exists a nonlinear $(16, 8, 5, 2)$-resilient function, but there exists no linear resilient function with these parameters. This resilient function can be constructed using an encoding algorithm for the (nonlinear) Nordstrom–Robinson code. The information bits are $z_1, \ldots, z_8$ and the parity-check bits are $z_9, \ldots, z_{16}$. The parity-check bits are computed as follows (all operations modulo 2):

$$
\begin{aligned}
z_9 &= z_1 + z_2 + z_4 + z_7 + z_8 + (z_1 + z_5)(z_2 + z_3 + z_4 + z_6) + (z_2 + z_3)(z_4 + z_6) \\
z_{10} &= z_2 + z_3 + z_5 + z_1 + z_8 + (z_2 + z_6)(z_3 + z_4 + z_5 + z_7) + (z_3 + z_4)(z_5 + z_7) \\
z_{11} &= z_3 + z_4 + z_6 + z_2 + z_8 + (z_3 + z_7)(z_4 + z_5 + z_6 + z_1) + (z_4 + z_5)(z_6 + z_1) \\
z_{12} &= z_4 + z_5 + z_7 + z_3 + z_8 + (z_4 + z_1)(z_5 + z_6 + z_7 + z_2) + (z_5 + z_6)(z_7 + z_2) \\
z_{13} &= z_5 + z_6 + z_1 + z_4 + z_8 + (z_5 + z_2)(z_6 + z_7 + z_1 + z_3) + (z_6 + z_7)(z_1 + z_3) \\
z_{14} &= z_6 + z_7 + z_2 + z_5 + z_8 + (z_6 + z_3)(z_7 + z_1 + z_2 + z_4) + (z_7 + z_1)(z_2 + z_4) \\
z_{15} &= z_7 + z_1 + z_3 + z_6 + z_8 + (z_7 + z_4)(z_1 + z_2 + z_3 + z_5) + (z_1 + z_2)(z_3 + z_5) \\
z_{16} &= \textstyle\sum_{i=1}^{15} z_i.
\end{aligned}
$$

A $(16, 8, 5, 2)$-resilient function, $f : \{0,1\}^{16} \to \{0,1\}^8$, can be computed according to the following algorithm:

1. Given $x = (x_1, \ldots, x_{16})$, compute parity-check bits $z_9, \ldots, z_{16}$ for the information bits $x_1, \ldots, x_8$.
2. Define $f(x) = (x_9 + z_9, \ldots, x_{16} + z_{16}) \bmod 2$.

See Also

§III.3	Orthogonal arrays of strength 2.
§III.7	Orthogonal arrays of strength $t > 2$.
§VII.1	Codes and orthogonal arrays.
[258]	Section 15.5 discusses OAs and resilient functions.
[1911]	The paper that introduced correlation-immune functions.
[188, 497]	The papers that introduced resilient functions.
[1973, 263, 432]	Further results on resilient functions.

References Cited: [188, 258, 263, 432, 497, 1911, 1973]

9 Costas Arrays

Herbert Taylor
Jeffrey H. Dinitz

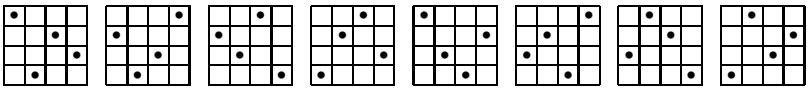
9.1 Definitions and Examples

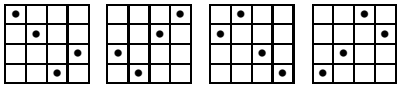
9.1 A *Costas array* of *order* n is an n by n array of dots and blanks that satisfies:

1. There are n dots and $n(n-1)$ blanks, with exactly one dot in each row and column.
2. All the segments between pairs of dots differ in length or in slope.

9.2 $C(n)$ denotes the number of distinct n by n Costas arrays.
$c(n)$ denotes the number of n by n Costas arrays, inequivalent under the dihedral group of rotations and reflections of the square.
$s(n)$ denotes the number of n by n Costas arrays that are symmetric across a diagonal and inequivalent under the dihedral group of rotations and reflections of the square.

9.3 **Example** $C(4) = 12, \quad c(4) = 2, \quad \text{and} \quad s(4) = 1.$





9.4 **Remark** For $n > 2$, if a Costas array is symmetric across a diagonal, its dihedral equivalence class contains four arrays; otherwise, it contains eight arrays. Thus, for $n > 2$, $C(n) = 8 \cdot c(n) - 4 \cdot s(n)$.

9.5 Let $\pi(j) = i$ when there is a dot at (i, j). A Costas array of order n can be presented in the form:

$\pi(1)$	$\pi(2)$	$\pi(3)$	$\pi(4)$		$\cdots\cdots$		$\pi(n-1)$	$\pi(n)$

9.6 **Example** $c(5) = 6$. One representative of each dihedral equivalence class.

1	3	4	2	5	1	5	3	2	4	1	5	4	2	3
2	1	5	3	4	2	4	1	5	3	2	5	1	3	4

9.7 **Example** A Costas array of order 7 that is not obtained by any known algebraic construction is the following:

3	6	7	1	5	2	4

.

9.8 **Theorem** [1431] For $n \geq 4$, two Costas arrays of order n cannot have disjoint sets of segments (with respect to length and slope) between pairs of dots.

9.2 Algebraic Constructions and Examples

9.9 **Construction** (*Welch construction*) Let p be prime and α be a primitive element in the field $\mathbb{F}_p$. Let $n = p - 1$. A Costas array of order n is obtained by placing a dot at (i, j) if and only if $i = \alpha^j$, for $a \leq j < n + a$, a a nonnegative integer, and $i = 1, \cdots, n$.

9.10 **Construction** Let α and β be primitive elements in the field $\mathbb{F}_q$ for q a prime power. Let $n = q - 2$. Costas arrays of order n are obtained by

1. *Lempel construction:* Put a dot at (i, j) if and only if $\alpha^i + \alpha^j = 1$, $1 \leq i, j \leq n$.
2. *Golomb construction:* Put a dot at (i, j) if and only if $\alpha^i + \beta^j = 1$, $1 \leq i, j \leq n$.

9.11 **Remark** $C(p-1) \geq 1$ and $C(q-2) \geq 1$ from Constructions 9.9 and 9.10, respectively. Also, if a corner dot is present in a Costas array of order n, it can be removed along with its row and column to obtain a Costas array of order $(n - 1)$.

9.12 **Theorem** If $q > 2$ is a prime power, then there exist primitive elements α and β in $\mathbb{F}_q$ such that $\alpha + \beta = 1$.

9.13 **Corollary** Removing the corner dot at $(1, 1)$ in the Costas array of order $(q - 2)$ from Construction 9.10(2) yields $C(q - 3) > 0$.

9.14 **Example** If there exist primitive elements α and β satisfying the conditions stated, then a Costas array of order n can be obtained by removing one or more corner dots.

Conditions	n
$\alpha^1 = 2$	$q - 3$
$\alpha^1 + \beta^1 = 1$ and $\alpha^2 + \beta^2 = 1$	$q - 4$
$\alpha^2 + \alpha^1 = 1$	$q - 4$
$\alpha^1 + \beta^1 = 1$ and $\alpha^2 + \beta^{-1} = 1$	$q - 4$
and necessarily $\alpha^{-1} + \beta^2 = 1$	$q - 5$

9.15 **Remark** For $n \geq 30$, except for $n = 31$ and $n = 53$, the only orders for which Costas arrays are known are orders $n = p - 1$ or $n = q - 2$ or orders for which some algebraic condition exists which guarantees corner dots whose removal leaves a smaller Costas array.

9.16 **Proposition** Costas arrays of order n are known to exist for all $1 \leq n \leq 359$ except for $n \in \{32, 33, 43, 48, 49, 54, 63, 73, 74, 83, 84, 85, 89 - 93, 97, 103, 109, 113 - 117, 120, 121, 131 - 133, 139 - 143, 151 - 153, 157 - 159, 163, 168, 169, 173, 174, 181 - 186, 193, 199 - 207, 211 - 219, 223, 229, 233, 234, 242 - 246, 251, 257 - 259, 263, 271 - 273, 277, 283 - 285, 288, 289, 293 - 303, 313, 317 - 327, 331 - 333, 337 - 339, 342, 343, 349, 353, 354\}$.

9.17 **Remark** The only known Costas array of order 53 was found by Carbonera by adding a corner dot to one of the Costas arrays of order 52. The only known Costas array of order 31 was found in similar fashion from one of order 30. Rickard [1804] found new Costas arrays of orders 29, 36, and 42 by starting with arrays constructed from Theorems 9.9 and 9.10 and using a so-called *1-gap augmentation*. This method failed to produce new Costas arrays for any other orders less than 100.

9.3 Singly Periodic Costas Arrays

9.18 Let an n by n array be extended left and right putting a dot at $(i, j + n)$ if and only if there is a dot at (i, j). A *singly periodic Costas array* of order n is an $n \times n$ array such that every $n \times n$ window in the left-right extension is a Costas array of order n.

9.19 **Example** A singly periodic Costas array of order 6 with $i = 3^j$ in $\mathbb{F}_7$.

$$\ldots, (1, 0), (3, 1), (2, 2), (6, 3), (4, 4), (5, 5), (1, 6), (3, 7), (2, 8), \ldots .$$

9.20 **Remarks** The only known singly periodic Costas arrays of order n come from Construction 9.9 when $n = p - 1$. A singly periodic Costas array of order n does not exist if $n > 1$ is odd, nor if $n \in \{8, 14, 20\}$.

9.21 **Theorem** [792] If M is a singly periodic Costas array of order $n > 4$ given by Construction 9.9, then the transpose of M is not a singly periodic Costas array.

9.22 **Remark** It remains open whether for $n > 20$ a matrix M exists such that both M and its transpose are singly periodic Costas arrays of order n.

9.23 **Proposition** [792] A singly periodic Costas array of order n is equivalent to a vatican square of order n constructed by the polygonal path construction. See §VI.62.

9.4 G-Symmetry (Glide-Reflection Symmetry)

9.24 A Costas array of order $2m$ has *G-symmetry* if for j from 1 to m there is a dot at (i, j) if and only if there is a dot at $(2m - i + 1,\ m + j)$.
A Costas array of order $(2m-1)$ has *G-symmetry* if there is a dot at (m, m), and for j from 1 to $(m-1)$ there is a dot at (i, j) if and only if there is a dot at $(2m-i,\ m+j)$.

9.25 $c_G(n)$ denotes the number of Costas arrays of order n that have G-symmetry and are inequivalent under the dihedral group of rotations and reflections of the square. $c_G^\star(n) = c_G(n)$ minus the number of those obtained from Construction 9.9.

9.26 **Example** [792] The only Costas array of order $2m$ different from its transpose, both having G-symmetry.

1	7	6	4	8	2	3	5

1	6	7	4	8	3	2	5

9.27 **Theorem** [792] For $2m > 8$, if a Costas array of order $2m$ has G-symmetry, then its transpose does not have G-symmetry.

9.28 **Remark** All known singly periodic Costas arrays of order n have G-symmetry.

9.5 Further Examples and Enumeration

9.29 **Example** The only known Costas array of order 31 (all arithmetic in $\mathbb{F}_{31}$).

0	3^3	3^4	3^5		.....		3^{30}	3^{31}	3^{32}

9.30 **Example** A Costas array of nonattacking kings.

3	5	8	1	7	4	2	6

9.31 A *honeycomb Costas array* is a Costas array of order $(2r+1)$ whose dot positions (i, j) are such that $(i - j)$ takes each value exactly once from $-r$ to r.

9.32 **Remark** Honeycomb arrays are discussed in [929] and are related to the *zero sum arrays* of Bennett and Potts [187].

9.33 **Example** A honeycomb Costas array not given by any known algebraic construction.

1	3	6	2	7	5	4

9.34 **Table** For each triple n, α, q given there exists a honeycomb Costas array of order n from Construction 9.10(1) with primitive α in $\mathbb{F}_q$.

n	7	9	9	15	15	21	27	45
α	$\alpha^2 = \alpha + 1$	2	7	3	5	7	3	30
q	9	11	11	17	17	23	29	47

9.35 **Remark** Proofs for the algebraic constructions are given in [926]. Cenkl and Rushanan report that honeycomb Costas arrays of orders 17 and 19 do not exist.

9.36 **Table** Enumeration of Costas arrays of order n, $1 \le n \le 32$ (see [929, 175])

n	$C(n)$	$s(n)$	$c(n)$	$c_G(n)$	$c_G^\star(n)$	n	$C(n)$	$s(n)$	$c(n)$	$c_G(n)$	$c_G^\star(n)$
1	1	1	1	1	0	2	2	1	1	1	0
3	4	1	1	0	0	4	12	1	2	2	0
5	40	2	6	1	1	6	116	5	17	4	1
7	200	10	30	0	0	8	444	9	60	3	3
9	760	10	100	0	0	10	2160	14	277	24	14
11	4368	18	555	0	0	12	7852	17	990	44	32
13	12828	25	1616	4	4	14	17252	23	2168	31	31
15	19612	31	2467	0	0	16	21104	20	2648	77	45
17	18276	19	2294	0	0	18	15096	10	1892	29	2
19	10240	6	1283	0	0	20	6464	4	810	3	3
21	3536	8	446	0	0	22	2052	5	259	55	0
23	872	10	114	0	0	24	200	0	25		
25	88	2	12			26	56	2	8		
27	≥ 28	7	≥ 7			28	≥ 1	0	≥ 1		
29	≥ 20	5	≥ 5			30	≥ 16	4	≥ 4		
31	≥ 1	0	≥ 1			32	?	0	?		

9.37 **Remark** The properties of a Costas array make it an ideal discrete waveform for Doppler sonar. Having one dot in each row and column minimizes reverberation. Distinct segments between pairs of dots give it a thumbtack ambiguity function because,

shifted left-right in time and up-down in frequency, copies of the pattern can only agree with the original in one dot, no dots, or all n dots at once. Thus, the spike of the thumbtack makes a sharp distinction between the actual shift and all the near misses. See [608, 929, 1431].

See Also

§VI.62	Proposition 9.23 gives a connection between Costas arrays and vatican squares.
[1431]	Chapter 8 contains a discussion of the use of Costas arrays as coded radar signals.
[1804]	Contains some useful references.

References Cited: [175, 187, 608, 792, 926, 929, 1431, 1804]

10 Covering Arrays

Charles J. Colbourn

10.1 Definitions and Applications

10.1 A *covering array* $\mathrm{CA}_\lambda(N; t, k, v)$ is an $N \times k$ array. In every $N \times t$ subarray, each t-tuple occurs at least λ times. Then t is the *strength* of the coverage of interactions, k is the number of components (*degree*), and v is the number of symbols for each component (*order*). Only the case when $\lambda = 1$ is treated; the subscript is then omitted in the notation. The size N is omitted when inessential in the context.

10.2 The size of a covering array is the *covering array number* $\mathrm{CAN}(t, k, v)$. The covering array is *optimal* if it contains the minimum possible number of rows.

10.3 **Example** A CA(13;3,10,2):

0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
1	1	1	0	1	0	0	0	0	1
1	0	1	1	0	1	0	1	0	0
1	0	0	0	1	1	1	0	0	0
0	1	1	0	0	1	0	0	1	0
0	0	1	0	1	0	1	1	1	0
1	1	0	1	0	0	1	0	1	0
0	0	0	1	1	1	0	0	1	1
0	0	1	1	0	0	1	0	0	1
0	1	0	1	1	0	0	1	0	0
1	0	0	0	0	0	0	1	1	1
0	1	0	0	0	1	1	1	0	1

10.4 A family of partitions is *t-qualitatively independent* when for every t of the partitions $R_{i_1}, \ldots R_{i_t}$ and for every choice of classes $M_{i_j} \in R_{i_j}$ for $1 \le j \le t$, one finds that $\bigcap_{j=1}^{t} M_{i_j} \neq \emptyset$.

10.5 **Remark** Let C be an $N \times k$ covering array. Suppose that rows are indexed by a set R of size N. Then each column can be viewed as a partition of R into exactly v classes

$(M_1, \ldots, M_v)$; the class M_i of a symbol $r \in R$ is determined by the value i appearing in row r in the chosen column. Hence, C gives a collection $\mathcal{P} = \{R_1, R_2, \ldots, R_k\}$ of partitions of R. Indeed, covering arrays of strength t having N rows are the same as t-qualitatively independent partitions of a set of size N.

10.6 **Remark** Covering arrays arise in screening for interactions of small strength among experimental factors. Factors affecting response are represented by columns, and entries within the columns represent settings or values for that factor. Rows represent tests to be run, in which a value for each factor is dictated. Among all tests of a $\mathrm{CA}(t, k, v)$, all v^t combinations of values for every set of the $\binom{k}{t}$ factors is tested at least once. Hence, covering arrays have been extensively studied for interaction testing among components consisting of software, hardware, and/or network elements, and also for chemical and biological interactions. See [530]. Not all factors have the same number of values in general.

10.7 A *mixed level covering array* $\mathrm{MCA}_\lambda(N; t, k, (v_1, v_2, \ldots, v_k))$ is an $N \times k$ array. Let $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, k\}$, and consider the subarray of size $N \times t$ obtained by selecting columns $i_1, \ldots, i_t$ of the MCA. There are $\prod_{i=1}^{t} v_i$ distinct t-tuples that could appear as rows, and an MCA requires that each appear at least once. $\mathrm{CAN}(t, k, (v_1, v_2, \ldots, v_k))$ denotes the smallest N for which such a mixed covering array exists.

10.8 **Theorems** (see [460])

Composition: $\mathrm{CAN}(t, k, vw) \le \mathrm{CAN}(t, k, v)\mathrm{CAN}(t, k, w)$.

Symbol identification: $\mathrm{CAN}(t, k, (v_1, v_2, \ldots, v_k)) \le \mathrm{CAN}(t, k, (v_1 - 1, v_2, \ldots, v_k))$ and $\mathrm{CAN}(t, k, v - 1) \le \mathrm{CAN}(t, k, v) - 1$.

Derivation: $\mathrm{CAN}(t - 1, k - 1, (v_2, \ldots, v_k)) \le \lfloor \mathrm{CAN}(t, k, (v_1, v_2, \ldots, v_k))/v_1 \rfloor$.

10.9 **Remark** Only for one nontrivial selection of (t, v) is $\mathrm{CAN}(t, k, v)$ known. The exact determination of $\mathrm{CAN}(2, k, 2)$ was completed by Rényi, Kleitman, and Spencer, and Katona (see [1061]). The largest number k for which a $\mathrm{CA}(N; 2, k, 2)$ exists is $\binom{N-1}{\lceil \frac{N}{2} \rceil}$.

10.10 $\kappa(N; t, v)$ is the largest k for which $\mathrm{CAN}(t, k, v) \le N$.

10.11 **Theorem** [1756] $\frac{et}{v} e^{\frac{N}{tv^t}} \le \kappa(N; t, v) \le \frac{k_{v,N}}{\sqrt{N}} 4^{\frac{N}{v^t - 1}}$, where $k_{v,N}$ is a constant depending only on v and N. (Informally, k grows exponentially in N for fixed t and v.)

10.2 Constructions

10.12 **Remark** An orthogonal array is a covering array; when its index is one, the covering array is optimal.

10.13 The *Turán number* $T(t, n)$ is the largest number of edges in a t-vertex simple graph having no $(n + 1)$-clique.

10.14 **Theorem** [1061] If a $\mathrm{CA}(N; t, k, v)$ and a $\mathrm{CA}(k^2; 2, T(t, v) + 1, k)$ both exist, then a $\mathrm{CA}(N \cdot (T(t, v) + 1); t, k^2, v)$ exists.

10.15 **Theorem** (see [264, 1531]) If a perfect hash family $\mathrm{PHF}(s; k, m, t)$ and a $\mathrm{CA}(N; t, m, v)$ both exist then a $\mathrm{CA}(sN; t, k, v)$ exists.

10.16 **Remark** There are many *product* or *Roux-type* constructions that make larger covering arrays from smaller ones. These are all subsumed by the constructions in [566] for strength two, [519, 567] for strength three, and [567] for strength four. At present only doubling constructions are known for strength $t > 4$; these are stated next.

10.17 Theorem [1530] $\mathrm{CAN}(t, 2\ell, v) \le \mathrm{CAN}(t, \ell, v)+(v-1)\mathrm{CAN}(t-1, \ell, v)+\mathrm{CAN}(t-2, \ell, v^2)$.

10.18 Theorem [1531] For $t \ge 4$ and $v \ge 2$, $\mathrm{CAN}(t, 2k, v) \le \mathrm{CAN}(t-1, k, v)+(v-1)\mathrm{CAN}(t-1, k, v) + \sum_{i=2}^{t-2} \mathrm{CAN}(i, k, v)\mathrm{CAN}(t-i, k, v)$.

10.19 Remark Deleting a column in a covering array produces a *resolution* of the remaining array. *Projection* instead employs a resolution to add new columns. Theorem 10.20 uses frame parallel classes obtained by deleting one symbol from each of many columns.

10.20 Theorem [531] Let q be a prime power. Let $1 \le t \le q$ and $1 \le s \le q-t$. Then there is an $\mathrm{MCA}(q^2-t; 2, q+1+t, (q-t)^{q+1}s^t)$. Indeed, there exists a $\mathrm{CA}(q^2-t; 2, q+1+t, q-t)$.

10.21 Remark Other direct constructions use computational methods, often in conjunction with structural assumptions such as restrictions on the automorphism group. Exact computational methods have been of limited use (see [1927]). Heuristic methods successfully employed include greedy [367, 516], hill-climbing [517], simulated annealing [517, 519], tabu search [1688, 2102], and constraint programming [1111]. Automorphism group restrictions are used in [460, 566, 1583]; a "permutation vector" representation is used in [2102].

10.3 Tables

10.22 Table Known lower bounds on $\kappa(N; t, v)$ for small parameters. Entries are of the form "$\underline{k}$ N^{α}". Select the smallest $\underline{k}$ for which $\underline{k} \ge k$, and let N be the corresponding size. Then $\mathrm{CAN}(t, k, v) \le N$, and the construction to establish this is specified by the authority α (given in Table 10.23).

$\kappa(N; 2, 3)$					
4	9^o	5	11^b	7	12^s
9	13^s	10	14^s	20	15^t
24	17^t	30	18^t	36	19^t
43	20^t	74	21^3	94	23^2
134	24^3	174	25^3	194	26^2
394	27^3	474	29^3	594	30^3
714	31^3	854	32^3	1474	33^3
1796	35^2	2364	36^2	3030	37^2
3766	38^2	6836	39^2	8238	41^2

$\kappa(N; 2, 4)$					
5	16^o	6	19^a	7	21^s
8	22^s	10	24^s	11	25^s
12	26^s	14	27^s	24	28^3
29	31^3	30	32^3	34	33^3
38	34^3	40	35^3	49	36^3
54	37^3	59	38^3	69	39^3
116	40^3	140	43^3	144	44^3
164	45^3	184	46^3	192	47^3
236	48^3	260	49^3	284	50^3

$\kappa(N; 2, 5)$					
6	25^o	7	29^b	8	33^b
9	35^s	10	37^s	11	38^s
12	40^s	13	41^s	14	42^s
15	43^s	16	44^s	35	45^3
41	49^3	42	52^3	48	53^2
52	55^3	54	56^3	59	57^3
65	58^3	71	60^3	77	61^3
83	62^3	90	63^3	95	64^3
205	65^3	240	69^3	245	72^3

$\kappa(N; 2, 6)$					
3	36^o	4	37^s	5	39^s
6	41^t	8	42^t	9	46^b
10	51^b	11	55^s	12	56^s
13	58^s	14	60^s	15	61^s
16	62^s	17	64^s	19	70^3
20	71^2	24	72^3	26	73^3
32	74^2	34	75^3	40	76^2
42	77^2	48	78^2	50	79^2
56	80^2	66	82^2	72	84^2

$\kappa(N;2,7)$					
8	49^{o}	10	61^{b}	11	67^{b}
12	73^{b}	13	78^{s}	14	81^{s}
15	83^{s}	16	85^{s}	17	87^{s}
18	89^{s}	63	91^{3}	64	97^{3}
79	103^{3}	80	105^{2}	87	109^{3}
99	115^{2}	100	117^{2}	103	120^{3}
109	121^{2}	112	123^{3}	119	125^{3}
120	126^{3}	127	127^{3}	135	129^{3}
143	131^{3}	497	133^{3}	504	139^{3}

$\kappa(N;2,8)$					
9	64^{o}	11	78^{a}	12	85^{b}
13	92^{b}	14	99^{b}	15	106^{b}
17	111^{s}	18	115^{s}	19	117^{s}
80	120^{3}	81	127^{3}	90	134^{3}
99	136^{2}	107	141^{3}	116	148^{3}
121	150^{2}	125	155^{3}	132	157^{2}
143	162^{2}	151	167^{3}	155	169^{2}
160	171^{3}	170	173^{3}	712	176^{3}
720	183^{3}	808	190^{3}	891	192^{3}

$\kappa(N;2,9)$					
10	81^{o}	13	105^{b}	14	113^{b}
15	121^{b}	16	129^{b}	17	137^{b}
18	145^{b}	99	153^{3}	100	161^{3}
129	177^{3}	139	185^{3}	140	191^{2}
149	193^{3}	168	201^{2}	181	209^{2}
182	215^{2}	195	217^{2}	196	223^{2}
981	225^{3}	990	233^{3}	1000	241^{3}
1278	249^{3}	1377	257^{3}	1400	263^{3}
1476	265^{3}	1665	273^{2}	1794	281^{2}

$\kappa(N;2,10)$					
4	100^{o}	6	101^{s}	13	120^{p}
15	136^{b}	16	145^{b}	17	154^{b}
18	163^{b}	19	172^{b}	20	174^{u}
21	190^{b}	24	191^{2}	35	192^{3}
36	201^{2}	52	210^{2}	78	211^{2}
89	227^{3}	169	230^{2}	195	246^{2}
208	255^{2}	224	262^{2}	239	271^{2}
255	280^{2}	260	284^{2}	271	289^{2}
288	298^{2}	312	301^{2}	468	302^{3}

$\kappa(N;3,2)$					
4	8^{o}	5	10^{n}	11	12^{y}
12	15^{t}	14	16^{y}	16	17^{y}
20	18^{ℓ}	22	19^{ℓ}	24	22^{ℓ}
28	23^{ℓ}	32	24^{ℓ}	40	25^{ℓ}
44	27^{ℓ}	48	30^{ℓ}	56	31^{ℓ}
64	32^{ℓ}	70	33^{ℓ}	80	34^{ℓ}
88	36^{ℓ}	96	39^{ℓ}	112	40^{ℓ}
128	41^{ℓ}	140	42^{ℓ}	160	44^{ℓ}
176	46^{ℓ}	192	49^{ℓ}	224	50^{ℓ}

$\kappa(N;3,3)$					
4	27^{o}	6	33^{n}	7	40^{f}
8	45^{ℓ}	9	50^{s}	10	51^{v}
12	57^{ℓ}	13	62^{s}	14	64^{ℓ}
15	68^{s}	16	69^{s}	17	73^{s}
18	74^{s}	22	75^{v}	23	82^{s}
25	85^{s}	27	87^{s}	29	91^{s}
30	93^{s}	32	95^{s}	34	98^{s}
37	99^{v}	38	102^{s}	39	104^{s}
40	105^{ℓ}	41	106^{s}	42	107^{s}

$\kappa(N;3,4)$					
6	64^{o}	8	88^{n}	10	112^{ℓ}
12	121^{ℓ}	16	124^{v}	20	160^{m}
24	169^{m}	34	184^{v}	40	232^{m}
64	244^{v}	68	283^{ℓ}	80	284^{ℓ}
96	301^{m}	120	304^{v}	136	331^{m}
222	364^{v}	236	406^{m}	256	409^{m}
272	448^{m}	276	449^{m}	320	452^{ℓ}
384	461^{ℓ}	464	472^{m}	480	481^{m}
544	506^{ℓ}	560	541^{m}	576	544^{m}

$\kappa(N;3,5)$					
6	125^{o}	10	185^{n}	12	225^{ℓ}
24	245^{v}	30	325^{m}	48	365^{v}
50	433^{m}	55	477^{m}	95	485^{v}
120	525^{m}	144	570^{ℓ}	160	605^{v}
175	645^{m}	205	661^{m}	210	673^{m}
240	677^{m}	250	753^{m}	264	774^{ℓ}
288	790^{ℓ}	295	813^{m}	325	817^{m}
355	825^{m}	385	829^{m}	415	833^{m}
450	837^{m}	475	841^{m}	576	850^{ℓ}

$\kappa(N;4,2)$					
5	16^{o}	6	21^{u}	10	24^{f}
12	48^{r}	14	53^{r}	16	54^{r}
20	55^{r}	25	80^{q}	28	91^{r}
30	92^{r}	32	94^{r}	40	96^{r}
81	120^{q}	88	178^{r}	96	181^{r}
112	182^{r}	128	183^{r}	140	184^{r}
160	189^{r}	162	191^{r}	176	249^{r}
189	252^{r}	192	253^{r}	224	257^{r}
252	259^{r}	256	263^{r}	280	265^{r}

$\kappa(N;4,3)$					
5	81^{o}	6	115^{s}	7	133^{s}
8	153^{s}	10	159^{v}	16	237^{v}
23	315^{v}	30	393^{v}	39	471^{v}
51	549^{v}	54	718^{r}	58	726^{r}
60	730^{r}	66	735^{r}	69	749^{r}
74	822^{r}	76	828^{r}	78	832^{r}
81	837^{r}	87	881^{r}	90	885^{r}
92	934^{r}	96	936^{r}	102	944^{r}
111	975^{r}	114	981^{r}	117	985^{r}

$\kappa(N;5,2)$						$\kappa(N;5,3)$					
6	32^o	8	56^u	10	62^v	6	243^o	7	377^s	8	457^s
12	92^v	14	110^v	16	152^v	10	483^v	13	723^v	16	963^v
17	176^v	20	194^j	24	261^i	19	1203^v	20	1530^i	26	2007^j
28	287^i	32	330^i	34	357^j	32	2247^j	38	2643^j	40	2970^j
40	375^j	64	392^q	81	434^q	46	3555^j	48	3711^j	52	3765^j
144	644^q	162	734^j	169	770^q	60	4005^j	64	4113^q	81	4347^q
176	1002^j	192	1005^j	224	1006^j	86	5733^j	92	5787^j	96	5943^j
252	1007^j	256	1025^j	280	1026^j	102	5997^j	104	6335^j	169	6507^q
288	1031^j	320	1121^j	324	1123^j	256	8667^q	258	9945^j	264	9949^j

10.23 Table The authorities used in Table 10.22 are:

2	[566, Theorem 2.2]	3	[566, Theorem 2.3]
a	1-rotational [1582, 1583]	b	1-rotational [566] and Colbourn (unpublished)
d	derivation	f	constraint programming [1111]
h	perfect hash family [1531]	i	Roux-type doubling [1531]
j	Roux-type doubling [1530]	ℓ	Roux-type [519]
m	Roux-type [567]	n	nearly resolvable design [460]
o	orthogonal array [1074]	p	projection [531]
q	Turán squaring [1061]	r	Roux-type [567]
s	simulated annealing [517]	t	tabu search [1688]
v	permutation vector [2102]	y	binary construction [1927]
z	composition	$\downarrow$	symbol identification

See Also

§III.3	MOLS and transversal designs of index one give covering arrays of strength two.
§III.7	Orthogonal arrays of strength t and index one give covering arrays.
[530, 1061]	Surveys on covering array applications and constructions.
[264]	Covering arrays CA$(t,k,2)$ arise from (k,t)-universal sets.
[1884]	Covering arrays of strength t are *t-surjective arrays*.

References Cited: [264, 367, 460, 516, 517, 519, 530, 531, 566, 567, 1061, 1074, 1111, 1530, 1531, 1582, 1583, 1688, 1756, 1884, 1927, 2102]

11 Coverings

Daniel M. Gordon
Douglas R. Stinson

11.1 Definitions and Examples

11.1 Let $v \geq k \geq t$. A t-(v,k,λ) *covering* is a pair $(X,\mathcal{B})$, where X is a v-set of elements (*points*) and $\mathcal{B}$ is a collection of k-subsets (*blocks*) of X, such that every t-subset of points occurs in at least λ blocks in $\mathcal{B}$. Repeated blocks in $\mathcal{B}$ are permitted.

11.2 The *covering number* $C_\lambda(v,k,t)$ is the minimum number of blocks in any t-(v,k,λ) covering. A t-(v,k,λ) covering $(X,\mathcal{B})$ is *optimal* if $|\mathcal{B}| = C_\lambda(v,k,t)$. If $\lambda = 1$, then write $C(v,k,t)$ for $C_1(v,k,t)$.

11.3 Examples Optimal coverings for certain parameter sets t-(v,k,λ).

t-(v,k,λ)	Covering
2-(5, 3, 1)	{1,2,3}, {1,4,5}, {2,3,4}, {2,3,5}
2-(6, 3, 1)	{0+i,1+i,3+i} modulo 6
2-(8, 3, 1)	{0+i,1+i,3+i} modulo 7, {0,1,∞}, {2,3,∞}, {4,5,∞}, {5,6,∞}
2-(6, 4, 1)	{1,2,3,4}, {1,2,5,6}, {3,4,5,6}
2-(9, 4, 1)	{1,2,3,4}, {1,2,5,6}, {1,7,8,9}, {2,4,6,8}, {2,7,8,9}, {3,5,8,9}, {3,6,7,9}, {4,5,7,9}

11.4 Remark The survey paper by Mills and Mullin [1614] covers much of the material in this chapter, and gives extensive references. A web site containing current bounds is `http://www.ccrwest.org/cover.html`. It also gives references to recent results.

11.2 Equivalent Combinatorial Objects

11.5 Theorem A t-(v,k,λ) covering with $\lambda\binom{v}{t}/\binom{k}{t}$ blocks is equivalent to a t-(v,k,λ) design or a Steiner system $S_\lambda(t,k,v)$ (possibly containing repeated blocks).

11.6 Let $v \geq m \geq k$. A (v,m,k) *Turán system* is a pair $(X,\mathcal{B})$, where X is a v-set of elements (*points*) and $\mathcal{B}$ is a collection of k-subsets (*blocks*) of X, such that every m-subset of points is a superset of at least one block $B \in \mathcal{B}$.

11.7 The *Turán number* $T(v,m,k)$ is the minimum number of blocks in any (v,m,k) Turán system.

11.8 Theorem $(X,\mathcal{B})$ is a (v,m,k) *Turán design* if and only if $(X, \{X\backslash B : B \in \mathcal{B}\})$ is a $(v-m)$-$(v,v-k,1)$ covering.

11.9 Corollary $T(v,m,k) = C(v,v-k,v-m)$.

11.10 An *(n,u,v,d) constant weight covering code* is a code of length n, constant weight u, such that every word with weight v is within Hamming distance d of at least one codeword. $K(n,u,v,d)$ is the minimum size of such a code.

11.11 Theorem For $u - v \geq 0$, a $(n,u,v,u-v)$ constant weight covering code is a (n,u,v) covering design.

11.12 Corollary For $u - v \geq 0$, $K(n,u,v,u-v) = C(n,u,v)$.

11.13 An (n,k,p,t)-*lottery scheme* is a set of k-element subsets (*blocks*) of an n-set such that each p-subset intersects some block in at least t elements.

11.14 Theorem A (v,k,t,t)-lottery scheme is a t-$(v,k,1)$ covering design.

11.15 A *quorum system* is a pair $(X,\mathcal{A})$, where X is a v-set of elements, and $\mathcal{A}$ is a collection of subsets (*quorums*) of X such that any two quorums in $\mathcal{A}$ have a nonempty intersection.

11.16 Remark Quorum systems are used to maintain consistency in distributed systems. Connections between quorum systems and coverings are given in [547].

11.17 A *directed* t-(v,k,λ) *covering* is a pair $(X,\mathcal{B})$, where X is a v-set of elements, and $\mathcal{B}$ is a collection of *ordered* subsets of X such that every ordered t-subset of X occurs, in the same order, at least λ times.

11.18 Remark A directed t-(v,k,λ) covering is a standard t-$(v,k,t!\,\lambda)$ covering. The size of a directed t-(v,k,λ) covering is denoted $DC_\lambda(v,k,t)$. See [116] for recent results on these numbers.

11.3 Lower Bounds

11.19 Theorem (*Schönheim bound*) $C_\lambda(v,k,t) \geq \lceil v\, C_\lambda(v-1,k-1,t-1)/k \rceil$. Iterating this bound yields $C_\lambda(v,k,t) \geq L_\lambda(v,k,t)$, where

$$L_\lambda(v,k,t) = \left\lceil \frac{v}{k} \left\lceil \frac{v-1}{k-1} \cdots \left\lceil \frac{\lambda(v-t+1)}{k-t+1} \right\rceil \right\rceil \right\rceil .$$

Write $L(v,k,t)$ for $L_1(v,k,t)$.

11.20 Theorem (Hanani) If $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 1 \pmod{k}$, then

$$C_\lambda(v,k,2) \geq L_\lambda(v,k,2) + 1.$$

11.21 $B_\lambda(v,k,t)$ denotes the lower bound implied by Theorems 11.19 and 11.20, (either $L_\lambda(v,k,t)$ or $L_\lambda(v,k,t)+1$). Write $B(v,k,t)$ for $B_1(v,k,t)$.

11.22 Theorem [439] For any k there is a $v_0 = v_0(k)$ such that $C(v,k,2) = B(v,k,2)$ for all $v > v_0$.

11.23 Table Aside from the Schönheim bound, most lower bound results in the literature are for individual covering numbers and typically require analysis of many cases or extensive computer searches. This table gives some recent results, all for $\lambda = 1$. References are given at `http://www.ccrwest.org/cover.html`. Values known to be exact are in **bold**.

v	k	t	lower bound	v	k	t	lower bound	v	k	t	lower bound
19	6	2	**15**	19	13	4	**11**	15	11	6	**21**
28	9	2	**14**	11	6	5	96	16	12	6	**19**
41	13	2	**14**	11	7	5	33	17	13	6	**17**
14	7	3	**15**	13	9	5	**19**	21	16	6	**17**
13	8	3	**10**	16	12	5	**12**	12	8	7	**126**
15	9	3	**10**	18	13	5	**15**	13	10	7	**30**
17	10	3	**11**	19	14	5	**14**	18	14	7	**24**
10	5	4	**51**	21	16	5	**12**	13	9	8	**185**
16	11	4	**12**	11	7	6	**84**	14	11	8	**40**
18	12	4	**12**	12	7	6	165	20	16	8	**26**

11.4 Determination of Covering Numbers

11.24 Theorem $C_\lambda(v,3,2) = B_\lambda(v,3,2)$.

11.25 Theorem $C(v,4,2) = L(v,4,2) + \epsilon$, where

$$\epsilon = \begin{cases} 1 & \text{if } v = 7, 9, \text{ or } 10 \\ 2 & \text{if } v = 19 \\ 0 & \text{otherwise.} \end{cases}$$

11.26 Theorem If $\lambda > 1$, then $C_\lambda(v,4,2) = L_\lambda(v,4,2)$.

11.27 Theorem $C(v,4,3) = L(v,4,3)$ except for $v = 7$ and possible exceptions of $v = 12k+7$ with $k \in \{1,2,3,4,5,7,8,9,10,11,12,16,21,23,25,29\}$.

11.28 Theorem $C(v,5,2) = B(v,5,2)$ except possibly when

1. $v = 15$,
2. $v \equiv 0 \pmod 4$, $v \le 280$
3. $v \equiv 9 \pmod{20}$, $v \le 429$,
4. $v \equiv 17 \pmod{20}$, $v \le 377$,
5. $v \equiv 13 \pmod{20}$, $v \in \{13, 53, 73\}$.

11.29 Theorem For $\lambda > 1$, $C_\lambda(v,5,2) = B_\lambda(v,5,2)$, except possibly when $\lambda = 2$ and $v \in \{9, 13, 15, 53, 63, 73, 83\}$, $v = 44$ and $\lambda \equiv 13 \pmod{20}$, or $v = 44$ and $\lambda = 17$.

11.30 Remark Theorem 11.29 is a recent result of Bluskov and Greig. The only cases with $\lambda > 1$ where $C_\lambda(v,5,2)$ is known to be greater than $B_\lambda(v,5,2)$ are when $\lambda = 2$ and $v \in \{9, 13, 15\}$.

11.31 Theorem The values $C(v,k,2)$ are known in the following cases:

1. $C(v,k,2) = 3$ for $1 < v/k \le 3/2$;
2. $C(v,k,2) = 4$ for $3/2 < v/k \le 5/3$;
3. $C(v,k,2) = 5$ for $5/3 < v/k \le 9/5$;
4. $C(v,k,2) = 6$ for $9/5 < v/k \le 2$;
5. $C(v,k,2) = 7$ for $2 < v/k \le 7/3$, except when $3v = 7k - 1$;
6. $C(v,k,2) = 8$ for $7/3 < v/k \le 12/5$, except when $12k - 5v = 0, 1$ and $v - k$ is odd;
7. $C(v,k,2) = 9$ for $12/5 < v/k \le 5/2$, except when $2v = 5k$ and $v - k$ is odd;
8. $C(v,k,2) = 10$ for $5/2 < v/k \le 8/3$, except when $8k - 3v \in \{0, 1\}$, $v - k$ is odd, and $k > 2$;
9. $C(v,k,2) = 11$ for $8/3 < v/k \le 14/5$, except when $14k - 5v \in \{0, 1\}$, $v - k$ is odd, and $k > 4$;
10. $C(v,k,2) = 12$ for $14/5 < v/k \le 3$, except when $v = 3k$, $k \not\equiv 0 \pmod 3$, and $k \not\equiv 0 \pmod 4$.
11. $C(v,k,2) = 13$ for $3 < v/k \le 13/4$, except for
    (a) $C(13r + 2, 4r + 1, 2) = 14, r \ge 2$,
    (b) $C(13r + 3, 4r + 1, 2) = 14, r \ge 2$,
    (c) $C(13r + 6, 4r + 2, 2) = 14, r \ge 2$,
    (d) $C(19, 6, 2) = 15$,
    (e) $C(16, 5, 2) = 15$.

11.32 Remark The exceptional cases are all known, and one block larger. The result on 13 blocks is recent and due to Greig, Li, and van Rees.

11.33 Table Upper bounds on $C(v,k,2)$ for $v \le 32$ and $k \le 16$. Values known to be exact are in **bold**. All other values are one more than the lower bound.

$t = 2$

$v\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	**1**													
4	**3**	**1**												
5	**4**	**3**	**1**											
6	**6**	**3**	**3**	**1**										
7	**7**	**5**	**3**	**3**	**1**									
8	**11**	**6**	**4**	**3**	**3**	**1**								
9	**12**	**8**	**5**	**3**	**3**	**3**	**1**							
10	**17**	**9**	**6**	**4**	**3**	**3**	**3**	**1**						
11	**19**	**11**	**7**	**6**	**4**	**3**	**3**	**3**	**1**					
12	**24**	**12**	**9**	**6**	**5**	**3**	**3**	**3**	**3**	**1**				
13	**26**	**13**	**10**	**7**	**6**	**4**	**3**	**3**	**3**	**3**	**1**			
14	**33**	**18**	**12**	**7**	**6**	**5**	**4**	**3**	**3**	**3**	**3**	**1**		

$v\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14	15	16
15	**35**	**19**	**13**	**10**	**7**	**6**	**4**	**3**	**3**	**3**	**3**	**3**	**1**	
16	**43**	**20**	**15**	**10**	**8**	**6**	**5**	**4**	**3**	**3**	**3**	**3**	**3**	**1**
17	**46**	**26**	**16**	**12**	**9**	**7**	**6**	**5**	**4**	**3**	**3**	**3**	**3**	**3**
18	**54**	**27**	**18**	**12**	**10**	**7**	**6**	**5**	**4**	**3**	**3**	**3**	**3**	**3**
19	**57**	**31**	**19**	**15**	**11**	**9**	**7**	**6**	**5**	**4**	**3**	**3**	**3**	**3**
20	**67**	**35**	**21**	**16**	**12**	**9**	**7**	**6**	**6**	**4**	**4**	**3**	**3**	**3**
21	**70**	**37**	**21**	**17**	**13**	**11**	**7**	**7**	**6**	**5**	**4**	**3**	**3**	**3**
22	**81**	**39**	**27**	**19**	**13**	**11**	**9**	**7**	**6**	**6**	**5**	**4**	**3**	**3**
23	**85**	**46**	**28**	21	16	**12**	**10**	**8**	**7**	**6**	**5**	**4**	**4**	**3**
24	**96**	**48**	**30**	22	**17**	**12**	**11**	**8**	**7**	**6**	**6**	**5**	**4**	**3**
25	**100**	**50**	**30**	**23**	**18**	**13**	**11**	**10**	**7**	**7**	**6**	**5**	**4**	**4**
26	**113**	**59**	**37**	**24**	**19**	**13**	**12**	**10**	**8**	**7**	**6**	**6**	**5**	**4**
27	**117**	**61**	**38**	**27**	**20**	17	**12**	**11**	**9**	**7**	**7**	**6**	**5**	**5**
28	**131**	**63**	**40**	**28**	22	**17**	**14**	**11**	**10**	**7**	**7**	**6**	**6**	**5**
29	**136**	**73**	43	30	23	**18**	**14**	**12**	**10**	**9**	**7**	**7**	**6**	**6**
30	**150**	**75**	**48**	**31**	25	**19**	**15**	**13**	**11**	**9**	**8**	**7**	**6**	**6**
31	**155**	**78**	**50**	**31**	**26**	**20**	17	**13**	**12**	**10**	**8**	**7**	**7**	**6**
32	**171**	**88**	**52**	**38**	**28**	**20**	18	**14**	**12**	**10**	**9**	**7**	**7**	**6**

11.34 Theorem (Mills) The values $C(v,k,3)$ are known in the following cases:

1. $C(v,k,3) = 4$ for $1 < v/k \le 4/3$;
2. $C(v,k,3) = 5$ for $4/3 < v/k \le 7/5$;
3. $C(v,k,3) = 6$ for $7/5 < v/k \le 3/2$, except when $2v = 3k$ and v is odd;
4. $C(v,k,3) = 7$ for $3/2 < v/k \le 17/11$, except when $11v = 17k - 1$;
5. $C(v,k,3) = 8$ for $17/11 < v/k \le 8/5$, except when $5v = 8k - 1$ and $k > 7$.

11.35 Table Upper bounds on $C(v,k,3)$ for $v \le 32$ and $k \le 16$. Values known to be exact are in **bold**.

$t = 3$

$v\backslash k$	4	5	6	7	8	9	10	11	12	13	14	15	16
4	**1**												
5	**4**	**1**											
6	**6**	**4**	**1**										
7	**12**	**5**	**4**	**1**									
8	**14**	**8**	**4**	**4**	**1**								
9	**25**	**12**	**7**	**4**	**4**	**1**							
10	**30**	**17**	**10**	**6**	**4**	**4**	**1**						
11	**47**	**20**	**11**	**8**	**5**	**4**	**4**	**1**					
12	**57**	29	**15**	**11**	**6**	**4**	**4**	**4**	**1**				
13	**78**	34	21	**13**	**10**	**6**	**4**	**4**	**4**	**1**			
14	**91**	43	25	**15**	**11**	**8**	**5**	**4**	**4**	**4**	**1**		
15	**124**	56	31	**15**	**13**	**10**	**7**	**5**	**4**	**4**	**4**	**1**	
16	**140**	65	38	24	**14**	**11**	**8**	**6**	**4**	**4**	**4**	**4**	**1**
17	**183**	**68**	44	27	18	**13**	**11**	**7**	**6**	**4**	**4**	**4**	**4**
18	**207**	**94**	**48**	33	**21**	16	12	10	**6**	**5**	**4**	**4**	**4**
19	258	108	60	35	27	17	14	11	**9**	**6**	**5**	**4**	**4**
20	**285**	133	71	45	**28**	21	15	12	10	**8**	**6**	**4**	**4**
21	**352**	151	77	49	35	24	18	14	**11**	**9**	**7**	**5**	**4**
22	**385**	172	**77**	59	38	29	19	15	**11**	11	**8**	**6**	**5**
23	**466**	187	**104**	67	40	32	24	**15**	14	**11**	10	**7**	**6**
24	**510**	231	116	78	50	35	**24**	20	**14**	13	11	**8**	**6**
25	**600**	256	130	83	57	38	30	23	17	14	12	10	**8**
26	**650**	**260**	**130**	94	65	39	33	26	18	15	13	11	**9**
27	**763**	**319**	**167**	105	74	**39**	36	27	22	**15**	14	**11**	11
28	**819**	362	188	124	79	56	36	32	24	19	15	13	11
29	**950**	418	221	134	91	59	42	33	27	21	**15**	**14**	12
30	**1020**	462	225	142	97	66	46	37	30	24	**15**	15	13
31	1165	517	273	153	105	74	48	39	32	26	21	**15**	**14**
32	**1240**	579	300	169	106	78	60	40	**32**	29	23	18	**14**

11.36 Table Upper bounds on $C(v,k,4)$ for $v \le 32$ and $k \le 16$. Values known to be exact are in **bold**.

$t = 4$

$v\backslash k$	5	6	7	8	9	10	11	12	13	14	15	16
5	**1**											
6	**5**	**1**										
7	**9**	**5**	**1**									
8	**20**	**7**	**5**	**1**								
9	**30**	**12**	**6**	**5**	**1**							
10	**51**	**20**	**10**	**5**	**5**	**1**						
11	**66**	**32**	**17**	**9**	**5**	**5**	**1**					
12	**113**	41	24	**12**	**8**	**5**	**5**	**1**				
13	157	66	30	**18**	**10**	**7**	**5**	**5**	**1**			
14	230	80	44	24	**16**	**9**	**6**	**5**	**5**	**1**		
15	295	117	57	30	20	14	**8**	**5**	**5**	**5**	**1**	
16	405	152	76	**30**	26	18	**12**	**7**	**5**	**5**	**5**	**1**
17	491	188	99	53	28	23	15	**10**	**7**	**5**	**5**	**5**
18	664	236	126	66	38	26	19	**12**	**9**	**6**	**5**	**5**
19	846	325	152	84	48	32	23	17	**11**	**9**	**6**	**5**
20	1083	386	202	93	63	36	28	20	16	**10**	**8**	**5**
21	1251	490	237	127	75	51	31	25	18	14	**9**	**7**
22	1573	580	252	157	97	54	38	28	22	17	12	**9**
23	**1771**	720	**253**	196	109	77	42	31	25	20	15	11
24	**2237**	784	**357**	234	122	89	59	31	28	23	18	12
25	2706	992	440	263	168	98	70	47	30	27	21	17
26	3222	1154	558	298	198	119	82	55	37	28	24	18
27	3775	**1170**	670	350	216	138	99	65	42	31	27	22
28	4501	**1489**	817	428	267	160	109	79	55	31	29	24
29	5229	1803	956	512	314	198	119	94	68	43	31	28
30	5956	2220	1102	560	366	231	144	102	74	50	31	29
31	6595	2627	1176	617	435	278	165	115	80	63	**31**	30
32	7703	3119	1440	620	479	323	184	132	101	67	52	**30**

11.37 Table Upper bounds on $C(v,k,5)$ for $v \le 32$ and $k \le 16$. Values known to be exact are in **bold**.

$t = 5$

$v\backslash k$	6	7	8	9	10	11	12	13	14	15	16
6	**1**										
7	**6**	**1**									
8	**12**	**6**	**1**								
9	**30**	**9**	**6**	**1**							
10	**50**	**20**	**8**	**6**	**1**						
11	100	34	**16**	**7**	**6**	**1**					
12	**132**	59	**26**	**12**	**6**	**6**	**1**				
13	**245**	78	42	**19**	**11**	**6**	**6**	**1**			
14	371	138	55	32	**14**	**10**	**6**	**6**	**1**		
15	579	189	89	42	27	**13**	**9**	**6**	**6**	**1**	
16	808	283	117	61	34	22	**12**	**8**	**6**	**6**	**1**
17	1213	405	178	79	48	30	**17**	**11**	**7**	**6**	**6**
18	1547	583	256	113	54	42	24	**15**	**9**	**6**	**6**
19	2175	706	356	149	83	49	37	21	**14**	**9**	**6**
20	2850	1003	492	220	108	65	42	33	18	**12**	**8**
21	3930	1320	603	271	145	79	56	38	28	16	**12**
22	4681	1701	723	378	190	110	64	48	34	22	14
23	6162	2044	757	489	263	131	85	56	44	30	20
24	**7084**	2710	**759**	615	297	204	86	67	49	38	24
25	**9321**	3163	**1116**	717	398	232	145	74	58	47	35
26	11952	4151	1452	830	514	273	175	103	66	54	41
27	15174	4680	2010	960	622	354	208	125	77	61	49
28	18369	**4680**	2551	1224	771	424	261	172	90	62	55
29	22870	**6169**	3180	1608	920	561	321	218	137	67	61
30	27136	7800	3998	2009	1123	644	379	255	162	102	62
31	32365	9953	4567	2418	1395	799	482	293	197	133	62
32	35882	12469	4820	2965	1649	1002	588	363	240	159	**62**

11.38 Theorem $C(v, v-1, t) = t+1$ for all t.

11.39 Theorem (Turán) Suppose $q = \left\lfloor \frac{v}{v-t-1} \right\rfloor$. Then $C(v, v-2, t) = qv - \binom{q+1}{2}(v-t-1)$.

11.5 Structure of Optimal Coverings

11.40 Let $(X, \mathcal{B})$ be a 2-$(v, k, 1)$ covering. The *excess graph* of $(X, \mathcal{B})$ is the multigraph (X, E), where each edge xy occurs with multiplicity $|\{B \in \mathcal{B} : \{x, y\} \subseteq B\}| - 1$.

11.41 Table Optimal 2-$(v, 3, 1)$ coverings.

$v \equiv$	$C(v, 3, 2)$	Excess Graph	Construction
$1, 3 \pmod 6$	$\frac{v^2 - v}{6}$	Empty	BIBD$(v, 3, 1)$
$0 \pmod 6$	$\frac{v^2}{6}$	$\frac{v}{2}K_2$	For $v \geq 18$, fill in each group of a $\{3\}$-GDD of type $6^{v/6}$ with an optimal covering on six points.
$2, 4 \pmod 6$	$\frac{v^2 + 2}{6}$	$K_{1,3} \cup \frac{v-4}{2}K_2$	For $v \equiv 4 \pmod 6$, $v \geq 22$, fill in each group of a $\{3\}$-GDD of type $6^{(v-4)/6}4^1$ with an optimal covering on four or six points; for $v \equiv 2 \pmod 6$, $v \geq 26$, fill in each group of a $\{3\}$-GDD of type $6^{(v-8)/6}8^1$ with an optimal covering on six or eight points.
$5 \pmod 6$	$\frac{v^2 - v + 4}{6}$	One edge of multiplicity 2	For $v \geq 11$, take a PBD$(v, \{3, 5^*\})$ on v points and fill in the block of size 5 with an optimal covering on five points.

11.42 Table Optimal 2-$(v, 4, 1)$ coverings, $v \notin \{7, 9, 10, 19\}$.

$v \equiv$	$C(v, 4, 2)$	Excess Graph	Construction
$1, 4 \pmod{12}$	$\frac{v^2 - v}{12}$	Empty	BIBD$(v, 4, 1)$
$0, 6 \pmod{12}$	$\frac{v^2}{12}$	$\frac{v}{2}K_2$	For $v \geq 30$, fill in each group of a $\{4\}$-GDD of type $6^{v/6}$ with an optimal covering on six points.
$3, 9 \pmod{12}$	$\frac{v^2 + 3}{12}$	$K_{1,4} \cup \frac{v-5}{2}K_2$	For $v \geq 51$, fill in each group of a $\{4\}$-GDD of type $6^{(v-15)/6}15^1$ with an optimal covering on six or fifteen points.
$7, 10 \pmod{12}$	$\frac{v^2 - v + 6}{12}$	One edge of multiplicity three	Take a PBD$(v, \{4, 22^*\})$ and replace the block of size 22 by an optimal covering on 22 points.

$v \equiv$	$C(v,4,2)$	Excess Graph	Construction
$8, 11 \pmod{12}$	$\dfrac{v^2+v}{12}$	A 2-regular multigraph on v points	Take an optimal covering on $v-1$ points in which the pair 12 occurs four times, and in which $\{1,2,3,4\}$ is a block. Then replace the block $\{1,2,3,4\}$ by the two blocks $\{1,3,4,v\}$ and $\{2,3,4,v\}$. Finally, adjoin new blocks $\{5,6,7,v\}, \ldots, \{v-3, v-2, v-1, v\}$.
$2, 5 \pmod{12}$	$\dfrac{v^2+v+6}{12}$	A multigraph on v points in which two vertices have degree 5 and the remaining $v-2$ vertices have degree 2, or one in which one vertex has degree 8 and the remaining $v-1$ vertices have degree 2	Take a BIBD$(v-1,4,1)$ and adjoin new blocks $\{1,2,3,v\}$, $\{4,5,6,v\}$, $\ldots$, $\{v-4, v-3, v-2, v\}$, and $\{v-3, v-2, v-1, v\}$.

11.6 Resolvable Coverings with $\lambda = 1$

11.43 A t-(v,k,λ) covering $(X,\mathcal{B})$ is *resolvable* if $\mathcal{B}$ can be partitioned into *parallel classes*, each of which consists of v/k disjoint blocks.

11.44 Example [1393] A resolvable 2-$(24,4,1)$ covering on $48 = L(24,4,2)$ blocks. Let $X = \mathbb{Z}_3 \times \{0,\ldots,7\}$. Three parallel classes are formed by developing the following class modulo 3:

$\{(0,0),(1,0),(1,1),(0,2)\}$ $\{(2,0),(2,3),(0,4),(0,6)\}$ $\{(0,1),(1,2),(0,3),(1,3)\}$
$\{(2,1),(2,2),(0,5),(0,7)\}$ $\{(1,4),(1,5),(2,6),(2,7)\}$ $\{(2,4),(2,5),(1,6),(1,7)\}$.

Three more parallel classes are formed by developing the following class modulo 3:

$\{(0,0),(2,1),(0,4),(2,4)\}$ $\{(1,0),(2,3),(1,5),(2,5)\}$ $\{(2,0),(1,3),(1,7),(2,7)\}$
$\{(0,1),(1,1),(1,6),(0,7)\}$ $\{(0,2),(1,2),(1,4),(0,5)\}$ $\{(2,2),(0,3),(0,6),(2,6)\}$.

The seventh parallel class is formed by developing the following two blocks modulo 3:

$$\{(0,0),(0,1),(2,5),(2,6)\}\ \{(0,2),(0,3),(2,4),(2,7)\}.$$

Finally, the eighth parallel class is formed by developing the following two blocks modulo 3: $\{(0,0),(1,2),(0,6),(1,7)\}$ $\{(0,1),(2,3),(2,4),(0,5)\}$.

11.45 Theorem Suppose $v \equiv 0 \pmod{k}$. If $v-1 \equiv 0 \pmod{(k-1)}$, then a resolvable 2-$(v,k,1)$ covering with $L(v,k,2)$ blocks is equivalent to a RBIBD$(v,k,1)$.

11.46 Theorem There exists a resolvable 2-$(v,3,1)$ covering having $L(v,3,2)$ blocks for all $v \equiv 0 \pmod{6}$, $v \geq 18$.

11.47 Theorem [9, 1393] There exists a resolvable 2-$(v,4,1)$ covering having $L(v,4,2)$ blocks for all $v \equiv 0 \pmod{4}$, $v \neq 12$, except possibly when $v \in \{108, 116, 132, 156, 204, 212\}$.

11.48 Let $r(q,k)$ denote the minimum number of parallel classes in a resolvable 2-$(kq,k,1)$ covering.

11.49 Theorem (Haemers) $r(q,k) \geq q+1$. Further, equality holds if and only if q divides k and q is the order of an affine plane.

11.50 Theorem (Haemers) Suppose that q is the order of an affine plane, and k is a positive integer such that $\lceil k/q \rceil \leq 2k/(2q-1)$. Then $r(q,k) \leq q+2$.

11.51 Theorem [2084] The following values of $r(q,k)$ for small q are known:

1. $r(2,k) = 3$ if k is even, 4 if k is odd;
2. $r(3,k) = 4$ if $k \equiv 0 \pmod 3$, 5 otherwise; and
3. $r(4,k) = 5$ if $k \equiv 0 \pmod 4$, 7 if $k \in \{2,3\}$, and 6 otherwise.

11.52 A resolvable 2-$(kq,k,1)$ covering is *equitable* if every pair of points occurs in either one or two blocks.

11.53 Theorem Let $s = (qk-1)/(k-1)$. If an equitable resolvable 2-$(kq,k,1)$ covering with r parallel classes exists, then $s \le r \le 2s$.

11.54 Theorem If an equitable resolvable 2-$(kq,k,1)$ covering exists, then

$$k < 2q - \sqrt{2q - 9/4}.$$

See Also

§II.1	BIBDs are coverings with void excess graph.
§III.4	Incomplete transversal designs are used extensively in various constructions for coverings.
§IV.4	Pairwise balanced designs and group divisible designs.
§VI.20	Directed coverings.
§VI.63	t-wise balanced designs.
§VI.32	Gives the connections among coverings, Turán designs, and lottery schemes.
[1614]	Survey of coverings and packings with an extensive bibliography. `http://www.ccrwest.org/cover.html` gives numerical results and tables of the best known coverings.
[2084]	Information on resolvable coverings.
[932]	Computational methods for coverings.

References Cited: [9, 116, 439, 547, 932, 1393, 1614, 2084]

12 Cycle Decompositions

Darryn Bryant
Chris Rodger

12.1 Definitions and Example

12.1 A (*directed*) *cycle decomposition* of a (directed) graph G is a collection of (directed) cycles whose edges partition the (directed) edges of G. If all the cycle have length m the notation *m-cycle decomposition* is used.

12.2 λK_n is the undirected graph on n vertices in which each pair of vertices is joined by exactly λ edges. For n even, $\lambda K_n - I$ is the graph obtained from λK_n by removing the $n/2$ edges in the 1-factor I. λK_n^* is the directed graph on n vertices in which, for each ordered pair of vertices (u,v), there are exactly λ arcs joining u to v.

12.3 A (*directed*) *m-cycle system of order n and index λ* is a (directed) m-cycle decomposition of λK_n (λK_n^*).

12.4 For m-cycle systems of λK_n, n is (m,λ)-*admissible* if m divides $\lambda n(n-1)/2$, $\lambda(n-1)$ is even, λ is even when $m = 2$, and either $n = 1$ or $n \geq m$. For directed m-cycle systems of λK_n^*, n is $(m,\lambda)^*$-*admissible* if m divides $\lambda n(n-1)$ and either $n = 1$ or $n \geq m$.

12.5 Example A 5-cycle system of order 11 and index 1.

$$C = \{(1+i, 2+i, 5+i, 3+i, 8+i) | i \in \mathbb{Z}_{11}\}.$$

12.2 Existence and Enumeration

12.6 Theorem (see [83]) For $\lambda = 1, 2$ and $m \geq 2$, there exists an m-cycle system of λK_n if and only if n is (m,λ)-admissible. For all $m \geq 2$, there exists a directed m-cycle system of K_n^* if and only if n is $(m,1)^*$-admissible and $(m,n) \neq (4,4), (3,6), (6,6)$.

12.7 Remark If there exist (directed) m-cycle systems of $\lambda_1 K_n$ and $\lambda_2 K_n$ ($\lambda_1 K_n^*$ and $\lambda_2 K_n^*$), then there exists a (directed) m-cycle system of $(\lambda_1+\lambda_2)K_n$ ($(\lambda_1+\lambda_2)K_n^*$). If there exists a directed m-cycle systems of λK_n^*, then there exists an m-cycle system of $2\lambda K_n$. Other than the results one can obtain from Theorem 12.6 using these simple observations, the known existence results for m-cycle systems of λK_n and directed m-cycle systems of λK_n^* are included in Theorem 12.8.

12.8 Theorem (see [1460]) For $\lambda \geq 3$, $2 \leq m \leq 14$, and $m = 16$, there exists an m-cycle system of λK_n if and only if n is (m,λ)-admissible. For $\lambda \geq 2$, $2 \leq m \leq 8$, and $m = 10, 12, 14$, there exists a directed m-cycle system of λK_n^* if and only if n is $(m,\lambda)^*$-admissible and $n \neq 4$ when $m = 4$ and λ is odd.

12.9 Conjecture (Alspach, see [149]) Let $3 \leq m_1, m_2, \ldots, m_t \leq n$, $m_1 + m_2 + \cdots + m_t = n(n-1)/2$ if n is odd, and $m_1 + m_2 + \cdots + m_t = n(n-2)/2$ if n is even. Then there exists a cycle decomposition of K_n, if n is odd, and of $K_n - I$, if n is even, into t cycles of lengths $m_1, m_2, \ldots, m_t$.

12.10 Theorem Conjecture 12.9 holds in each of the following cases.

1. $m_1 = m_2 = \cdots = m_t$ (see [83]);
2. $n \geq N$ (N a large fixed constant) and $m_1, m_2, \ldots, m_t \leq \lfloor (n-112)/20 \rfloor$ [149];
3. $n \leq 14$ [149]; and
4. $\{m_1, m_2, \ldots, m_t\} \subseteq \{\{3,4,5\}, \{3,4,6\}, \{3,n\}, \{2^k, 2^{k+1}\}$ any $k \geq 2$, $\{4,10\}$, $\{6,8\}$, $\{6,10\}$, $\{8,10\}$, $\{n-2, n-1, n\}\}$ [62, 150, 364, 1083].

12.11 Remark Conjecture 12.9 asks for a decomposition of K_n or $K_n - I$ into cycles with specified numbers of edges. The following two theorems address similar problems where the requirement that the subgraphs be cycles is relaxed so that only 2-regular subgraphs or connected subgraphs with all vertices having even degree are required.

12.12 Theorem [362] Let $m_1, m_2, \ldots, m_t$ be integers. The complete graph K_n has a decomposition $\{G_1, G_2, \ldots, G_t\}$ where G_i is some 2-regular graph with m_i edges for $i = 1, 2, \ldots, t$ if and only if n is odd, $3 \leq m_1, m_2, \ldots, m_t \leq n$ and $m_1 + m_2 + \cdots + m_t = n(n-1)/2$.

12.13 Theorem [150] Let $m_1, m_2, \ldots, m_t$ be integers and let $e = m_1 + m_2 + \cdots + m_t$. There exists a subgraph of K_n having a decomposition $\{G_1, G_2, \ldots, G_t\}$ where G_i is some connected graph with exactly m_i edges and with all vertices having even degree if and only if $m_1, m_2, \ldots, m_t \geq 3$, $e = n(n-1)/2$ or $e \leq n(n-1)/2 - 3$ when n is odd, and $e \leq n(n-2)/2$ when n is even.

12.14 Table [666] The number N of nonisomorphic m-cycle systems of order n and index 1.

m	3	5	3	7	3	4	6	9
n	3	5	7	7	9	9	9	9
N	1	1	1	2	1	8	640	122

12.3 Decompositions into Isomorphic 2-Factors

12.15 A 2-*factor* in a graph G is a 2-regular spanning subgraph. A 2-*factorization* of a graph G is a partition of the edges of G into 2-factors.

12.16 Remark Petersen's Theorem (see [1822]) guarantees that every regular graph of even degree has a 2-factor and hence a 2-factorization.

12.17 Remark A connected 2-factor is a *hamiltonian cycle*. Results on decompositions into hamiltonian cycles are too numerous to cover here. See [624] for a survey.

12.18 Conjecture (Alspach, see [624]) Every connected Cayley graph of even degree on a finite abelian group has a decomposition into hamiltonian cycles.

12.19 Conjecture (Nash-Williams, see [1176]) Let G be a k-regular graph on n vertices with $k \geq \frac{n-1}{2}$. Then G has a decomposition into $\frac{k}{2}$ hamiltonian cycles when k is even, and a decomposition into $\frac{k-1}{2}$ hamiltonian cycles and a 1-factor when k is odd.

12.20 Remark Graphs satisfying the conditions of Conjecture 12.18 or Conjecture 12.19 contain at least one hamiltonian cycle.

12.21 The 2-regular graph consisting of exactly α_i m_i-cycles for $i = 1, 2, \ldots, t$ is denoted by $[m_1^{\alpha_1}, m_2^{\alpha_2}, \ldots, m_t^{\alpha_t}]$. A 2-factor with n vertices consisting entirely of m-cycles may be denoted by $[m^*]$ rather than $[m^{\frac{n}{m}}]$.

12.22 Let $n \geq 3$, let $G = K_n$ when n is odd and let $G = K_n - I$ when n is even. The problem of determining whether G has a 2-factorization in which each 2-factor is isomorphic to $[m_1^{\alpha_1}, m_2^{\alpha_2}, \ldots, m_t^{\alpha_t}]$ is the *Oberwolfach Problem* and is denoted by $\mathrm{OP}(m_1^{\alpha_1}, m_2^{\alpha_2}, \ldots, m_t^{\alpha_t})$.

12.23 Theorem Other than $\mathrm{OP}(3,3)$, $\mathrm{OP}(3,3,3,3)$, $\mathrm{OP}(4,5)$, and $\mathrm{OP}(3,3,5)$, none of which has a solution (see [1822]), the following Oberwolfach problems all have solutions.

1. $\mathrm{OP}(m^t)$ for all $t \geq 1$ and $m \geq 3$ (see [1474]);
2. $\mathrm{OP}(m_1^{\alpha_1}, m_2^{\alpha_2}, \ldots, m_t^{\alpha_t})$ for $\alpha_1 m_1 + \alpha_2 m_2 + \cdots + \alpha_t m_t \leq 17$ (see [1822]);
3. $\mathrm{OP}(3^k, 4)$ for all odd $k \geq 1$ [665];
4. $\mathrm{OP}(3^k, 5)$ for all even $k \geq 4$ [1994];
5. $\mathrm{OP}(r^k, n - kr)$ for $n \geq 6kr - 1$, $k \geq 1$, $r \geq 3$ [1101];
6. $\mathrm{OP}(r, n - r)$ for $r = 3, 4, 5, 6, 7, 8, 9$ and $n \geq r + 3$ [1101];
7. $\mathrm{OP}(r, r, n - 2r)$ for $r = 3, 4$ and $n \geq 2r + 3$ [1101];
8. $\mathrm{OP}(2r_1, 2r_2, \ldots, 2r_k)$ for all $r_i \geq 2$ and $r_1 + r_2 + \cdots + r_k$ odd [1010];
9. $\mathrm{OP}(r, r+1)$ and $\mathrm{OP}(r, r+2)$ for $r \geq 3$;
10. $\mathrm{OP}(2s+1, 2s+1, 2s+2)$ for $s \geq 1$;
11. $\mathrm{OP}(3, 4s, 4s)$ for $s \geq 1$;
12. $\mathrm{OP}(4^\alpha, 2s+1)$ for $s \geq 1$, $\alpha \geq 0$;
13. $\mathrm{OP}((4s)^\alpha, 2s+1)$ for $s \geq 1$, $\alpha \geq 0$.

12.24 $\lambda K_q^{(p)}$ is the multigraph with pq vertices partitioned into p parts each of size q having no edges joining pairs of vertices in the same part and having exactly λ edges joining each pair of vertices from different parts.

12.25 Theorem [1746] Other than $K_6^{(2)}$, which has no 2-factorization in which each 2-factor is isomorphic to $[6^2]$, there exists a 2-factorization of $K_n^{(2)}$ in which each 2-factor is isomorphic to $[m_1^{\alpha_1}, m_2^{\alpha_2}, \ldots, m_t^{\alpha_t}]$ if and only if n is even, $m_i \geq 4$ is even for $i = 1, 2, \ldots, t$, $\alpha_1 m_1 + \alpha_2 m_2 + \ldots + \alpha_t m_t = 2n$.

12.26 Theorem (see [1474]) There exists a 2-factorization of $\lambda K_q^{(p)}$ in which each 2-factor is isomorphic to $[m^*]$ if and only if m divides pq, $\lambda(p-1)q$ is even, m is even when $p = 2$, and $(p, q, m, \lambda) \notin \{(2, 6, 6, 1), (3, 6, 3, 1), (6, 2, 3, 1), (3, 2, 3, 2i+1), (6, 1, 3, 4i+2) : i \geq 0\}$

12.27 Theorem [1092] Let m be even. There exists a 2-factorization of $\lambda K_q^{(p)} - I$ in which each 2-factor is isomorphic to $[m^*]$ if and only if q is odd, p is even, and m divides pq.

12.28 Theorem [165] For all $r, s \geq 2$, there exists a 2-factorization of $2K_{r+s}$ in which each 2-factor is isomorphic to $[r, s]$, except that there is no 2-factorization of $2K_6$ in which each 2-factor is isomorphic to $[3, 3]$.

12.4 Other 2-Factorizations

12.29 A 2-factorization consisting of exactly β_i 2-factors isomorphic to F_i for $i = 1, 2, \ldots, k$ is of *type* $[F_1^{\beta_1}, F_2^{\beta_2}, \ldots, F_k^{\beta_k}]$. Let G be a d-regular graph on n vertices. A 2-factorization of G of type $[F_1^{\beta_1}, F_2^{\beta_2}, \ldots, F_k^{\beta_k}]$ is *admissible* if d is even, F_i is a 2-regular graph on n vertices for $i = 1, 2, \ldots, k$, and $\beta_1 + \beta_2 + \cdots + \beta_k = \frac{d}{2}$.

12.30 Table The following types of 2-factorizations of K_n do not exist (see [60]).

n	type
7	$[[3, 4]^2, [7]]$
9	$[[3^3]^3, [4, 5]]$, $[[3^3]^3, [3, 6]]$, $[[3^3]^3, [9]]$, $[[3^3]^2, [4, 5]^2]$, $[[3^3]^2, [4, 5], [3, 6]]$ $[[3^3]^2, [4, 5], [9]]$, $[[3^3]^2, [3, 6], [9]]$, $[[3^3], [4, 5], [3, 6]^2]$, $[[4, 5]^4]$
11	$[[3^2, 5]^5]$
13	All Exist
15	$[[3^5]^6, [3^2, 4, 5]]$, $[[3^5]^6, [3, 5, 7]]$, $[[3^5]^6, [5^3]]$, $[[3^5]^6, [4^2, 7]]$, $[[3^5]^6, [7, 8]]$
17	All Exist

12.31 Theorems The following types of 2-factorizations of K_n exist.

1. For $n \leq 17$, every admissible type except the types in Table 12.30 (see [60]).
2. For $n = 19$, $[[3^5, 4]^8, F]$ for any 2-factor F of K_{19} [60].
3. For $n = 21$, $[[3^7]^9, F]$ for any 2-factor F of K_{21} with the possible exception of $F = [3^3, 6^2]$ [60, 665].
4. For odd $n \geq 11$, $[F_1, F_2, F_3, [n]^{\frac{n-7}{2}}]$ for any three 2-factors F_1, F_2, F_3 of K_n [358].
5. For n an odd prime, $[F_1, F_2, \ldots, F_\alpha, [n]^{\frac{n-1}{2}-\alpha}]$ where $\alpha = \frac{n-1}{4}$ if $r \equiv 0 \pmod 4$, $\alpha = \frac{n-1}{4} - \frac{n-1}{2r}$ if $r \equiv 2 \pmod 4$, $\alpha = \frac{n-1}{4} - \frac{n-1}{4r}$ if r is odd, and r is the multiplicative order of 2 in $\mathbb{Z}_n$ [358].
6. For odd $n \geq 9$, $[[3, n-3], [4, n-4], \ldots, [\frac{n-1}{2}, \frac{n+1}{2}], [n], F]$ where $F = [n]$ or F is any 2-factor of K_n consisting of one odd and two even length cycles [1958].
7. For $n = a \cdot 3^m$ where $a \in \{5, 7, 13, 19\}$ and $m \geq 1$, $[[3^*]^r, [n]^s]$ for all r, s satisfying $r + s = \frac{n-1}{2}$ (see [1822]).
8. For $n \equiv 15 \pmod{30}$, $[[3^*]^r, [5^*]^s], [[3^*]^r, [15^*]^s]$ and $[[5^*]^r, [15^*]^s]]$ for all r, s satisfying $r + s = \frac{n-1}{2}$ with the definite exception of $[[3^5]^6, [5^3]]$ for $n = 15$, and the possible exception of $[[3^*]^{\frac{n-3}{2}}, [5^*]]$ for $n \geq 45$ (see [1822]).

9. For $n = p^m$ where p is an odd prime and $m \geq 1$, $[[n]^{k_0}, [(\frac{n}{p})^*]^{k_1}, [(\frac{n}{p^2})^*]^{k_2}, \ldots, [p^*]^{k_{m-1}}]$ for any sequence $k_0, k_1, \ldots, k_{m-1}$ of nonnegative integers satisfying $k_0 + k_1 + \cdots + k_{m-1} = \frac{n-1}{2}$ with the definite exception of $[[3^3]^3, [9]]$ for $n = 9$, and the possible exception of sequences where the first nonzero term is 1 for $n \geq 27$ (see [1822]).

12.32 Table The following types of 2-factorizations of $K_n - I$ do not exist.

n	type
6	$[[3^2]^2]$
8	$[[3,5]^2, [4,4]]$, $[[3,5],[4,4]^2]$
10	All Exist
12	$[[3^4]^5]$

12.33 Theorem The following types of 2-factorizations of $K_n - I$ exist.

1. For $n \leq 10$, every admissible type except the types in Table 12.32 (see [60]).
2. For even $n \geq 8$, $[F_1, F_2, [n]^{\frac{n-6}{2}}]$ for any two 2-factors F_1 and F_2 of K_n [358].
3. For even $n \geq 2$, $[[3, n-3], [4, n-4], \ldots, [\frac{n}{2}, \frac{n}{2}], [n]]$ [1958].
4. For all $n \equiv 0 \pmod{12}$, $[[4^*]^r, [6^*]^s]$ for all r, s satisfying $r + s = \frac{n-2}{2}$ [56].
5. For $n = 2^m$ and $m \geq 1$, $[[4^*]^{k_2}, [8^*]^{k_3}, [16^*]^{k_4}, \ldots, [n]^{k_m}]$ for any sequence k_2, k_3, …, k_m of nonnegative integers satisfying $k_2 + k_3 + \cdots + k_m = \frac{n-2}{2}$ [775].

12.34 Remark The problem of finding, for any pair F_1 and F_2 of 2-factors and any pair of integers r and s, all admissible types of 2-factorization of K_n and $K_n - I$ of type $[F_1^r, F_2^s]$ is known as the *Hamilton–Waterloo Problem*.

12.35 Remark A 2-factorization of K_n or $K_n - I$ is *pancyclic* if for each $m \in \{3, 4, \ldots, n-3, n\}$, there is at least one occurrence of an m-cycle in some 2-factor. Item 6 of Theorem 12.31 and Item 3 of Theorem 12.33 settle the existence problem for pancyclic 2-factorizations of K_n and $K_n - I$. See [1958] for bipartite analogs. Many additional specific types of 2-factorizations can be obtained by using the techniques from the references cited in Theorems 12.23, 12.31, and 12.33.

12.36 Table Let $G = K_n$ if n is odd, $G = K_n - I$ if n is even. For the indicated values of m and n, the values of t for which there exists a 2-factorization of G containing exactly t m-cycles are $t \in \{0, 1, \ldots, \lfloor \frac{n-1}{2} \rfloor \frac{n}{m}\}$ if m divides n, and $t \in \{0, 1, \ldots, \lfloor \frac{n-1}{2} \rfloor \lfloor \frac{n-3}{m} \rfloor\}$ otherwise, with the indicated definite and possible exceptions (see [1364, 1995]).

m	n	Definite Exceptions, (n,t)	Possible Exceptions, (n,t)
3	$1, 5 \pmod 6$	(7,2),(11,10)	(23,65),(25,83),(29,107) $(29,109), (29,110), (29,111)$ $(31,134), (35,169), (37,197)$ $(41,237), (41,238), (41,239)$
3	$3 \pmod 6$	$(n, \frac{n(n-1)}{6} - 1)$, $(9,7), (9,9), (9,10)$	$(33,171), (33,173), (33,174)$ $(39,242), (39,244), (39,245)$
4	$0 \pmod 4$	$(n, \frac{n(n-2)}{8} - 1)$ $(8,1), (8,3)$	
4	$1, 2, 3 \pmod 4$	$(7,2), (9,4)$	
6	odd		
8	all		$(33,47), (34,45), (34,47)$

12.37 Remark Table 12.36 includes results from [60] that cover some cases originally listed as possible exceptions for $m = 3$.

12.38 Theorem (see [1822]) Other than the definite exceptions $(n,t) \in \{(7,5),(9,11)\}$ and the possible exceptions $(n,t) \in \{(n, \frac{n-1}{2}\lfloor \frac{n}{3} \rfloor - 1) : n = 23,25,29,31,33,35,37,39\}$, there exists a 2-factorization of K_n in which the total number of cycles in all 2-factors is t if and only if n is odd and t is an integer in the range $\frac{n-1}{2} \le t \le \frac{n-1}{2}\lfloor \frac{n}{3} \rfloor$.

12.39 Theorem (see [363]) Let $p \ge 2$, $q \ge 1$ and let F be any 2-factor of $K_q^{(p)}$. Then there exists a 2-factorization of $K_q^{(p)}$ of type $[[pq]^{\frac{(p-1)q}{2}-1}, F]$ if and only if $(p-1)q$ is even, and there exists a 2-factorization of $K_q^{(p)} - I$ of type $[[pq]^{\frac{(p-1)q-1}{2}-1}, F]$ if and only if $(p-1)q$ is odd.

12.5 Resolvable and Almost Resolvable Cycle Systems

12.40 A (directed) m-cycle system of order n and index λ is *resolvable* if the (directed) m-cycles can be partitioned into 2-factors.

12.41 Remark A resolvable m-cycle system of order n and index λ is equivalent to a 2-factorization of λK_n in which each 2-factor is isomorphic to $[m^*]$. The existence problem is thus settled by Theorem 12.26. The directed case is covered next.

12.42 Theorem (see [59]) For $m \in \{3,4\}$ there exists a resolvable directed m-cycle system of order n and index λ if and only if m divides n, $(m,n,\lambda) \notin \{(3,6,2i+1),(4,4,2i+1) : i \ge 0\}$.

12.43 An *almost 2-factor* of a graph G is a 2-regular spanning subgraph of $G - v$ for some vertex v in G. A (directed) m-cycle system of order n and index λ is *almost resolvable* if the (directed) m-cycles can be partitioned into almost 2-factors.

12.44 Theorem [837] There exists an almost resolvable m-cycle system of order n and index λ if and only if m divides $n-1$ and λ is even.

12.45 Theorem [837, 840] For $m \in \{3,5\}$ and m even, there exists an almost resolvable directed m-cycle system of order n and index λ if and only if m divides $n-1$. For $m \equiv 3 \pmod 6$, there exists an almost resolvable directed m-cycle system of order n and index λ whenever m divides $n-1$ except possibly when $n \in \{3m+1, 6m+1\}$.

12.6 i-Perfect m-Cycle Systems

12.46 If c is a cycle, let $c(i)$ be the graph formed from c on the same vertex set by joining two vertices if and only if they are distance i apart in c. An m-cycle system C of order n and index λ is *i-perfect* if and only if $C(i) = \{c(i) : c \in C\}$ is a m'-cycle system of order n and index λ for some integer $m' \ge 3$.

12.47 Example The 5-cycle system in Example 12.5 is 2-perfect.

12.48 Remark One can assume that $2 \le i < m/2$, because i-perfect m-cycle systems are $(m-i)$-perfect. If there exists an i-perfect m-cycle system of order n and index λ, then there exists a j-perfect m-cycle system of order n and index λ whenever $ij \equiv 1$ or $m-1 \pmod m$ (see [57]).

12.49 Theorem (see [1460]) If m is prime and there exists a 2-perfect m-cycle system of order $2m+1$ and index 1, then there exists a 2-perfect m-cycle system of order n and index 1 for all admissible n except possibly $n \in \{3m, 4m+1, 6m+1\}$.

12.50 Table For the given values of m, λ, and i, i-perfect m-cycle systems of order n and index λ are known to exist for all (m,λ)-admissible integers n other than the indicated exceptions and possible exceptions (see [57]).

m	λ	i	Exceptions (n,λ)	Possible Exceptions (n,λ)
5	all	2	$(15,1)$	
6	all	2	$(9,1)$, $(6,4t+2)$ for $t \geq 0$	
7,11,12, 16,17	1	all		
8	all	2	$(8,2)$	$(185,2)$
8	1	3		
9	1	2,4	$(9,1)$	$(45,1)$
9	all	3		
10	1	2,4		$(221,1)$, $(20t+5,1)$ for $t \geq 2$
10	1	3		
13	1	2,3,4,6		
13	1	5		$(n,1)$ for $n \in \{183,209,235,261,$ 287,339,391,703,807,885,963, 1015,1119,1197,1431,1639$\}$, $(26t+13,1)$ for $t \geq 1$
14	1	2		$(309,1)$, $(477,1)$ $(28t+21,1)$ for $t \geq 0$
14	1	3,4,5,6		$(28t+21,1)$ for $t \geq 1$
15	1	2,4,5,7		$(55,1)$
15	1	3,6		$(55,1)$, $(30t+21,1)$ for $t \geq 2$, $(30t+25,1)$ for $t \geq 1$
18	1	2,3,5,7		$(36t+9,1)$ for $t \geq 1$
18	1	4,6		$(217,1)$, $(36t+9,1)$ for $t \geq 1$
19	1	2,9		$(57,1)$
19	1	3,4,5,6,7,8		

12.51 Remark m-cycle systems that are 2-perfect or $((m-1)/2)$-perfect for m odd can be used to construct quasigroups satisfying certain identities (see [1460] and §III.2).

12.7 Maximal Partial Cycle Systems

12.52 A *partial (directed) m-cycle system of a (directed) graph K* is a (directed) m-cycle system of some (directed) subgraph of K. A partial (directed) m-cycle system of λK_n (λD_n) is a *partial (directed) m-cycle system of order n and index λ*.

12.53 A partial m-cycle system C of a graph K is *maximal* if there is no partial m-cycle system B of K with $C \subseteq B$ and $|B| > |C|$.

12.54 Table For m and K, the precise values of t for which there exists a maximal partial m-cycle system C of K with $|C| = t$. (See [839, 1824].)

m	K	t
$m = n$	K_n	$\lfloor (n+3)/4 \rfloor \leq t \leq (n-1)/2$
$m = pq$	$K_q^{(p)}$	$\lceil q(p-1)/4 \rceil \leq t \leq \lfloor q(p-1)/2 \rfloor$ with the definite exceptions of $t = q(p-1)/4$ when q is odd and $p \equiv 1 \pmod 4$; $t = q/4$ when $p = 2$; $t = (p-1)/4$ when $q = 1$; and the possible exceptions of $t = \lceil q(p-1)/4 \rceil$ when $q = 3$ and p is odd.
3	K_n	Completely settled (see [1824])
5	K_n	Completely settled (see [1824])

12.55 A *maximal partial 2-factorization* of K_n is a 2-factorization of a subgraph H of K_n such that the graph obtained from K_n by removing the edges of H contains no 2-factor.

12.56 Theorem There is a maximal partial 2-factorization of K_n consisting of t 2-factors if and only if $t = (n-1)/2$ when n is odd, and if and only if $(n - n^{\frac{1}{2}})/2 \leq t \leq (n-2)/2$ when n is even.

12.8 Embedding and Incomplete m-Cycle Systems

12.57 A partial (directed) m-cycle system B is *embedded* in a (directed) m-cycle system C if $B \subseteq C$.

12.58 Table For the given m and λ, any partial m-cycle system of index λ and order n can be embedded in an m-cycle system of order v for the indicated values of v (see [361, 1118, 1457, 1461]). Admissible means m, λ)-admissible here.

m	λ	v
3	1	all admissible $v \geq 2n+1$
4	1	all admissible $v \geq 2n+9$
6	1	all $v \geq 3n+10$ with $v \equiv 13 \pmod{36}$
10	1	all $v \geq 5n+16$ with $v \equiv 21 \pmod{100}$
$2k$	1	$v = kx + y$, for all $x \geq n$ where if k is even, then $y \geq k/2(k-1)$ is admissible and $x \equiv 0 \pmod{2k}$. If k is odd, then $y \geq k/2(k+1)$, $y+k$ is admissible and $x \equiv 1 \pmod{4k}$.
$2k+1$	1	all $v \geq m(2n+1)$ with $v \equiv m \pmod{2m}$
3	even	all admissible $v \geq 2n+1$
$2k+1$	$\lambda \geq 3$	all $v \geq m(4n+17)$ with $v \equiv m \pmod{2m}$
$2k$	odd	all $v \geq 2mn+1$ with $v \equiv 1 \pmod{2m}$
$2k$	even	all $v \geq mn$ with $v \equiv 0 \pmod{m}$

12.59 Table For the given values of m and λ, any partial directed m-cycle system of index λ and order n can be embedded in a directed m-cycle system of index λ and order v for the indicated values of v (see [1461]). Admissible means (m, λ^*)-admissible here.

m	λ	v
3	1	all admissible $v \geq 4n$ for $n \geq 14$
$2k+1$	$\lambda \geq 3$	all $v \geq m(2n+1)$ with $v \equiv m \pmod{2m}$
4,6	any	all $v \geq mn+1$ with $v \equiv 1 \pmod{m}$
$2k \geq 8$	any	all $v \geq mn$ with $v \equiv 0 \pmod{m}$

12.60 For $v \geq n$, $K_v - K_n$ is the subgraph of K_v formed by removing the edges in a complete subgraph on n vertices. An *incomplete m-cycle system of order v with a hole of size n* is an m-cycle decomposition of $K_v - K_n$.

12.61 Remark If an m-cycle system of order n is embedded in an m-cycle system of order v then the embedding produces an incomplete m-cycle system of order v with a hole of size n.

12.62 Theorem (see [366]) If there exists an incomplete m-cycle system of order $v > n$ with a hole of size n then (1) v and n are odd; (2) $(v-n)(v+n-1) \equiv 0 \pmod{2m}$; (3) $v \geq n(m+1)/(m-1)+1$ if m is odd; and (4) $(v-m)(v-1) \geq n(n-1)$.

12.63 Theorem (see [366]) Conditions (1) to (4) of Theorem 12.62 are sufficient for the existence of an incomplete m-cycle system of order $v > n$ with a hole of size n when

1. $m \in \{3, 4, 5, 6, 7, 8, 10, 12, 14\}$,
2. $m \in \{9, 11, 13\}$ and n is $(m, 1)$-admissible,
3. m is even and $v \equiv n \pmod{2m}$, and
4. m is odd, $n \equiv 1$ or $m \pmod{2m}$, and $v \equiv 1$ or $m \pmod{2m}$ except possibly for the smallest such v in some cases.

12.64 An (almost) resolvable m-cycle system C_1 is *resolvably embedded* in an (almost) resolvable m-cycle system C_2 if C_1 is embedded in C_2 in such a way that each (almost) 2-factor in the resolution of C_1 is contained in an (almost) 2-factor in the resolution of C_2. (An analogous definition exists for directed cycle systems.)

12.65 Theorem (see [1478]) A resolvable 3-cycle system of order n and index λ can be resolvably embedded in resolvable 3-cycle system of order v and index λ if and only if $v \geq 3n$, $n \equiv v \equiv 3 \pmod 6$ if λ is odd, and $n \equiv v \equiv 0 \pmod 3$ and $n \neq 6$ if λ is even.

12.66 Theorem [1478] An almost resolvable 3-cycle system of order n and index λ can be resolvably embedded in an almost resolvable 3-cycle system of order v and index λ if and only if $v \geq 3n + 1$, and $n \equiv v \equiv 1 \pmod 3$.

12.67 Theorem (see [1478]) A directed resolvable 3-cycle system of order n and index 1 can be resolvably embedded in a resolvable 3-cycle system of order v and index 1 if and only if $v \geq 3n$, except possibly if (n, v) is one of 71 unresolved cases listed in the reference.

12.9 Nesting of m-Cycle Systems

12.68 A *nesting* of an m-cycle system C of K_n with vertex set V is a function $f : C \to V$ such that $\{\{x, f(c)\} | c \in C, x \in V(c)\}$ partitions the edges of K_n (into stars).

12.69 Remark If there exists a nesting of an m-cycle system of K_n, then $n \equiv 1 \pmod{2m}$.

12.70 Table There exists an m-cycle system of K_n with a nesting for the indicated values of m and n (see [1812]).

m	All $n = 2xm + 1$ except possibly if
2^e	$x \in \{2, 3, 4, 7, 8, 12, 14, 18, 19, 23, 24, 33, 34\}$
$\neq 2^e$	$x \in \{2, 3, 4, 6, 22, 23, 24, 26, 27, 28, 30, 34, 38\}$
$3 \leq m \leq 15$, m odd	$(m, x) \in \{(7, 4), (7, 6), (9, 3), (11, 6), (13, 4), (15, 3)\}$
odd	$x \in \{3, 4, 6\}$, providing there is an m-cycle system of K_{4m+1} with a nesting

12.71 An *x-nesting* of a directed cycle system C of K_n^* with vertex set V is a function $f : C \to V$ such that $\{(x_1, f(c)), (f(c), x_2) | c \in C, x_1 \in X_1, x_2 \in X_2, V(c) = X_1 \cup X_2, |X_1| = x, |X_2| = m - x\}$ partitions the directed edges of K_n^* (into directed stars).

12.72 Remark If there exists an x-nesting of a directed m-cycle system of K_n^*, then $n \equiv 1 \pmod m$.

12.73 Table There exists a directed m-cycle system of K_n^* with an x-nesting for the indicated values of m, x and n (see [1812]).

m	x	n
odd	$\lfloor m/2 \rfloor$	all $n \equiv 1 \pmod m$, except possibly $n \in \{3m + 1, 6m + 1\}$
even	even	all $n \equiv 1 \pmod m$, except possibly $n = 2m + 1$
2 (mod 4)	$m/2$	all $n \equiv 1 \pmod{2m}$ except possibly $n = 4m + 1$

12.10 Cyclic and 1-Rotational m-Cycle Systems

12.74 An m-cycle system C of K_n is *cyclic* if there exists a labeling of the vertex set of K_n with the elements of $\mathbb{Z}_n$ such that the permutation $x \mapsto x+1$ preserves the cycles of C.

12.75 An m-cycle system C of K_n is 1-*rotational* if there exists a labeling of the vertex set of K_n with the elements of $\mathbb{Z}_{n-1} \cup \{\infty\}$ such that the permutation $x \mapsto x+1$ for $x \in \mathbb{Z}_{n-1}$ and $\infty \mapsto \infty$ preserves the cycles of C.

12.76 Theorem (see [2099]) Let $m \geq 3$ and $n \equiv 1$ or $m \pmod{2m}$. There exists a cyclic m-cycle system of order n if and only if n is odd and $(m,n) \notin \{(3,9),(15,15)\} \cup \{(p^\alpha, p^\alpha) : p \text{ is prime, } \alpha \geq 2\}$.

12.77 Theorem [2171] Let $m = 2q$ where q is a prime power. There exists a cyclic m-cycle system of order n if and only if n is $(m,1)$-admissible and $n \neq 3q$ when $q \equiv 3 \pmod 4$.

12.78 Theorem [2171] Let $3 \leq m \leq 32$. There exists a cyclic m-cycle system of order n if and only if n is $(m,1)$-admissible and $(m,n) \notin \{(3,9),(6,9),(9,9),(14,21),(15,15),(15,21),(15,25),(20,25),(22,33),(24,33),(25,25),(27,27),(28,49)\}$.

12.79 Theorem [387] Let $m \geq 3$ and $n \equiv 1$ or $m \pmod{2m}$. There exists a 1-rotational m-cycle system of order n if and only if m is odd, m is composite when $n \equiv 1 \pmod{2m}$, and $n \not\equiv 15$ or $21 \pmod{24}$ when $m = 3$.

12.80 Theorem (see [387]) Let $m \geq 3$ be odd and $n \leq 3m$. There exists a 1-rotational m-cycle system of order n if and only if n is $(m,1)$-admissible and m is composite when $n = 2m+1$.

See Also

§III.2	2-perfect m-cycle systems give rise to quasigroups.
§VI.24	Decompositions of graphs into other subgraphs.
§VII.5	Factorizations of graphs.
[87]	The method of amalgamations.
[578]	3-cycle systems are triple systems.
[1822]	A survey of 2-factorizations of complete graphs.

References Cited: [56, 57, 59, 60, 62, 83, 87, 149, 150, 165, 358, 361, 362, 363, 364, 366, 387, 578, 624, 665, 666, 775, 837, 839, 840, 1010, 1083, 1092, 1101, 1118, 1176, 1364, 1457, 1460, 1461, 1474, 1478, 1746, 1812, 1822, 1824, 1958, 1994, 1995, 2099, 2171]

13 Defining Sets

Ken Gray
Anne Penfold Street

13.1 Definitions and Basic Results

13.1 A set of blocks that is a subset of a unique t-(v,k,λ) design $D = (V, \mathcal{B})$ is a *defining set* (DS) of that design. A DS is *minimal* (MDS) if it does not properly contain a DS of D, and *smallest* (SDS) if no DS of D has fewer blocks; the number of blocks in an SDS is denoted by s. These DSs are related to *trades*; see §VI.60.

13.2 **Example** For the 2-$(9, 3, 1)$ design of Example II.1.22, $S_1 = \{456, 789, 258, 369\}$ is an SDS and $S_2 = \{123, 456, 147, 249, 159\}$ is a MDS.

13.3 **Theorem** [742, 956] Let D be a t-(v, k, λ_t) design, with minimal trades $\{T_i, T_i'\}$ for $i = 1, \ldots, n$, and MDSs S_j for $j = 1, \ldots, m$, where $T_i \subseteq \mathcal{B}$ for each i and $S_j \subseteq \mathcal{B}$ for each j. Then $S \subseteq \mathcal{B}$ is a defining set of D if and only if $S \cap T_i \neq \emptyset$ for each $i = 1, \ldots, n$; if $T \subseteq \mathcal{B}$ and if $T \cap S_j \neq \emptyset$ for each $j = 1, \ldots, m$, then $T \supseteq T_i$ for some i.

13.4 **Theorem** If designs $D_1 = (V, \mathcal{B}_1)$, $D_2 = (V, \mathcal{B}_2)$, and $D = (V, \mathcal{B}_1 \cup \mathcal{B}_2)$ have SDSs S_1, S_2, S, respectively, then $|S| \geqslant |S_1| + |S_2|$.

13.5 A group is *single-transposition-free* (STF) if none of its elements is a single transposition (ij). A design D is STF if its automorphism group, $Aut(D)$, is STF. A design is *simple* if it has no repeated blocks and *full* if it is $\binom{V_v}{k}$, the simple $(v, k, \binom{v-2}{k-2})$ design.

13.6 **Proposition** [742] For $2 < k < v - 2$, all t-$(v, k, 1)$ designs and all symmetric 2-(v, k, λ) designs are STF.

13.7 **Theorem** [742, 956] Let S be a DS of a design D, and let $\rho \in Aut(D)$. Then $\rho(S)$ is a DS of $\rho(D) = D$, $Aut(S) \leqslant Aut(D)$, and $Aut(D) = \{\rho \mid \rho(S) \subseteq D\}$.

13.8 **Theorem** [742, 956] Let S be a DS of a STF design D. Then at least $v - 1$ elements occur in the blocks of S; if the elements i and j appear only once each in the blocks of S, they appear in different blocks; and if D is simple, it contains $|Aut(D)|/|Aut(S)|$ isomorphic copies of S.

13.9 **Theorem** [742, 956] Let D be a simple STF t-design and let $S \subseteq \mathcal{B}$, where S contains at least $v - 1$ distinct elements and there are $|Aut(D)|/|Aut(S)|$ configurations in D isomorphic to S. If S is not contained in any design with the same parameters as D, but not isomorphic to D, then S is a DS of D.

13.10 **Theorem** Suppose that S is a DS of the full design $\binom{V_v}{k}$, and $D = (V, \mathcal{B})$ is a simple (v, k, λ) design. Then the set of blocks $S \cap \mathcal{B}$ is a DS of D.

13.11 **Theorem** [742, 956] If $(V, \mathcal{B})$ is a t-(v, k, λ) design with blocks $\mathcal{B}_i$, $i = 1, \ldots, b$ and $t \leqslant k \leqslant v - t$, then the complementary blocks $\{V \setminus \mathcal{B}_i : i = 1, \ldots, b\}$ also form a t-design $\bar{D}$; if $t = 2$, $\bar{D}$ is a $(v, v - k, b - 2r + \lambda)$ design; and if $S \subseteq \mathcal{B}$ is a DS of D, then $\bar{S}$, the set of blocks complementary to those in S, is a DS of $\bar{D}$.

13.12 **Table** [742] Sizes of SDSs are listed for small 2-designs with $k \leqslant v/2$. The notation s^m indicates that, among the designs with these parameters, those in m of the isomorphism classes have SDSs of s blocks each. If $m = 1$, it is omitted. In addition, * denotes a 3-design regarded as a 2-design, q a design from quadratic residues, B the 104 STS(19) with $|Aut(D)| \geqslant 9$, and g the point/hyperplane design from PG$(n, 2)$.

v	b	r	k	λ	s	v	b	r	k	λ	s
7	7	3	3	1	3	8	14	7	4	3	6^4
9	12	4	3	1	4	15	15	7	7	3	9, 8, 7^3
13	13	4	4	1	6	9	24	8	3	2	10^5, 9^{21}, 8^{10}
6	10	5	3	2	3	9	18	8	4	3	8^9, 6^2
16	20	5	4	1	7	19	57	9	3	1	23^2, 22^{14}, 21^{68},
21	21	5	5	1	8						20^{17}, 19^2, 18 (B)
11	11	5	5	2	5	7	21	9	3	3	9^9, 7
13	26	6	3	1	9, 8	10	18	9	5	4	8, 7^{18}, 6^2
7	14	6	3	2	6^4	19	19	9	9	4	8^6
10	15	6	4	2	8, 6, 5	23	23	11	11	5	8 (q)

v	b	r	k	λ	s	v	b	r	k	λ	s
25	30	6	5	1	10	7	28	12	3	4	12^{34}, 10
31	31	6	6	1	11	10	30	12	4	4	16 (*)
16	16	6	6	2	9, 7^2	27	27	13	13	6	$\leqslant 11$ (q)
15	35	7	3	1	16, 14^3, 13^4,	31	31	15	15	7	$\leqslant 10$ (q), 24 (g)
					12^{20}, 11^{52}	63	63	31	31	15	52–55 (g)

13.13 Table [742] Sizes of SDSs for small t-designs, with $t = 3, 4$, or 5, and $k \leqslant v/2$, are listed in increasing order of r for each value of t. Notation and references are the same as for Table 13.12. Q denotes an extension of a 2-design from quadratic residues.

t	v	b	r	k	λ	s	t	v	b	r	k	λ	s
3	8	14	7	4	1	3	3	22	77	21	6	1	8
3	12	22	11	6	2	5	3	24	46	23	12	5	8 (Q)
3	10	30	12	4	1	4	3	28	54	27	14	6	$\leqslant 11$ (Q)
3	8	28	14	4	2	6^4	3	8	56	28	4	4	12^{30}, 10
3	16	30	15	8	3	9, 8, 7^3	3	32	62	31	16	7	$\leqslant 10$ (Q)
3	10	36	18	5	3	8^4, 6^2, 5	4	11	66	30	5	1	5
3	20	38	19	10	4	8^3	4	23	253	77	7	1	8
3	17	68	20	5	1	7	5	12	132	66	6	1	5
3	8	42	21	4	3	9^9, 7	5	24	759	253	8	1	8

13.14 Remark [742] For a 2-$(6, 3, \lambda)$ design with λ even, $s = 3\lambda/2$. For 2-$(7, 3, \lambda)$ designs, it is known only that $1/3 \leqslant s/b \leqslant 16/35$, and for 3-$(8, 4, \lambda)$ designs, that $1/6 \leqslant s/b \leqslant 8/35$.

13.2 Finite Geometries, STSs, and Latin Squares

13.15 Theorem [939] In the projective geometry $\mathrm{PG}(d, 2)$, with $d \geqslant 2$, there exists a set of $d + 1$ hyperplanes such that no point of $\mathrm{PG}(d, 2)$ is incident with all of them. The hyperplanes of such a set cover a total of $(\frac{2}{3})4^d - (\frac{1}{2})3^d - 2^d + (\frac{5}{6})$ lines that form a MDS of the point-line design of $\mathrm{PG}(d, 2)$, that is, an $\mathrm{STS}(2^{d+1} - 1)$. In the affine geometry $\mathrm{AG}(d, 3)$, there is a set of $2d$ hyperplanes, two from each of d parallel classes, such that no line of $\mathrm{AG}(d, 3)$ is incident with any d of them, and there is a point of $\mathrm{AG}(d, 3)$ incident with none of them. The hyperplanes of such a set cover a total of $[3^d(3^d - 1) - 7^d + 1]/6$ lines that form a MDS of the point-line design of $\mathrm{AG}(d, 3)$, that is, an $\mathrm{STS}(3^d)$ (see §VII.2).

13.16 Remark From Theorem 13.15, by adapting a construction [1975] for critical sets in latin squares, other MDSs can be found [741] in STSs associated with $\mathrm{PG}(n, 2)$, $\mathrm{AG}(n, 3)$ and nonaffine Hall triple systems of order 3^n (HTS) (see §VI.28). Thus, there are MDSs of volume t in $\mathrm{STS}(2^n - 1)$ associated with $\mathrm{PG}(n, 2)$ where $\alpha = (4^n - 3 \cdot 2^n + 5)/6$ and $t \in \{\alpha - 3^n/6, \alpha - 37 \cdot 3^n/162, \alpha - 29 \cdot 3^n/162\}$, and MDSs of volume t in $\mathrm{STS}(3^n)$ associated with $\mathrm{AG}(n, 3)$ where $\beta = (9^n - 3^n + 1)/6$ and $t \in \{\beta - 7^n/6, \beta - 7^{n-2}/6 - 7^{n-1}, \beta - 7^{n-3}/6 - 52 \cdot 7^{n-3}\}$. In nonaffine $\mathrm{HTS}(3^n)$, there are MDSs of volume $\beta - (7^n/6)$.

13.17 Theorem [296] A projective plane of order q has a defining set of size $\mathrm{o}(q^2)$.

13.3 Finding Defining Sets and Spectra

13.18 Remark Early algorithms [742] start from a lower bound, n, for the size s of an SDS of design D and determine whether any set of n blocks of D completes uniquely to a

BIBD with the parameters of D. If not, sets of $n+1$ blocks are considered, and so on, until an SDS is found. Such algorithms require a *completion program* and techniques involving trades (Theorem 13.3) and find only SDSs of D. A later algorithm [1067] avoids these requirements. From a list of all designs with the same parameters as a given design D, it finds in one pass all MDSs of D.

13.19 The *spectrum* of MDSs of a design D is $spec(D) = \{|M| : M \text{ is a MDS of } D\}$. If $h \notin spec(D)$, but D has MDSs with cardinalities both smaller and larger than h, then h is a *hole* in $spec(D)$. A *gap* in $spec(D)$ is a maximal length sequence of consecutive holes. If $spec(D)$ has no holes, then it is *continuous*.

13.20 Example [1067] When $D = \binom{V_6}{3}$, then $spec(D) = \{6, 7, 8, 10\}$; up to isomorphism, there are 1, 2, 3, 2 MDSs of sizes 6, 7, 8, 10, respectively, as listed; $h = 9$ is a hole (and a gap) in $spec(D)$. Below are $8 = 1 + 2 + 3 + 2$ representative MDSs.

123, 124, 125, 134, 135, 145	123, 124, 134, 136, 146, 234, 235, 245
123, 124, 125, 126, 134, 135, 136	135, 136, 145, 146, 156, 234, 235, 236,
123, 124, 125, 134, 135, 234, 235	245, 246
123, 124, 125, 126, 134, 146, 234, 235	126, 135, 145, 146, 156, 234, 235, 236,
123, 124, 125, 126, 146, 156, 234, 235	246, 345

13.21 Proposition [742] The spectrum of the point-line design of PG$(3, 2)$ is continuous: $\{16, \ldots, 22\}$.

13.22 Theorem [72] Let $D = \binom{V_v}{3}$ be the full 2-$(v, 3, v-2)$ design, where $v \geqslant 6$. Let $\mathcal{B}_v$ and $\mathcal{B}_{12}$ be the sets of blocks of D containing element v and set $\{1, 2\}$, respectively. Then $\binom{V_v}{3} \setminus (\mathcal{B}_v \cup \mathcal{B}_{12})$ is a MDS of D.

See Also

§VI.60	Trades and defining sets are closely related.
[742]	Table for smallest defining sets.

References Cited: [72, 296, 741, 742, 939, 956, 1067, 1975]

14 Deletion-correcting Codes

Vladimir I. Levenshtein

14.1 Combinatorics of Subsequences and Supersequences

14.1 Let F_v^n be the set of sequences $(x_1, \ldots, x_n)$ over the alphabet $F_v = \{0, 1, \ldots, v-1\}$ for $v \geq 2$. For $n \leq v$, let A_v^n be the subset of F_v^n consisting of sequences of different letters (directed subsets of F_v). The sequence $Y = (x_{i_1}, \ldots, x_{i_m})$ with $0 \leq m \leq n$ and $1 \leq i_1 < \cdots < i_m \leq n$ is a *subsequence* of length m of $X = (x_1, \ldots, x_n)$; X is a *supersequence* of Y of length n. The subsequence Y is obtained from X by *deletions* of $s = n - m$ letters whose indices differ from $i_1, \ldots, i_m$; X is obtained from Y by *insertions* of $s = n - m$ letters before and after letters of Y. For any $X \in F_v^n$ and integer s, $s \geq 0$, $D_s(X)$ is the set of all different subsequences of X of length $n - s$ and $I_s(X)$ is the set of all different supersequences of X of length $n + s$.

14.2 If $X = (x_1, \ldots, x_n)$ is a sequence, a *run* in X is a maximal interval of X consisting of the same letter. Denote by $r(X)$ the number of runs in X.

14.3 **Example** For $X = 0110 \in F_2^n$, $r(X) = 3$, $D_1(X) = \{110, 010, 110\}$, and $I_1(X) = \{10110, 00110, 01010, 01110, 01100, 01101\}$.

14.4 **Theorem** [1103, 1433] For any $X \in F_v^n$, $\sum_{i=0}^{s} \binom{r(X)-s}{i} \le |D_s(X)| \le \binom{r(X)+s-1}{s}$. In particular, $|D_1(X)| = r(X)$.

14.5 **Theorem** [409, 1103, 1440] Let $D_v(n,s) = \max_{X \in F_v^n} |D_s(X)|$ and let $X_{n,v} = (x_1, \ldots, x_n)$ where $x_i = b \in F_v$ if $i - 1 \equiv b \pmod{v}$. Then $D_v(n,s) = |D_s(X_{n,v})|$,

$$D_v(n,s) = \sum_{i=0}^{v-1} D_v(n-i-1, s-i) = \sum_{i=0}^{s} \binom{n-s}{i} D_{v-1}(s, s-i),$$

$$D_v(n,s) = \sum_{i=0}^{\lfloor s/v \rfloor} (-1)^i \binom{n-s}{i} \binom{n-vi}{n-s}.$$

In particular, $D_2(n,s) = \sum_{i=0}^{s} \binom{n-s}{i}$, $\quad D_3(n,s) = \sum_{i=0}^{s} \binom{n-s}{i} \sum_{j=0}^{s-i} \binom{i}{j}$.

14.6 **Theorem** [1435] For any $X \in F_v^n$, $|I_s(X)| = \sum_{i=0}^{s} \binom{n+s}{i} (v-1)^i$.

14.7 **Corollary** $\frac{1}{v^n} \sum_{X \in F_v^n} |D_s(X)| = v^{-s} \sum_{i=0}^{s} \binom{n}{i} (v-1)^i$.

14.8 For any n, s, and v, consider the maximum number of common subsequences of two different sequences $N_v^-(n,s) = \max_{X,Z \in F_v^n;\ X \ne Z} |D_s(X) \cap D_s(Z)|$ and the maximum number of common supersequences of two different sequences $N_v^+(n,s) = \max_{X,Z \in F_v^n;\ X \ne Z} |I_s(X) \cap I_s(Z)|$.

14.9 **Theorem** [1440] $N_v^+(n,s) = \sum_{i=0}^{s-1} \binom{n+s}{i} (v-1)^i (1 - (-1)^{s-i})$ and

$$N_v^-(n,s) = \sum_{i=0}^{s-1} \binom{n-s-1}{i} \left(D_{v-1}(s, s-i-1) + D_{v-1}(s-1, s-i-1) \right).$$

In particular, $N_2^-(n,s) = 2 \sum_{i=0}^{s-1} \binom{n-s-1}{i}$, $N_2^+(n,s) = 2 \sum_{i=0}^{s-1} \binom{n+s-1}{i}$

14.10 **Remark** The number $N_v^-(n,s) + 1$ is the minimum N for which an arbitrary $X = (x_1, \ldots, x_n) \in F_v^n$ can be reconstructed from any N of its different subsequences of length $n-s$,; $N_v^+(n,s)+1$ is the minimum N for which an arbitrary $X = (x_1, \ldots, x_n) \in F_v^n$ can be reconstructed from any N of its different supersequences of length $n+s$. This problem differs from reconstructing an unknown sequence $X = (x_1, \ldots, x_n) \in F_v^n$ from the multiset $M_m(X)$ of all $\binom{n}{m}$ its subsequences $Y = (x_{i_1}, \ldots, x_{i_m})$ of length m where $1 \le i_1 < \cdots < i_m \le n$ (reconstruction by fragments). This problem consists of finding the minimum number $m = m_v(n)$ such that $M_m(X) \ne M_m(Z)$ for any different $X, Z \in F_v^n$ and is far from being settled (see [1345, 1427, 1521, 2198]).

14.2 Codes in Deletion/Insertion Metric

14.11 The deletion/insertion distance $\rho(X,Y)$ between sequences $X \in F_v^n$ and $Y \in F_v^n$ is the minimum number of deletions and insertions of symbols translating X to Y.

14.12 **Lemma** For any $X \in F_v^n$ and $Y \in F_v^n$, $\rho(X,Y) = L(X,Y) - \ell(X,Y)$ where $\ell(X,Y)$ is the maximum length of a common subsequence and $L(X,Y)$ is the minimum length of a common supersequence of X and Y.

14.13 A set $W \subseteq F_v^n$ is an s-deletion-correcting code if $\rho(X,Y) > 2s$ for any different $X, Y \in W$. An s-deletion-correcting code $W \subseteq F_v^n$ (and $W \subseteq A_v^n$ for $v \geq n$) is *perfect* if any sequence of F_v^{n-s} (respectively, of A_v^{n-s}) is a subsequence of a unique sequence of W. Denote by $M_v(n,s)$ the maximum size of a s-deletion-correcting code $W \subseteq F_v^n$.

14.14 Remark A perfect s-deletion-correcting code $W \subset A_v^n$ is the same as a directed design $T(t,n,v)$ with $t = n-s$, and its cardinality equals $\binom{v}{t}t!/\binom{n}{t}$ if it exists. See §VI.20 for the equivalence and for related results.

14.15 Remark Any s-deletion-correcting code allows one to correct deletions and insertions of letters if their total number does not exceed s.

14.16 Theorem [1433, 1437] For any n the set F_2^n is partitioned into $n+1$ perfect 1-deletion-correcting codes $W_2^{n,a}$, $a = 0, 1, \ldots, n$, where

$$W_2^{n,a} = \{X = (x_1, \ldots, x_n) \in F_2^n : \ \textstyle\sum_{i=1}^n ix_i = a \pmod{n+1}\}.$$

14.17 Theorem [909] $\max_a |W_2^{n,a}| = |W_2^{n,0}| = \frac{1}{2(n+1)} \sum_{d,\ d|n+1,\ (d,2)=1} 2^{\frac{n+1}{d}} \varphi(d)$.

14.18 Example A partition of F_2^5 into (six) perfect 1-deletion-correcting codes $W_2^{5,a}$.

00000	00110	00101	00011	00010	00001
00111	01001	01000	00100	01101	01011
01010	10000	01111	01110	10011	01100
00001	10111	10110	10101	10100	10010
11011	11010	11001	11000	11110	11101
11100			11111		

14.19 Remark Perfect 1-deletion-correcting codes in F_v^3 and F_v^4 exist for any v [1437, 2113]. Necessary and sufficient conditions for perfect deletion-correcting codes in F_v^5 and F_v^6 are given in Theorem 20.18. Constructions of perfect $(n-2)$-deletion-correcting codes in F_v^n for some v are given in [311, 2186] .

14.20 Theorem [1433] For fixed v and s, $M_v(n,s) \lesssim \frac{s!v^n}{(v-1)^s n^s}$ as $n \to \infty$.

14.21 Corollary [1433] $M_2(n,1) \sim \frac{2^n}{n}$ as $n \to \infty$.

14.22 Theorem [1437, 2017] $\frac{v^{n-1}}{n} \leq M_v(n,1) \leq \frac{v^{n-1}+(n-2)v^{n-2}+v}{n}$. Hence $M_v(n,1) \sim \frac{(v-1)^n}{n}$ if $n \to \infty$ and $v/n \to \infty$.

14.23 Conjecture For fixed $v \geq 2$,

$$M_v(n,1) \sim \tfrac{v^n}{(v-1)n}$$

as $n \to \infty$.

14.24 Theorem [1441] $M_v(n,s) \geq \frac{v^{n+s}}{\left(\sum_{i=0}^s \binom{n}{i}(v-1)^i\right)^2}$.

14.25 Proposition $M_v(n, \frac{v-1}{v}n) = v$.

14.26 Remark The code $V_2^n = \{X = (x_1, \ldots, x_n) \in F_2^n : \ \sum_{i=1}^n ix_i = 0 \pmod{2n}\}$ is capable to correct deletion, insertion or substitution of a single symbol. It has cardinality $\frac{1}{2n} \sum_{d,\ d|n,\ (d,2)=1} 2^{n/d}\varphi(d)$ [1433, 1434]. A table of cardinality of codes capable of correcting similar errors can be found in [1136].

14.3 Perfect Deletion-Correcting Codes as Directed Designs

14.27 For $X = (x_1, \ldots, x_n) \in A_v^n$, the sequence $Y = (y_1, \ldots, y_{n-1}) \in F_2^{n-1}$, where $y_i = 0$ if $x_i < x_{i+1}$ and $y_i = 1$ if $x_i > x_{i+1}$, is an *up-and-down sequence* of X and is denoted by $UD(X)$

14.28 Theorem [1437] For each n the set A_n^n (or the set S_n of permutations of n elements) is partitionable into n perfect single-deletion-correcting codes $S_{n,a}$, $a = 0, 1, \ldots, n-1$, where $S_{n,a} = \{X = (x_1, \ldots, x_n) \in S_n : \ UD(X) \in W_2^{n-1,a}\}$.

14.29 Example A partition of $A_4^4 = S_4$ into 4 perfect deletion-correcting codes $S_{4,a}$.

0123	1023	0213	1230
1032	2013	0312	0132
2031	3012	1302	0231
3021	0321	1203	3201
2130	1320	2301	3102
3120	2310	3210	2103

14.30 Remark Directed designs $T(t, k, v)$ (see §VI.20) were investigated in [1436, 1437] as perfect s-deletion-correcting codes in A_v^n where $k = n$ and $t = n - s$. Thus, Theorem 14.28 implies that for each k, S_k can be partitioned into k directed designs $T(k-1, k, k)$.

14.31 Theorem [1437] If there exists a t-wise balanced design with parameters t-$(v, K, 1)$, where $K \subseteq \{k, \ldots, v\}$ and for each $n \in K$, there exists $T(t, k, n)$, a $T(t, k, v)$ exists.

14.32 Remark All known infinite families and many examples of $T(t, k, v)$ with $t \geq 3$ can be constructed using Theorem 14.31. See §VI.63 for results on t-wise balanced designs.

14.33 Conjecture For $3 \leq t \leq k - 2$, directed designs $T(t, k, k)$ do not exist except for $T(4, 6, 6)$ (found in [1554]).

14.34 Remark If multiple occurrences of symbols are permitted in the strings, analogous definitions yield codes (still termed *perfect s-deletion-correcting codes*) denoted $T^*(t, k, v)$. The existence of a $T^*(t, k, v)$ implies the existence of a $T(t, k, v)$. The existence of $T^*(2, k, v)$ has been completely settled for $3 \leq k \leq 6$ (with four possible exceptions when $k = 6$). It has been shown that a $T^*(2, 7, v)$ exists for all $v \geq 2350$ and that a $T^*(3, 4, v)$ exists when v is even. See [2113, 2115] and references therein.

See Also

§VI.20 §VI.63	Directed designs are the same as perfect deletion-correcting codes. t-wise balanced designs are used to construct deletion-correcting codes.
[1136]	Tables of best known codes for the "edit distance" allowing deletions, insertions, and substitutions.

References Cited: [311, 409, 909, 1103, 1136, 1345, 1427, 1433, 1434, 1435, 1436, 1437, 1440, 1441, 1521, 1554, 2017, 2113, 2115, 2186, 2198]

15 Derandomization

K. Gopalakrishnan
Douglas R. Stinson

15.1 Monte Carlo Algorithms

15.1 A *decision problem* is a problem that has a "yes" or "no" answer for every problem instance I.

15.2 A *yes-biased Monte Carlo Algorithm* having error probability ϵ is a randomized algorithm to solve a decision problem such that:

1. If the instance I is a no-instance, then the algorithm answers "no."
2. If the instance I is a yes-instance, then the probability that the algorithm answers "yes" is at least $1 - \epsilon$.

A *no-biased* Monte Carlo Algorithm is defined analogously.

15.3 Algorithm Solovay–Strassen Algorithm for Composites

Input: an odd integer n;
choose a random integer a, $1 \leq a \leq n-1$;
if $\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod{n}$
then answer "no: n is prime"
else answer "yes: n is composite".

In this algorithm, $\left(\frac{a}{n}\right)$ is a Jacobi symbol (see §VII.8). The Solovay–Strassen algorithm for Composites is a yes-biased Monte Carlo algorithm having error probability $\epsilon \leq 1/2$.

15.4 Remark Despite the fact that Monte Carlo algorithms can give wrong answers, the error probability can be made as small as desired by repeated application of the algorithm. Suppose one has a yes-biased algorithm and applies the algorithm k times. If at least one "yes" answer is obtained, then the algorithm is finished, since the instance I must be a yes-instance. On the other hand, if I is a yes-instance, then the probability of getting k "no" answers is at most ϵ^k.

15.2 Two-Point Based Sampling

15.5 Remark The analysis in Remark 15.4 is based on the assumption that the random numbers used in successive trials are independent. In the implementation of randomized algorithms in practice, one typically uses a pseudo-random number generator, which invalidates this assumption.

Two-point sampling, an alternative technique developed by Chor and Goldreich [496], is amenable to more realistic implementation and analysis. This technique essentially uses orthogonal arrays. Suppose $\log n$ random bits are needed for one trial of the algorithm and k trials of the algorithm are to be conducted. Instead of generating $k \log n$ random bits, which would ensure independence, one can use orthogonal arrays to generate pairwise independent random numbers as follows. Consider any $OA(2, k, n)$. This array has n^2 rows. Generate $2 \log n$ random bits and use them to index a specific row of the OA. Now apply the Monte Carlo algorithm using the k points that are elements of the row selected. By elementary combinatorial arguments

[931], the probability of getting k "no" answers for a yes-instance is bounded above by $\frac{\epsilon}{1+(k-1)(1-\epsilon)}$.

15.6 Example An application of the two-point sampling technique, to the problem of random pattern VLSI chip testing, deserves special mention due to its practical importance. Consider a combinational circuit with n inputs. One can test the circuit by applying all 2^n possible test vectors to the circuit and checking for the response of the circuit. As the number of test patterns is too high for exhaustive testing, usually the circuit is tested with some smaller number of random input patterns. The probability of not detecting a specific fault in the circuit can then be analyzed. But the analysis is invalid if successive test vectors applied are not independent.

In view of this problem, Spencer [1950] developed a pseudo-random pattern generator based on the idea of two-point sampling. This generator can be efficiently implemented as a modification of the classical linear feedback shift register (LFSR), and it is amenable to a realistic analysis. This generator is, in fact, an orthogonal array $OA(2, k, 2^n)$.

15.7 Remark Dukes and Ling [759] considered the natural generalization of two-point sampling that uses an orthogonal array $OA(t, k, n)$. This method is called t-point sampling because an $OA(t, k, n)$ contains n^t rows and a t-tuple of points serves to identify a unique row in the orthogonal array. The resulting error bound (for even t) is stated in Theorem 15.8. A slightly different bound is proven for odd t.

15.8 Theorem The error probability of $2s$-point sampling, using an $OA(2s, k, n)$, is at most

$$\frac{\epsilon^s}{\sum_{i=0}^{s} \binom{k-1-i}{s-i}(1-\epsilon)^{s-i}}.$$

15.3 Total Derandomization

15.9 Remark In some randomized algorithms for search problems, it is possible to eliminate completely the random bits needed, thus converting the algorithm into a deterministic algorithm. This process is *(total) derandomization*. Using orthogonal arrays of strength t, derandomization can be accomplished for randomized algorithms whose analysis depends only on t-wise rather than fully independent random choices. This method was first developed by Luby [1486] for the case $t = 2$ in the context of the maximal independent set problem and later generalized to arbitrary strength t by Alon, Babai, and Itai [77].

15.10 Example An illustration of the idea using the "Monochromatic K_4s" problem [79].

For any integer $n \geq 4$, there is an edge-coloring of K_n with two colors such that the number of monochromatic induced K_4s is at most $\binom{n}{4}/32$. This can be seen using a probabilistic argument as follows. For a 2-edge-coloring c of K_n, let $M(c)$ denote the number of monochromatic induced K_4s. Let $\overline{M}$ denote the average value of $M(c)$ over all colorings c. Then

$$\begin{aligned} \overline{M} \times 2^{\binom{n}{2}} &= \sum_c M(c) &&= \sum_{A \subseteq V, |A|=4} |\{c : |\{c(u,v) : u, v \in A\}| = 1\}| \\ &= \binom{n}{4} \times 2 \times 2^{\binom{n}{2}-6} &&= \binom{n}{4} \times 2^{\binom{n}{2}-5}. \end{aligned}$$

Hence $\overline{M} = \binom{n}{4}/32$. So there must exist a coloring with at most $\binom{n}{4}/32$ monochromatic induced K_4s.

How would one actually find such a coloring? A randomized algorithm would simply generate a random coloring and check whether it has the desired property. Since the total number of possible colorings, $2^{\binom{n}{2}}$, is exponential in n, it is not possible to test every coloring in polynomial time. Hence, there is no guarantee that a suitable coloring is found in time $poly(n)$.

However, it is not necessary that the color of every edge be chosen independently at random. It suffices to consider a sample space $\mathbf{S}$ where every subset of six edges has colors chosen independently at random. Since only a 6-wise independent sample space is needed, the rows of an $\mathrm{OA}_\lambda\left(6, \binom{n}{2}, 2\right)$ can be used as the sample space $\mathbf{S}$. A deterministic algorithm checks the colorings determined by all the rows of the OA, until one is found in which the number of monochromatic induced K_4s is at most $\binom{n}{4}/32$.

The proof that this approach works is as follows: Within the sample space $\mathbf{S}$,

$$\begin{aligned} \overline{M} \times \lambda 2^6 &= \textstyle\sum_{c\in\mathbf{S}} M(c) \\ &= \textstyle\sum_{A\subseteq V, |A|=4} |\{c \in \mathbf{S} : |\{c(u,v) : u, v \in A\}| = 1\}| \\ &= \textstyle\binom{n}{4} \times 2\lambda, \end{aligned}$$

and so $\overline{M} = \binom{n}{4}/32$, as before.

Now, it is possible to check deterministically any particular coloring in polynomial time. Thus, one has a polynomial-time deterministic algorithm provided that $\lambda = poly(n)$. This can be accomplished as follows. Let m be such that $\binom{n}{2} \le 2^m - 1$. Then construct an orthogonal array $\mathrm{OA}_{2^{3(m-2)}}\left(6, \binom{n}{2}, 2\right)$ as the dual code of a BCH code with designed distance 7 (see §VII.1). The size of the sample space is $O(n^6)$, and so it is a $poly(n)$-sized sample space.

15.11 Remark More generally, suppose that the analysis of a randomized algorithm does not require the complete independence of n random bits, but only t-wise independence. Then, one can use any $OA_\lambda(t, n, 2)$ as the sample space instead of the sample space with 2^n points. As in Example 15.10, appropriate sample spaces can be obtained from BCH codes with designed distance $t + 1$, as shown in Theorem 15.12.

15.12 Theorem Suppose that $n = 2^m - 1$ and $t = 2e$. Then there exists an orthogonal array $OA_{2^{e(m-2)}}(2e, n, 2)$, which yields a t-wise independent sample space of size $(n + 1)^e$.

15.13 Remark This approach can also be parallelized. Thus, it yields both a $poly(n)$-time sequential algorithm and a $polylog(n)$-time parallel algorithm with $poly(n)$ processors.

See Also

§III.3	Orthogonal arrays of strength 2.
§III.7	Orthogonal arrays of strength $t > 2$.
[258]	Section 15.6 discusses OAs and resilient functions.
[996]	A general survey of randomized algorithms.
[1219]	Chapter 26 concerns derandomization.
[1971]	Chapter 11 discusses OAs and two-point sampling.
[2138]	A collection of references on pairwise independence and derandomization techniques.

References Cited: [77, 79, 258, 496, 759, 931, 996, 1219, 1486, 1950, 1971, 2138]

16 Difference Families

R. Julian R. Abel
Marco Buratti

16.1 Definitions and Examples

16.1 Let $B = \{b_1, ..., b_k\}$ be a subset of an additive group G. The *G-stabilizer* of B is the subgroup G_B of G consisting of all elements $g \in G$ such that $B + g = B$. B is *full* or *short* according to whether G_B is or is not trivial. The *G-orbit* of B is the set $Orb_G B$ of all distinct right translates of B, namely, $Orb_G B = \{B + s \mid s \in S\}$ where S is a complete system of representatives for the right cosets of G_B in G.

16.2 The *list of differences from B* is the multiset $\Delta B = \{b_i - b_j \mid i, j = 1, \ldots, k; i \neq j\}$. The multiplicity in ΔB of an element $g \in G$ is of the form $\mu_g |G_B|$ for some integer μ_g. The *list of partial differences from B* is the multiset ∂B where each $g \in G$ appears exactly μ_g times.

16.3 **Remark** $\Delta B = \partial B$ if and only if B is a full block.

16.4 Let G be a group of order v. A collection $\{B_1, ..., B_t\}$ of k-subsets of G form a (v, k, λ) *difference family* (or *difference system*) if every nonidentity element of G occurs λ times in $\partial B_1 \cup ... \cup \partial B_t$. The sets B_i are *base blocks*. A difference family having at least one short block is *partial*.

16.5 **Remarks**

1. All definitions given can be extended to a multiplicative group by replacing $B+g$ with $B \cdot g$ and $b_i - b_j$ with $b_i b_j^{-1}$.
2. If $t = 1$, then B_1 is a (v, k, λ) difference set. (See §VI.18.)
3. If $\{B_1, \ldots, B_t\}$ is a (v, k, λ) difference family over the group G, then $Orb_G(B_1) \cup \ldots \cup Orb_G(B_t)$ is the collection of blocks of a BIBD(v, k, λ) admitting G as a sharply point-transitive automorphism group. This BIBD is *cyclic (abelian, nonabelian, dihedral, ...)* if the group G has the respective property. In this case the difference family is a *cyclic (abelian, nonabelian, dihedral, ...) difference family*.
4. A BIBD(v, k, λ) with an automorphism group G acting sharply transitively on the points is (up to isomorphisms) generated by a suitable (v, k, λ) difference family.
5. Every short block of a $(v, k, 1)$ difference family over an abelian group G is a coset of a suitable subgroup of G.

16.6 **Examples**

1. $B_1 = \{0, 1, 3, 5, 10, 11\}$, $B_2 = \{0, 6, 1, 7, 3, 9\}$, and $B_3 = \{0, 4, 8, 1, 5, 9\}$ form a (12,6,5) difference family over $\mathbb{Z}_{12}$. The stabilizers of B_1, B_2, B_3 are $\{0\}$, $\{0, 6\}$, and $\{0, 4, 8\}$, respectively.
2. $B_1 = \{1, x, x^4\}$, $B_2 = \{1, x^2, yx\}$, $B_3 = \{1, x^5, y\}$, $B_4 = \{1, x^6, yx^2\}$, and $B_5 = \{1, x^7, yx^5\}$ form a (16,3,2) difference family over the dihedral group $< x, y | x^8 = y^2 = 1; yx = x^7 y >$.

3. The set of order p subgroups of $\mathbb{F}_{p^n}$ form a $(p^n, p, 1)$ difference family generating the point-line design associated with the affine geometry $AG(n, p)$.
4. For further difference families over nonabelian (Frobenius type) groups, see the $(21, 6, 4)$, $(57, 9, 3)$, $(111, 6, 1)$ and $(171, 6, 1)$ BIBDs in Table II.3.32.

16.7 Let H be a subgroup of order h of a group G of order v. A collection $\{B_1, ..., B_t\}$ of k-subsets of G forms a (v, h, k, λ) *difference family over G and relative to H* if $\partial B_1 \cup ... \cup \partial B_t$ covers each element of $G - H$ exactly λ times and covers no element in H.

16.8 Remarks

1. A $(v, 1, k, \lambda)$ difference family simply is a (v, k, λ) difference family.
2. If $\{B_1, \ldots, B_t\}$ is a (v, h, k, λ) difference family over G and relative to H, then $Orb_G(B_1) \cup \ldots \cup Orb_G(B_t)$ is the collection of blocks of a (k, λ) GDD of type $h^{v/h}$ where the groups are the right cosets of H in G. This GDD admits G as a sharply point-transitive automorphism group.
3. A (k, λ) GDD of type $h^{v/h}$ with an automorphism group G acting sharply transitively on the points is, up to isomorphisms, generated by a suitable (v, h, k, λ) difference family.
4. If $\{B_1, \ldots, B_t\}$ is a (v, k, k, λ) difference family over G and relative to H, then $\{B_1, \ldots, B_t\} \cup \{\underbrace{H, ..., H}_{\lambda \text{ times}}\}$ is a (v, k, λ) difference family.

16.9 Remark Sometimes the BIBD generated by a difference family over G may possess automorphisms other than those generated by G. If such an automorphism is also an automorphism of the group G, then it is a *multiplier* of the DF. The most common situation occurs when G is an additive group and one can define multiplication as well as addition over G (G is a ring). When this occurs, the definitions below apply. However, not all multipliers are of this type. For instance, if G is the order 16 dihedral group $< x, y | x^8 = y^2 = 1; yx = x^7 y >$, then the base blocks $\{1, x, x^3, yx^2\}$, $\{1, x, x^3, yx^6\}$ together with the short block $\{1, x^4, y, yx^4\}$ (2 times) generate a $(16, 4, 2)$ difference family with order 2 multiplier α where $\alpha(x^t) = x^t$ and $\alpha(yx^t) = yx^{t+4}$. For another case, see Examples 16.76(4).

16.10

1. $C = \{c_1, \ldots, c_k\}$ is a *multiple* of $B = \{b_1, \ldots, b_k\}$ if, for some w, $c_i = w \cdot b_i$ for all i.
2. w is a *multiplier* (of order n) of $B = \{b_1, \ldots, b_k\}$ if
   (a) for some $g \in G$, $B = w \cdot B + g$ $(= \{w \cdot b_1 + g, w \cdot b_2 + g \ \ldots \ w \cdot b_k + g\})$
   (b) $w^n = 1$ but $w^i \neq 1$ for $0 < i < n$.
3. w is a *multiplier* of a difference family D if, for each base block B in D, $w \cdot B + g = C$ for some base block C in D and some $g \in G$.
4. If q is a prime power and D is a (q, k, λ) difference family over $\mathbb{F}_q$ in which one base block, B, has a multiplier of order k or $k - 1$ and all other base blocks are multiples of B, then D is *radical*.

16.11 Examples

1. $B_1 = \{0, 1, 4\}, B_2 = \{0, 2, 8\}, B_3 = \{0, 5, 10\}$ form a partial (15,3,1) difference family over $\mathbb{Z}_{15}$ in which 2 is a multiplier of order 4 and B_3 is a short block.
2. $B_1 = \{0, 1, 3, 24\}, B_2 = \{0, 4, 9, 15\}, B_3 = \{0, 7, 17, 25\}$ form a (37,4,1) difference family over $\mathbb{Z}_{37}$ with no multiplier.
3. $B_1 = \{0, 1, 3, 24\}, B_2 = \{0, 10, 18, 30\} = 10 \cdot B_1, B_3 = \{0, 4, 26, 32\} = 26 \cdot B_1$ form a (37,4,1) difference family over $\mathbb{Z}_{37}$ in which 10 is a multiplier of order 3.

16.12 Examples $(v, 3, 1)$ cyclic difference families for $7 \le v \le 81$; short blocks are *slanted*.

v	Base Blocks							
7	0 1 3							
13	0 1 4	0 2 7						
15	0 1 4	0 2 9	*0 5 10*					
19	0 1 4	0 2 9	0 5 11					
21	0 1 3	0 4 12	0 5 11	*0 7 14*				
25	0 1 3	0 4 11	0 5 13	0 6 15				
27	0 1 3	0 4 11	0 5 15	0 6 14	*0 9 18*			
31	0 1 12	0 2 24	0 3 8	0 4 17	0 6 16			
33	0 1 3	0 4 10	0 5 18	0 7 19	0 8 17	*0 11 22*		
37	0 1 3	0 4 26	0 5 14	0 6 25	0 7 17	0 8 21		
39	0 1 3	0 4 18	0 5 27	0 6 16	0 7 15	0 9 20	*0 13 26*	
43	0 1 3	0 4 9	0 6 28	0 7 23	0 8 33	0 11 30	0 12 26	
45	0 1 3	0 4 10	0 5 28	0 7 34	0 8 32	0 9 29	0 12 26	*0 15 30*
49	0 1 3	0 4 9	0 6 17	0 7 23	0 8 30	0 10 31	0 12 36	0 14 34
51	0 1 3	0 4 9	0 6 25	0 7 35	0 8 22	0 10 21	0 12 27	0 13 31
	0 17 34							
55	0 1 3	0 4 9	0 6 16	0 7 32	0 8 29	0 11 42	0 12 27	0 14 36
	0 17 37							
57	0 1 3	0 4 9	0 6 13	0 8 26	0 10 33	0 11 32	0 12 40	0 14 41
	0 15 35	*0 19 38*						
61	0 1 3	0 4 9	0 6 13	0 8 25	0 10 33	0 11 30	0 12 32	0 14 40
	0 15 37	0 16 34						
63	0 1 3	0 4 9	0 6 13	0 8 25	0 10 41	0 11 44	0 12 36	0 14 37
	0 15 43	0 16 34	*0 21 42*					
67	0 1 3	0 4 9	0 6 13	0 8 23	0 10 38	0 11 33	0 12 42	0 14 32
	0 16 43	0 17 36	0 20 46					
69	0 1 3	0 4 9	0 6 13	0 8 24	0 10 38	0 11 47	0 12 32	0 14 40
	0 15 50	0 17 42	0 18 39	*0 23 46*				
73	0 1 3	0 4 10	0 5 35	0 7 32	0 8 24	0 9 55	0 11 53	0 12 52
	0 13 39	0 14 29	0 17 54	0 22 45				
75	0 1 67	0 2 47	0 3 41	0 4 69	0 5 68	0 11 55	0 13 61	0 15 33
	0 16 52	0 17 43	0 19 40	0 22 51	*0 25 50*			
79	0 1 29	0 2 19	0 3 14	0 4 42	0 5 13	0 6 22	0 7 52	0 9 55
	0 10 53	0 12 59	0 15 54	0 18 48	0 21 56			
81	0 1 39	0 2 58	0 3 34	0 4 21	0 5 67	0 6 15	0 7 36	0 8 59
	0 10 63	0 11 37	0 12 61	0 13 48	0 16 40	*0 27 54*		

16.13 Examples $(v, 3, 2)$ cyclic difference families.

v	Base Blocks							
16	0 1 2	0 2 8	0 3 7	0 4 7	0 5 10			
28	0 1 12	0 2 11	0 2 12	0 3 7	0 3 13	0 4 9	0 5 13	0 6 7
	0 6 14							
40	0 1 4	0 1 16	0 2 7	0 2 9	0 3 17	0 4 17	0 5 19	0 6 16
	0 6 18	0 8 18	0 8 19	0 9 20				

16.14 Examples $(v, 4, 1)$ cyclic difference families; short blocks are shown *slanted*.

v	Base Blocks					
13	0 1 3 9					
37	0 1 3 24	0 4 26 32	0 10 18 30			
40	0 1 4 13	0 2 7 24	0 6 14 25	*0 10 20 30*		
49	0 1 3 8	0 4 18 29	0 6 21 33	0 9 19 32		
52	0 1 3 7	0 5 19 35	0 8 20 31	0 9 24 34	*0 13 26 39*	
64	0 1 3 7	0 5 18 47	0 8 33 44	0 9 19 43	0 12 26 49	*0 16 32 48*
76	0 1 7 22	0 2 11 45	0 3 59 71	0 4 32 50	0 10 37 51	0 13 36 60
	0 19 38 57					
85	0 2 41 42	0 17 32 38	0 18 27 37	0 13 29 36	0 11 31 35	0 12 26 34
	0 5 30 33					

16.15 Examples $(v, 4, \lambda)$ cyclic difference families; short blocks are shown *slanted*.

v	Base Blocks					
11,6	0 1 8 9	0 2 5 7	0 1 4 5	0 2 3 5	0 4 5 9	
15,6	0 1 2 3	0 2 4 6	0 4 8 12	0 8 1 9	3 6 9 12	0 1 5 10
	0 2 5 10					
19,2	0 1 3 12	0 1 5 13	0 4 6 9			
21,3	0 2 3 7	0 3 5 9	0 1 7 11	0 2 8 11	0 1 9 14	
22,2	0 4 16 17	0 12 14 21	0 14 16 19	*0 4 11 15*		
29,3	0 2 5 7	0 1 12 13	0 4 19 23	0 3 22 25	0 6 15 21	0 8 9 17
	0 11 16 27					
31,2	0 1 8 11	0 1 13 17	0 2 11 14	0 5 7 13	0 5 9 15	
34,2	0 1 22 24	0 1 19 25	0 2 6 29	0 4 7 20	0 5 8 20	*0 8 17 25*
43,2	0 1 6 36	0 3 18 22	0 9 11 23	0 10 12 26	0 26 27 33	0 13 35 38
	0 19 28 39					
46,2	0 2 7 10	0 4 19 32	0 10 34 35	0 5 8 24	0 26 30 39	0 17 26 32
	0 28 34 45	*0 2 23 25*				

16.16 Examples $(v, 5, 1)$ cyclic difference families; short blocks are shown *slanted*. Those for $v = 121, 161, 201$ are *perfect* (as defined in §16.3).

v	Base Blocks			
21	0 1 4 14 16			
41	0 1 4 11 29	0 2 8 17 22		
61	0 1 3 13 34	0 4 9 23 45	0 6 17 24 32	
65	0 1 3 31 45	0 4 10 19 57	0 5 16 41 48	*0 13 26 39 52*
81	0 1 5 12 26	0 2 10 40 64	0 3 18 47 53	0 9 32 48 68
121	0 14 26 51 60	0 15 31 55 59	0 10 23 52 58	0 3 36 56 57
	0 7 18 45 50	0 8 30 47 49		
141	0 33 60 92 97	0 3 45 88 110	0 18 39 68 139	0 12 67 75 113
	0 1 15 84 94	0 7 11 24 30	0 36 90 116 125	
161	0 19 34 73 80	0 16 44 71 79	0 12 33 74 78	0 13 30 72 77
	0 11 36 67 76	0 18 32 69 75	0 10 48 68 70	0 3 29 52 53
201	0 1 45 98 100	0 3 32 65 89	0 4 54 70 75	0 6 49 69 91
	0 7 58 81 95	0 8 34 72 90	0 9 36 77 96	0 10 35 83 94
	0 12 40 79 92	0 15 46 76 93		
221	0 1 24 61 116	0 3 46 65 113	0 4 73 89 130	0 5 77 122 124
	0 6 39 50 118	0 7 66 81 94	0 8 38 64 139	0 9 29 80 107
	0 10 35 93 135	0 12 34 52 88	0 14 31 63 84	

16.17 Examples $(v, 5, \lambda)$ cyclic difference families; short blocks are shown *slanted*.

v, λ	Base Blocks				
13,5	0 1 2 4 8	0 1 3 6 12	0 2 5 6 10		
15,6	0 1 2 3 6	0 2 4 7 8	0 2 4 9 10	0 3 6 10 11	*0 3 6 9 12*
17,5	0 1 4 13 16	0 3 5 12 14	0 2 8 9 15	0 6 7 10 11	
31,2	0 1 3 7 15	0 3 9 14 21	0 4 5 13 15		
33,5	0 2 3 7 25	0 3 13 14 29	0 4 5 12 13	0 2 12 16 26	0 3 12 20 31
	3 9 12 15 27	0 8 13 14 31	0 2 7 13 29		
35,2	0 2 8 12 13	0 3 18 22 27	0 17 23 32 33	*0 7 14 21 28*	*0 7 14 21 28*
51,2	0 1 14 31 35	0 1 9 23 33	0 11 16 18 42	0 7 13 36 39	0 4 10 12 15
71,2	1 5 25 54 57	3 4 15 20 29	9 12 16 45 60	27 36 38 48 64	2 10 37 43 50
	6 8 30 40 58	18 19 24 32 49			

16.18 Examples $(v, 6, \lambda)$ cyclic difference families; short blocks are shown *slanted*.

v, λ	Base Blocks			
21,3	0 2 10 15 19 20	0 3 7 9 10 16		
21,5	0 2 6 12 15 16	0 3 6 7 11 19	0 7 15 16 17 18	*0 2 7 9 14 16*
22,5	0 1 2 5 10 13	0 1 5 6 8 15	0 2 3 6 16 18	*0 2 6 11 13 17*
28,5	0 4 7 8 16 21	5 7 8 9 14 20	7 12 14 16 17 25	1 4 7 13 14 24
	2 4 8 16 18 22			
33,5	0 3 12 17 18 28	0 2 3 16 28 29	0 16 20 26 28 30	0 2 3 12 16 27
	0 6 20 21 28 30	*0 4 11 15 22 26*		
39,5	0 3 4 17 19 32	0 1 5 12 30 36	0 3 8 9 25 27	0 7 10 12 17 21
	0 16 18 19 27 35	0 2 18 27 28 33	0 6 13 19 26 32	
41,3	0 1 10 16 18 37	0 6 14 17 19 26	0 2 20 32 33 36	0 11 12 28 34 38
46,2	0 1 3 11 31 35	0 1 4 10 23 29	0 2 7 15 32 41	
51,3	15 17 18 27 34 48	3 17 30 34 42 45	9 17 24 33 34 39	3 25 41 43 44 48
	3 5 25 29 43 48			
61,2	12 15 28 34 35 59	1 13 18 47 51 53	8 10 11 21 29 43	16 20 25 32 40 50
61,3	0 1 9 20 58 34	0 2 7 18 40 55	0 4 14 19 36 49	0 8 11 28 37 38
	0 13 15 16 22 56	0 26 30 32 44 51		
91,1	0 1 3 7 25 38	0 16 21 36 48 62	0 30 40 63 74 82	

16.19 Theorem There exists a $(v, 3, 1)$ cyclic difference family for every $v \equiv 1, 3 \pmod 6$. Constructions VI.53.17 and VI.53.19 give one explicit solution for each congruence class.

16.20 A *disjoint difference family* is a difference family where every pair of base blocks is disjoint.

16.21 Theorem (see [719]) There exists a $(v, 3, 1)$ disjoint cyclic difference family for every $v \equiv 1, 3 \pmod 6$ except $v = 9$.

16.22 Remark Novak's conjecture (Conjecture I.2.111) states that in *every* cyclic Steiner triple system $(V, \mathcal{B})$ of order $v \equiv 1 \pmod 6$, it is always possible to find a set of $(v-1)/6$ blocks from $\mathcal{B}$ that form a $(v, 3, 1)$ *disjoint* cyclic difference family.

16.23 Theorem [590] If $v \equiv 1, 3 \pmod{\frac{6}{\gcd(6,\lambda)}}$ and $(v, \lambda) \neq (9,1)$ or $(9,2)$, there exists a $(v, 3, \lambda)$ difference family (possibly partial) over $\mathbb{Z}_v$, except when $v \equiv 2 \pmod 4$ and $\lambda \equiv 2 \pmod 4$.

16.24 Construction When $v = 2t + 1$, $t \geq 1$, the set $\{\{0, i, 2i\} : 1 \leq i \leq t\}$ is a $(v, 3, 3)$-difference family over $\mathbb{Z}_v$.

16.25 Theorem Suppose $q \equiv 7 \pmod{12}$ is a prime power and there exists a cube root of unity ω in $\mathbb{F}_q$ such that $x = \omega - 1$ is a primitive root. Then the following base blocks form a $(7q,4,1)$ difference family over $\mathbb{Z}_7 \times \mathbb{F}_q$:

1. $\{(0,0), (0,(x-1)x^{2t-1}), (0,\omega(x-1)x^{2t-1}), (0,\omega^2(x-1)x^{2t-1})\}$ for $1 \le t \le (q-7)/12$,
2. $\{(0,0), (1,x^{2t}), (2,\omega x^{2t}), (4,\omega^2 x^{2t})\}$ for $1 \le t \le (q-3)/2$, $x^{2t} \ne \omega$, and
3. $\{(0,0), (2^t,\omega^t), (2^t, x\cdot\omega^t), (2^{t+2},0)\}$ for $0 \le t \le 2$.

16.26 Remark $(7q,4,1)$ difference families are obtainable by Theorem 16.25 for $q = 7$, 19, 31, 43, 67, 79, 103, 127, 151, 163, 199, 211, 367, 379, 439, 463, 487, 571, but not for $q = 139$, 223, 271, 283, 307, 331, 523, 547. A more general construction for $(7q,4,1)$ difference families with q a prime power $\equiv 7 \pmod{12}$ can be found in [23].

16.27 Remark Theorem 16.28 updates some known results for $k = 4, 5$ in [1537].

16.28 Theorem [23, 30]

1. A $(12t{+}1,4,1)$ difference family exists for $1 \le t \le 50$ except for $t = 2$.
2. A $(20t{+}1,5,1)$ difference family exists for $1 \le t \le 50$ except possibly for $t = 16$, 25, 31, 34, 40, 45.

16.29 Theorem [2144] Suppose q is a prime power, and $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$. Then a (q,k,λ) difference family over $\mathbb{F}_q$ exists if one of the following holds:

1. λ is a multiple of $k/2$ or $(k-1)/2$.
2. $\lambda \ge k(k-1)$.
3. $q > \binom{k}{2}^{k(k-1)}$.

16.30 Examples More (v,k,λ) cyclic difference families; short blocks are again slanted.

v,k,λ	Base Blocks
21,10,9	{0,1,2,3,4,7,8,11,14,16}, {0,6,7,9,11,12,15,16,17,19}
21,8,14	{0,9,10,13,14,15,18,19}, {0,1,4,7,9,15,16,18}, {0,1,2,4,6,14,15,16}, {0,1,3,4,8,14,16,18}, {0,1,4,9,11,12,14,16}
22,7,4	{0,2,6,8,9,10,13}, {0,3,5,6,12,13,17}
22,8,8	{0,1,5,7,13,17,20,21}, {0,2,7,11,13,14,16,17}, {0,3,4,12,14,15,17,21}
22,8,12	{1,2,3,5,6,9,15,18}, {1,2,3,5,8,9,10,15}, {1,3,4,9,13,18,19,21}, {*2,4,6,12,13,15,17,1*}, {*2,4,8,12,13,15,19,1*}, {*2,4,8,16,13,15,19,5*}
29,7,3	{1,7,16,20,23,24,25}, {2,3,11,14,17,19,21}
29,8,4	{0,1,7,16,20,23,24,25}, {0,2,3,11,14,17,19,21}
29,8,6	{0,5,10,11,12,13,16,20}, {0,8,10,12,17,22,23,26}, {0,4,5,11,13,23,25,26}
34,12,8	{0,5,9,14,15,17,20,25,26,27,28,30}, {0,6,7,10,13,17,18,20,22,24,25,26}
34,12,10	{0,2,3,4,8,9,11,13,14,24,27,30}, {0,2,6,7,8,11,13,14,22,25,26,32}, {*0,2,10,18,22,32,17,19,27,1,5,15*}
37,10,5	{0,1,7,9,10,12,16,26,33,34}, {0,2,14,15,18,20,24,29,31,32}
43,7,2	{0,1,11,19,31,38,40}, {0,2,10,16,25,38,42}
43,7,3	{1,4,11,16,21,35,41}, {3,5,12,19,20,33,37}, {9,13,14,15,17,25,36}
43,8,4	{0,1,4,11,16,21,35,41}, {0,3,5,12,19,20,33,37}, {0,9,13,14,15,17,25,36}
43,15,10	{1,3,6,13,18,21,22,25,26,27,33,35,36,38,40}, {9,10,11,13,16,17,19,23,26,27,28,33,35,38,39}
45,11,5	{1,3,7,10,22,25,30,35,37,38,44}, {0,2,3,14,22,26,27,28,31,32,38}
46,10,4	{3,7,13,16,23,24,25,28,30,42}, {2,10,12,18,25,34,40,43,44,45}
46,10,5	{0,4,6,11,12,15,24,25,28,42}, {0,2,5,7,8,9,14,24,34,35}, {*0,2,12,32,40,23,25,35,9,17*}
46,10,6	{0,2,11,13,21,22,30,33,34,40}, {0,2,6,7,22,23,28,32,35,38}, {0,2,4,7,8,9,12,23,26,41}
49,9,3	{0,1,3,5,9,14,19,25,37}, {0,2,12,13,16,19,34,41,42}

v,k,λ	Base Blocks
53,13,6	{1,10,13,15,16,24,28,36,42,44,46,47,49}, {2,3,19,20,26,30,31,32,35,39,41,45,48}
53,14,7	{0,1,10,13,15,16,24,28,36,42,44,46,47,49}, {0,2,3,19,20,26,30,31,32,35,39,41,45,48}
55,9,4	{0,4,21,25,26,42,45,53,54}, {0,6,8,25,37,39,45,48,52}, {2,5,6,13,15,20,25,39,45}
55,10,5	{0,5,11,15,20,22,25,33,44,45}, {3,7,8,10,31,37,39,45,46,49} twice
57,7,3	{0,1,11,12,15,35,53}, {0,7,17,20,27,29,48}, {0,5,18,26,32,49,51}, {0,2,6,9,14,41,42}
61,10,3	{1,4,18,20,32,35,36,41,42,54}, {11,13,14,21,23,28,34,39,43,47}
61,15,7	{0,1,3,4,8,10,13,22,30,35,44,45,46,50,58}, {0,1,3,5,13,18,29,34,35,37,41,43,44,51,55}
67,11,5	{1,9,14,15,22,24,25,40,59,62,64}, {2,13,18,28,30,44,48,50,51,57,61}, {4,21,26,29,33,35,36,47,55,56,60}
67,12,4	{1,8,23,25,28,29,31,37,47,54,55,64}, {3,20,25,32,36,39,44,45,54,55,57,59}
67,12,6	{0,1,9,14,15,22,24,25,40,59,62,64}, {0,2,13,18,28,30,44,48,50,51,57,61}, {0,4,21,26,29,33,35,36,47,55,56,60}
71,7,3	{1,20,30,32,37,45,48}, {2,3,19,25,40,60,64}, {4,6,9,38,49,50,57}, {5,8,12,18,27,29,43}, {10,15,16,24,36,54,58}
71,8,4	{0,1,20,30,32,37,45,48}, {0,2,3,19,25,40,60,64}, {0,4,6,9,38,49,50,57}, {0,5,8,12,18,27,29,43}, {0,10,15,16,24,36,54,58}
73,10,5	{0,1,2,4,8,16,32,37,55,64}, {0,5,7,10,14,20,28,39,40,56}, {0,25,27,35,49,50,54,61,67,70}, {0,11,15,21,22,30,42,44,47,60}
85,7,2	{0,1,11,20,32,35,39}, {0,2,6,16,29,50,65}, {0,3,9,27,55,72,80}, {0,5,7,30,47,48,59}
85,7,3	{0,7,23,27,28,31,71}, {0,12,22,41,61,74,79}, {0,6,11,13,38,42,77}, {0,1,7,16,19,27,49}, {0,9,26,39,54,56,71}, {0,2,3,12,37,53,63}
85,8,2	{24,31,39,50,67,68,70,82}, {20,49,51,55,56,60,72,81}, {9,19,29,37,43,56,59,81}
97,9,3	{1,2,25,35,46,58,61,70,90}, {3,4,8,38,43,50,69,86,87}, {6,12,16,32,53,55,57,75,82}, {9,18,24,26,31,34,37,48,64}
181,10,2	{1,7,40,42,51,59,113,125,135,151}, {19,22,31,35,36,64,74,133,154,156}, {10,15,34,47,58,65,83,87,161,164}, {12,18,32,52,77,78,142,157,165,172}
217,7,1	{0,1,37,67,88,92,149}, {0,15,18,65,78,121,137}, {0,8,53,79,85,102,107}, {0,11,86,100,120,144,190}, {0,29,64,165,198,205,207}, {*0,31,62,93,124,155,186*}

16.31 Examples Difference families over products of cyclic groups.

v,k,λ	Group	Base Blocks
25,7,7	$\mathbb{Z}_5 \times \mathbb{Z}_5$	{(0,0),(0,1),(0,4),(1,1),(1,2),(4,3),(4,4)}, {(0,0),(1,0),(1,3),(2,3),(3,2),(4,0),(4,2)}, {(0,0),(0,2),(0,3),(2,2),(2,4),(3,1),(3,3)}, {(0,0),(1,4),(2,0),(2,1),(3,0),(3,4),(4,1)}
25,8,7	$\mathbb{Z}_5 \times \mathbb{Z}_5$	{(0,1),(0,2),(0,3),(0,4),(1,2),(2,4),(3,1),(4,3)}, {(1,0),(2,0),(3,0),(4,0),(1,1),(2,2),(3,3),(4,4)}, {(1,3),(2,1),(3,4),(4,2),(1,4),(2,3),(3,2),(4,1)}
45,5,1	$\mathbb{Z}_3^2 \times \mathbb{Z}_5$	{(0,1,0),(0,2,0),(1,0,2),(2,0,2),(0,0,1)}, {(2,1,0),(1,2,0),(2,2,2),(1,1,2),(0,0,1)}, {*(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,0,4)*}
75,5,2	$\mathbb{Z}_5 \times \mathbb{Z}_{15}$	{(0,0),(1,10),(1,2),(4,1),(4,2)}, {(0,0),(2,5),(2,10),(3,7),(3,13)}, {(0,0),(1,10),(1,8),(4,4),(4,8)}, {(0,0),(2,5),(2,10),(3,14),(3,11)}, {(0,0),(1,4),(1,5),(4,1),(4,8)}, {(0,0),(1,1),(1,5),(4,4),(4,2)}, {(0,0),(2,7),(2,13),(3,1),(3,4)}, {*(0,0),(1,0),(2,0),(3,0),(4,0)*} (twice)

v,k,λ	Group	Base Blocks
121,6,1	$\mathbb{Z}_{11}\times\mathbb{Z}_{11}$	{(0,0),(0,3),(0,4),(1,1),(1,7),(4,6)}, {(0,0),(0,2),(2,5),(4,7),(6,4),(8,0)}, {(0,0),(1,5),(2,0),(4,1),(6,0),(7,2)}, {(0,0),(1,0),(3,9),(4,8),(6,1),(9,5)}
121,10,3	$\mathbb{Z}_{11}\times\mathbb{Z}_{11}$	{(0,1),(0,3),(0,4),(0,5),(0,9),(1,8),(3,2),(4,10),(5,7),(9,6)}, {(1,2),(3,6),(4,8),(5,10),(9,7),(10,2),(8,6),(7,8),(6,10),(2,7)}, {(1,7),(3,10),(4,6),(5,2),(9,8),(1,4),(3,1),(4,5),(5,9),(9,3)}, {(10,10),(8,8),(7,7),(6,6),(2,2),(1,0),(3,0),(4,0),(5,0),(9,0)}
121,16,4	$\mathbb{Z}_{11}\times\mathbb{Z}_{11}$	{(0,0),(0,1),(0,3),(0,9),(0,5),(0,4),(2,1),(6,3), (7,9),(10,5),(8,4),(1,8),(3,2),(9,6),(5,7),(4,10)}, {(0,0),(8,3),(2,9),(6,5),(7,4),(10,1),(10,7),(8,10), (2,8),(6,2),(7,6),(8,1),(2,3),(6,9),(7,5),(10,4)}
153,9,2	$\mathbb{Z}_3^2\times\mathbb{Z}_{17}$	{*(0,0,0),(0,1,0),(0,2,0),(1,0,0),(1,1,0),(1,2,0),(2,0,0),(2,1,0), (2,2,0)*} (twice), {(0,0,0),(0,1,t),(0,1,16t),(0,2,4t),(0,2,13t), (1,0,3t),(1,0,14t),(2,0,5t),(2,0,12t)} for t =1, 2, 3, and 6.
175,7,1	$\mathbb{Z}_7\times\mathbb{Z}_5^2$	{*(0,0,0),(1,0,0),(2,0,0),(3,0,0),(4,0,0),(5,0,0),(6,0,0)*}, {(0,0,0),(1,1,3),(1,4,2),(2,2,2),(2,3,3),(4,2,0),(4,3,0)}, {(0,0,0),(1,3,4),(1,2,1),(2,2,2),(2,3,2),(4,0,2),(4,0,3)}, {(0,0,0),(1,1,2),(1,4,3),(2,1,4),(2,4,4),(4,0,1),(4,0,4)}, {(0,0,0),(1,3,1),(1,2,4),(2,4,1),(2,1,4),(4,1,0),(4,4,0)}
259,7,1	$\mathbb{Z}_7\times\mathbb{Z}_{37}$	{*(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0)*}, $\{(0,0),(0,z),(0,6z),(y,4z),(2y,19z),(3y,25z),(6y,25z)\}$, $\{(0,0),(0,4z),(y,25z),(y,34z),(2y,24z),(2y,35z),(4y,10z)\}$, for (y,z) = (1,1), (2,10) and (4,26).

16.32 Example A (49,21,10) difference family over $\mathbb{Z}_7\times\mathbb{Z}_7$. Base blocks are the short block $\bigcup_{i=0}^{6}\{(i,1),(i,2),(i,4)\}$, and the block

$$\left(\bigcup_{i=1,2,4}\{(i,0),(i,1),(i,2),(i,4)\}\right)\cup\left(\bigcup_{i=3,5,6}\{(i,3),(i,5),(i,6)\}\right).$$

16.2 Basic Recursive Constructions

16.33 Theorem [379] If there exists a (q,k,λ) difference family for every prime factor q of v, then there exists a (v,k,λ) difference family over any group G of order v.

16.34 Theorem [1220] If there exist (v_i,k,λ_i) difference families over H_i for $i=1,2$ and a (v_2,k,λ_2) difference matrix over H_2, then a $(v_1v_2,k,\lambda_1\lambda_2)$ difference family over $H_1\times H_2$ exists.

16.35 Theorem Suppose that there exists a (v,k,λ_1) (possibly partial) difference family over $\mathbb{Z}_v$ having μ base blocks in the orbit of $\{0,\frac{v}{k},2\frac{v}{k},\ldots,(k-1)\frac{v}{k}\}$, and all other base blocks generating v distinct blocks under the action of $\mathbb{Z}_v$. If in addition there exist

1. a $(u,k,(\lambda_1-\mu)\lambda_2)$ (possibly partial) difference family over $\mathbb{Z}_u$,
2. a $(ku,k,\mu\lambda_2)$ partial difference family over $\mathbb{Z}_{ku}$, and
3. a (u,k,λ_2)-difference matrix over $\mathbb{Z}_u$,

then there exists a $(uv,k,\lambda_1\lambda_2)$ difference family over $\mathbb{Z}_{uv}$.

16.36 Corollary

1. Let k be a prime or prime power, and $v\equiv 1 \pmod{k(k-1)}$. If a $(v,k,1)$ difference family over $\mathbb{Z}_v$ exists and a $(u,k,1)$ (possibly partial) difference family over $\mathbb{Z}_u$ exists, then a $(uv,k,1)$ difference family over $\mathbb{Z}_{uv}$ exists.

2. Let k be prime and $v \equiv k \pmod{k(k-1)}$. If a $(v,k,1)$ partial difference family over $\mathbb{Z}_v$ exists and a $(ku,k,1)$ partial difference family over $\mathbb{Z}_{ku}$ exists, then a $(uv,k,1)$ partial difference family over $\mathbb{Z}_{uv}$ exists.

16.3 Perfect Difference Families

16.37 If $v = k(k-1)t+1$, then t blocks $B_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,k}\}$ form a *perfect* $(v,k,1)$ difference family over $\mathbb{Z}_v$ if the $tk(k-1)/2$ differences $b_{i,m} - b_{i,n}$ $(i = 1,\ldots,t,$ $1 \le m < n \le k)$ cover the set $\{1,2,\ldots,(v-1)/2\}$. If instead, they cover the set $\{1,2,\ldots,(v-3)/2\} \cup \{(v+1)/2\}$, the difference family is (*quasi-perfect).*

16.38 Example $\{0,1,12\}, \{0,2,8\}, \{0,5,9\}$, and $\{0,3,10\}$ form a perfect (25,3,1) difference family.

16.39 Theorem [225, p. 483] If $v \equiv 1$ or $7 \pmod{24}$, then a $(v,3,1)$ perfect difference family exists.

16.40 Theorem ([23, 1143, 1537] and §IV.19) Perfect $(12t{+}1,4,1)$ difference families are known for the following values of $t < 50$: 1, 4-33, 36 and 41.

16.41 Theorem [1537] Suppose a $(w,4,1)$ perfect difference family exists. Then there exist $(v,4,1)$ perfect difference families $v = 5w{+}8$, $13w$, $19w{+}30$, $23w{+}38$, $25t{+}36$, $25t{+}48$ and a quasi-perfect $(v,4,1)$ difference family for $v = 7w{+}6$.

16.42 Remark [30, 1537] $(20t+1,5,1)$ perfect difference families are known for $t = 6,8,10$ (see Example 16.16) but for no other small values of t.

16.43 Theorem There are no $(v,k,1)$ perfect difference families for the following values:

1. $k = 3$, $v \equiv 13$ or $19 \pmod{24}$,
2. $k = 4$, $v \in \{25, 37\}$,
3. $k = 5$, $v \equiv 21 \pmod{40}$ or $v \in \{41, 81\}$,
4. $k \ge 6$ [1537].

16.4 Prime Power Difference Families

16.44 Remarks Here (q,k,λ) difference families are examined, for q a prime power and all base blocks multiples of one block. For all of these, x denotes a primitive element of $\mathbb{F}_q$, B the initial base block, and n the highest order of a multiplier of B. The other base blocks are then $x^m \cdot B, x^{2m} \cdot B, \ldots, x^{(t-1)m} \cdot B$ for $t = \lambda(q-1)/(k(k-1))$ and $m = (q-1)/2t = k(k-1)/(2n\lambda)$. The initial block $B = \{b_1, b_2 \ldots b_k\}$ has the property that the $k(k-1)/2$ differences $b_i - b_j$ $(1 \le i < j \le k)$ are evenly spread among the multiplicative cosets H_i where $H_i = \{x^a : a \equiv i \pmod{k(k-1)/(2n\lambda)}\}$. Three main cases are considered: (1) $n = k$ or $k-1$ (radical difference families), (2) $n = 3$, and (3) $n = 1$ (no multiplier). If q is a power of a prime, x is taken to be a root of the appropriate primitive polynomial in Table 16.45.

16.45 Table Primitive polynomials for finite fields, $\mathbb{F}_q$, $q \le 7921$.

q	Polynomial	q	Polynomial	q	Polynomial
25	$x^2 - x - 3$	49	$x^2 - 3x - 2$	121	$x^2 - 8x - 3$
169	$x^2 - 4x - 7$	289	$x^2 - 6x - 3$	361	$x^2 - 6x - 6$
529	$x^2 - 7x - 4$	625	$x^4 + x^3 + x^2 + x + 3$	729	$x^6 - 2x - 1$
841	$x^2 - 3x - 2$	961	$x^2 - 3x - 7$	1369	$x^2 - 3x - 5$
1681	$x^2 - 5x - 7$	1849	$x^2 - 7x - 9$	2197	$x^3 - x^2 - 2$
2401	$x^4 - 3x^3 - x - 2$	2809	$x^2 - 3x - 3$	5041	$x^2 - 5x - 4$
5329	$x^2 - 3x - 5$	6889	$x^2 - 6x - 4$	7921	$x^2 - 2x - 6$

▷ Radical Difference Families

16.46 Theorem Suppose q is an odd prime power. Then there exists a (q, k, λ) radical difference family if either:

1. λ is a multiple of $k/2$ and $q \equiv 1 \pmod{k-1}$, or
2. λ is a multiple of $(k-1)/2$ and $q \equiv 1 \pmod{k}$.

16.47 Remark For radical difference families with $\lambda = 1$, the multiplier must have odd order (that is, order k if k is odd, or order $k-1$ if k is even).

16.48 Theorem [377] Let $q = 12t + 1$ be a prime power and 2^e be the largest power of 2 dividing t. Then a $(q, 4, 1)$ radical difference family in $\mathbb{F}_q$ exists if and only if -3 is not a 2^{e+2}th power in $\mathbb{F}_q$. (This condition holds for $q = 13$, 25, 73, 97, 109, 121, 169, 181, 193, 229, 241, 277, 289, 313, 337, 409, 421, 433, 457, 529, 541, 577, 601, 625, 673, 709, 733, 757, 769, 829, 841.)

16.49 Theorem [377] Let $q = 20t + 1$ be a prime power, and let 2^e be the largest power of 2 dividing t. Then a $(q, 5, 1)$ radical difference family in $\mathbb{F}_q$ exists if and only if $(11 + 5\sqrt{5})/2$ is not a 2^{e+1}th power in $\mathbb{F}_q$. (This condition holds for $q = 41$, 61, 81, 241, 281, 401, 421, 601, 641, 661, 701, 761, 821, 881.)

16.50 Remark In [378], necessary and sufficient conditions are given for a $(q, k, 1)$ radical difference family with $k \in \{6, 7\}$ to exist over $\mathbb{F}_q$; a sufficient condition is also given for $k \geq 8$.

16.51 Theorem [378, 957, 2144] $(q, k, 1)$ radical difference families exist, among others, for the following values of q and k:

1. $k = 6$: $q = 181$, 211, 241, 631, 691, 1531, 1831, 1861, 2791, 2851, 3061.
2. $k = 7$: $q = 337$, 421, 463, 883, 1723, 3067, 3319, 3823, 3907, 4621, 4957, 5167, 5419, 5881, 6133, 8233, 8527, 8821, 9619, 9787, 9829.
3. $k = 8$: $q = 449$, 1009, 3137, 3697, 6217, 6329, 8233, 9869.
4. $k = 9$: $q = 73$, 1153, 1873, 2017, 6481, 7489, 7561, 8359.

16.52 Theorem [888] If there exists a $(p, k, 1)$ radical difference family with p a prime and k odd, then there exists a cyclic RBIBD$(kp, k, 1)$ whose resolution is invariant under the action of $\mathbb{Z}_{kp}$.

▷ Difference Families Where the Blocks Have a Multiplier of Order 3

16.53 Remark Here $q \equiv 1 \pmod 3$ and w denotes a cube root of unity in $\mathbb{F}_q$. The initial base block is a union of sets of the form $\{c_i, w \cdot c_i, w^2 \cdot c_i\}$, plus the zero element of $\mathbb{F}_q$ if $k \equiv 1 \pmod 3$. For convenience, c_1 is taken to be 1. Tables 16.54 through 16.57 give the other c_is for $\lambda = 1$, $k \in \{6, 7, 9\}$ and $\lambda = 2$, $k = 9$.

16.54 Table $(q, 6, 1)$ difference families.

q	c_2	q	c_2	q	c_2	q	c_2	q	c_2
31	27	151	7	181	4	211	9	241	13
271	9	331	24	361	x^{42}	421	74	541	100
571	20	601	46	631	52	661	6	691	60
751	39	811	6	841	x^{164}	961	x^2	991	2
1021	29	1051	11	1171	112	1201	19	1231	53
1291	2	1321	11	1381	5	1471	12	1531	79
1621	8	1681	x^{112}	1741	21	1801	47	1831	63
1861	22	1951	16	2011	19	2131	84	2161	39

q	c_2	q	c_2	q	c_2	q	c_2	q	c_2
2221	20	2251	4	2281	37	2311	4	2341	37
2371	47	2401	x^6	2521	44	2551	5	2671	16
2731	58	2791	53	2851	111	2971	3	3001	9

16.55 Table $(q, 7, 1)$ difference families.

q	c_2	q	c_2	q	c_2	q	c_2	q	c_2
421	4	463	190	631	363	967	904	1009	115
1051	464	1093	936	1303	472	1429	1308	1723	898
1849	x^{223}	1933	1222	2017	139	2143	1063	2269	865
2311	1792	2437	929	2521	372	2647	1132	2689	156
2731	1504	2857	1537	3067	1052	3109	556	3319	2237
3361	2957	3529	2758	3571	3505	3613	1004	3697	370
3739	506	3823	1078	3907	1896	4159	3334	4201	3632
4243	3361	4327	145	4621	2115	4663	4658	4789	3279
4831	4251	4957	197	4999	3635	5041	x^{33}	5209	1865
5419	4060	5503	4907	5839	1501	5881	3387	5923	383
6007	2538	6133	5730	6217	4012	6301	1018	6343	5552
6427	3371	6469	3920	6637	4649	6763	391	7057	25

16.56 Table $(q, 9, 1)$ difference families.

q	c_2	c_3	q	c_2	c_3	q	c_2	c_3	q	c_2	c_3
937	82	211	1153	868	950	1297	233	810	1369	x^{30}	x^{223}
1657	11	855	1801	143	1740	1873	44	1540	2017	212	1506
2089	138	1570	2161	417	1858	2377	275	1942	2521	534	1002
2593	963	1430	2809	x^5	x^{145}	2953	572	2252	3169	989	1743
3313	464	1108	3457	322	2708	3529	564	2815	3673	735	933
3889	342	2179	4177	473	3595	4969	525	748	5041	x^2	x^{927}

16.57 Table $(q, 9, 2)$ difference families.

q	c_2	c_3	q	c_2	c_3	q	c_2	c_3	q	c_2	c_3
109	6	77	181	4	143	289	x^3	x^{49}	361	x^5	x^{93}
397	5	282	541	8	235	577	5	304	613	5	246
757	6	83	829	2	653	1117	2	220	1549	4	1501
1621	4	1361	1693	5	1202	2053	5	959	2197	x^2	x^{395}
2269	2	1441	2341	7	674	2557	5	531	2917	5	1618
3061	6	2496	3637	2	2151	3709	2	577	3853	2	1639
4357	5	2297	4789	2	1562	4861	11	1636	4933	25	918

16.58 Example A $(577, 9, 1)$ difference family. In $\mathbb{Z}_{577}$, $x = 5$ is a primitive element, and $w = 363$ is a cube root of unity. Base blocks are obtained by multiplying $B = \{1, w, w^2, 8, 8w, 8w^2, 208, 208w, 208w^2\}$ by x^{6i+24j} for $i = 0, 1$, $j = 0, 1, 2, 3$ [376].

▷ Difference Families Where No Base Block has a Multiplier

16.59 Remarks These are given for $\lambda = 1$, $k \in \{4, 5, 8\}$ and $\lambda = 2$, $k = 8$. They are also given for $\lambda = 1$, $k \in \{7, 9\}$ if no difference family with a multiplier of order 3 was possible (Remarks 16.44 apply here as well). The full initial base block is given for these difference families.

16.60 Example Consider a (q, k, λ) difference family for $(q, k, \lambda) = (61, 4, 1)$. Using the notation in Remarks 16.44, $n = 1$ (no multiplier), $t = \lambda(q-1)/k(k-1) = 5, m =$

$(q-1)/2t = 6$, and $x = 2$ is a primitive element of $\mathbb{F}_{61}$. Suitable base blocks are $B = \{0,1,5,11\}$, $2^6B = 3B = \{0,3,15,33\}$, $2^{12}B = 9B = \{0,9,45,38\}$, $2^{18}B = 27B = \{0,27,13,53\}$, and $2^{24}B = 20B = \{0,20,39,37\}$.

16.61 Table $(q,4,1)$ difference families.

q	Base Block	q	Base Block	q	Base Block	q	Base Block
25	$\{0,1,x,x^3\}$	37	{0,1,3,24}	49	$\{0,1,x,x^3\}$	61	{0,1,5,11}
73	{0,1,5,18}	97	{0,1,4,30}	109	{0,1,3,60}	121	$\{0,1,x,x^{10}\}$
157	{0,1,3,72}	181	{0,1,3,19}	193	{0,1,5,11}	229	{0,1,3,39}
241	{0,1,3,22}	277	{0,1,3,94}	289	$\{0,1,x,x^{17}\}$	313	{0,1,3,31}
337	{0,1,3,20}	349	{0,1,3,21}	361	$\{0,1,x,x^{16}\}$	373	{0,1,3,11}
397	{0,1,3,39}	409	{0,1,3,158}	421	{0,1,3,19}	433	{0,1,6,67}
457	{0,1,6,36}	529	$\{0,1,x,x^{35}\}$	541	{0,1,3,32}	577	{0,1,5,21}
601	{0,1,7,69}	613	{0,1,5,25}	625	$\{0,1,x,x^{356}\}$	661	{0,1,6,23}
709	{0,1,3,33}	733	{0,1,3,87}	757	{0,1,7,24}	829	{0,1,3,47}
841	$\{0,1,x^2,x^{58}\}$	853	{0,1,5,98}	877	{0,1,3,15}	937	{0,1,3,83}

16.62 Table $(q,5,1)$ difference families.

q	Base Block	q	Base Block	q	Base Block
61	{0,1,4,11,27}	101	{0,1,4,16,41}	121	$\{0,1,x^2,x^{15},x^{118}\}$
181	{0,1,3,10,137}	241	{0,1,6,19,173}	281	{0,1,3,14,150}
361	$\{0,1,x,x^3,x^{89}\}$	401	{0,1,3,12,109}	421	{0,1,3,9,341}
461	{0,1,4,16,413}	521	{0,1,3,9,217}	541	{0,1,3,7,210}
601	{0,1,3,17,430}	641	{0,1,7,18,245}	661	{0,1,5,19,89}
701	{0,1,3,8,392}	761	{0,1,3,7,149}	821	{0,1,4,11,68}
841	$\{0,1,x,x^4,x^{25}\}$	881	{0,1,3,9,34}	941	{0,1,3,17,65}
961	$\{0,1,x,x^3,x^{414}\}$	1021	{0,1,5,21,851}	1061	{0,1,3,7,411}

16.63 Table $(q,8,1)$ difference families.

q	Base Block	q	Base Block
449	{0,1,3,8,61,104,332,381}	617	{0,1,3,16,133,334,371,508}
673	{0,1,3,18,218,252,462,529}	729	$\{0,1,x,x^3,x^8,x^{362},x^{543},x^{685}\}$
841	$\{0,1,x,x^3,x^{378},x^{524},x^{824},x^{834}\}$	953	{0,1,3,18,247,370,789,794}
1009	{0,1,4,14,215,272,834,959}	1289	{0,1,3,7,68,297,466,551}
1681	$\{0,1,x,x^3,x^{21},x^{198},x^{471},x^{536}\}$	1849	$\{0,1,x,x^3,x^{24},x^{386},x^{459},x^{1353}\}$
2017	{0,1,3,9,43,695,1249,1483}	2129	{0,1,3,7,55,341,1336,1413}
2297	{0,1,3,9,58,1949,2068,2099}	2521	{0,1,3,9,75,1578,1817,2467}
2633	{0,1,3,7,48,1035,2009,2224}	2689	{0,1,3,7,32,1019,1632,2539}
2801	{0,1,3,11,54,1726,1749,1864}	2857	{0,1,6,15,85,878,1269,2329}
2969	{0,1,3,7,65,567,1379,2003}	3137	{0,1,3,7,15,269,1814,2254}

16.64 Table $(q,8,2)$ difference families.

q	Base Block	q	Base Block
113	{0,1,3,9,24,50,85,97}	169	$\{0,1,x,x^3,x^4,x^{21},x^{81},x^{117}\}$
197	{0,1,3,9,25,38,80,109}	281	{0,1,3,7,16,100,165,267}
337	{0,1,3,7,16,68,211,228}	421	{0,1,3,7,16,44,305,334}
701	{0,1,3,7,16,48,298,629}	757	{0,1,3,7,24,50,141,662}
1093	{0,1,3,7,16,173,495,974}	1373	{0,1,3,7,21,74,326,1310}
1429	{0,1,3,7,17,37,160,1300}	1597	{0,1,3,7,17,51,985,1356}
1709	{0,1,3,7,18,39,467,868}	1877	{0,1,3,7,17,45,848,1117}
1933	{0,1,3,7,16,36,1532,1636}	2213	{0,1,3,7,16,38,243,1853}
2269	{0,1,3,7,16,39,871,2141}	2381	{0,1,3,7,16,34,128,1040}

16.65 Table $(q, 7, 1)$ difference families and $(q, 9, 1)$ difference families for $q = 433, 1009$.

q	Base Block	q	Base Block
169	$\{0, 1, x, x^3, x^8, x^{51}, x^{58}\}$	337	{0,1,3,15,54,103,164}
379	{0,1,3,24,74,167,245}	547	{0,1,3,8,67,169,373}
673	{0,1,3,7,74,180,392}	757	{0,1,5,11,186,392,620}
841	$\{0, 1, x, x^{12}, x^{172}, x^{278}, x^{393}\}$	883	{0,1,3,7,242,423,505}
1471	{0,1,3,7,35,620,1126}	1597	{0,1,5,11,83,372,503}
1681	$\{0, 1, x, x^3, x^{17}, x^{1339}, x^{1441}\}$	5167	{0,1,3,7,18,2535,2976}
6091	{0,1,6,14,34,987,5380}	6553	{0,1,5,11,67,644,4144}
6889	$\{0, 1, x, x^3, x^4, x^{590}, x^{2830}\}$	8317	{0,1,3,7,26,67,6577}
8779	{0,1,5,18,43,1178,7108}	9661	{0,1,3,7,15,487,1093}
433	{0,1,3,30,52,61,84,280,394}	1009	{0,1,3,38,45,409,427,516,988}

16.66 Theorem [479, 481, 482] Let q be a prime power $\equiv 1 \pmod{k(k-1)}$. Then a $(q, k, 1)$ difference family over $\mathbb{F}_q$ exists in the following cases:

1. $k \in \{4, 5, 6\}$, except when $(q, k) = (61, 6)$.
2. $k = 7$, except when $q = 43$ and possibly when either (a) $q \in \{127, 211, 31^6\}$ or (b) $q \in [261239791, 1.236597 \times 10^{13}]$ and $(-3)^{(q-1)/14} = 1$ in $\mathbb{F}_q$.
3. $k \in \{8, 9\}$ and $q < 10000$, except possibly for $k = 8$, $q = 113, 169, 281, 337$, and $k = 9$, $q = 289, 361$.

16.67 Theorem Suppose q is an odd prime power, $q \equiv 1 \pmod{k(k-1)/\gcd(k(k-1), \lambda)}$ and $\lambda > 1$. Then if either (1) $k \leq 6$ [474] or (2) $k \in \{7, 8, 9\}$ and $q \leq 10000$, a (q, k, λ) difference family over $\mathbb{F}_q$ exists, except for $(q, k, \lambda) = (29, 8, 2)$, $(25, 9, 3)$ and possibly for $(q, k, \lambda) = (49, 9, 3)$. In addition, a cyclic $(49, 9, 3)$ difference family exists [1628].

16.5 Relative Difference Families

16.68 Theorem A summary of the known results for relative difference families with small block size.

1. [386, 476] If t is relatively prime to 30, then a cyclic $(6t, 6, 4, 1)$ relative difference family exists.
2. [842, 2001] Cyclic $(9t, 9, 4, 1)$ and $(15t, 15, 4, 1)$ relative difference families exist if all prime factors of t are congruent to 1 (mod 4) and $\neq 5$ (in both cases).
3. [454] Let u be a product of primes $\equiv 1 \pmod 6$. Then a cyclic $(4^n u, 4, 4, 1)$ relative difference family exists if either (1) $n \geq 3$ or (2) $n = 2$ and $\gcd(u, 7 \cdot 13 \cdot 19) \neq 1$.
4. [386] If every prime factor of t is congruent to 1 (mod 6) then a cyclic $(8t, 8, 4, 1)$ relative difference family exists.
5. [1376] If every prime factor of v is congruent to 1 (mod 12), then a resolvable cyclic $(4v, 4, 4, 1)$ relative difference family exists.
6. [386] If every prime factor of v is of the form $6pn + 1$ with $p \leq 19$ a prime and $n \geq 1$, then a $(4v, 4, 4, 1)$ relative difference family over $\mathbb{Z}_{4v}$ exists.
7. [457] If $p \equiv 1 \pmod{10}$ is prime and $p \neq 11$, then a cyclic $(4p, 4, 5, 1)$ relative difference family exists.
8. [457] If $p \equiv 11 \pmod{20}$ is prime and $u \in \{2, 3\}$, then a cyclic $(4up, 4, 5, 1)$ relative difference family exists.
9. [225] If v is odd and $v \not\equiv 3, 15 \pmod{18}$, then a $(5v, 5, 5, 2)$ relative difference family exists.

16.69 Remark For several known (v,k,k,λ) relative difference families, $v=kq$ where k,q are odd prime powers, $k-1\equiv 0 \pmod{2\lambda}$, and $\lambda(q-1)\equiv 0 \pmod{k-1}$. These relative difference families are over $\mathbb{F}_k \times \mathbb{F}_q$. In each case there are λ identical base blocks containing the values $(i,0)$ $(i\in\mathbb{F}_k)$. There is an initial base block of the form $B = \{(0,0), (c_1,\pm z_1), (c_2,\pm z_2),\ldots (c_{(k-1)/2},\pm z_{(k-1)/2})\}$ where the c_i's are the quadratic residues in $\mathbb{F}_k$ and the values z_i depend on q. Other base blocks are obtained by multiplying B by $(1,x^{mn})$ for $m=\frac{k-1}{2\lambda}$ and $n=1,2,\ldots,\frac{\lambda(q-1)}{k-1}-1$.

16.70 Examples Relative difference families arising from the method in Remark 16.69.

1. $k=5, q=17$: $(v,k,\lambda)=(85,5,1)$: B={(0,0),(1,1),(1,16),(4,7),(4,10)}.
2. $k=5, q=29$: $(v,k,\lambda)=(145,5,1)$: B={(0,0),(1,1),(1,28),(4,12),(4,17)}.
3. $k=7, q=13$: $(v,k,\lambda)=(91,7,1)$: B={(0,0),(1,1),(1,12),(2,4),(2,9),(4,3),(4,10)}.
4. $k=7, q=11$: $(v,k,\lambda)=(77,7,3)$: B={(0,0),(1,1),(1,10),(2,2),(2,9),(4,4),(4,7)}.
5. $k=9, q=13$: $(v,k,\lambda)=(117,9,2)$: B={(0,0), (1,1), (1,12), (2,5), (2,8), (x+1,2), ($x+1$,11), ($2x+2$,3), ($2x+2$,10)}.
6. $k=9, q=89$: $(v,k,\lambda)=(801,9,1)$: B={(0,0), (1,1), (1,88), (2,34), (2,55), (x+1,15), (x+1,74), (2x+2,24), (2x+2,65)} (here x is a primitive element of $\mathbb{F}_9$ satisfying $x^2=x+1$).

16.71 Theorem [4, 958] Suppose $q\equiv 1 \pmod{k-1}$ is a prime power. Then a $(kq,k,k,1)$ relative difference family over $\mathbb{F}_k\times\mathbb{F}_q$ exists if one of the following holds:

1. $k\in\{3,5\}$ (for $k=5$, the initial block B can be taken as $\{(0,0),(1,1),(1,-1),(4,x),(4,-x)\}$ where x is any nonsquare in $\mathbb{F}_q$ such that exactly one of $x-1, x+1$ is a square).
2. $k=7$, $q<5000$ and $q\neq 19$.
3. $k=9$, $q<5834$ and $q\notin\{17,25,41,97,113\}$.
4. $k=11, q<1202$, q is prime, and $q\notin$ [30,192], [240,312] or [490,492].

Using Weil's theorem, it can be shown that the conditions $q<5000$ and $q<5834$ parts 2 and 3 above can be removed.

16.72 Theorem [381]

1. Let $q=12t+1$ be a prime power, and let 3^e be the largest power of 3 dividing t. If, in $\mathbb{F}_q$, 3 and $2+\sqrt{3}$ are both 3^eth powers but not 3^{e+1}th powers and 6 is not a 3^{e+1}th power, then a $(13q,13,13,1)$ relative difference family exists.
2. If p and q are odd prime powers with $q>p$, then a $(pq,p,p,(p-1)/2)$ relative difference family exists. If further $p\equiv 1 \pmod 4$ and $q\equiv 1 \pmod{p-1}$, then a $(pq,p,p,(p-1)/4)$ relative difference family exists.

16.6 1-Rotational Designs

16.73 Remark Let G be a group and let ∞ be a symbol not belonging to G. If B is a subset of G, then the list of partial differences from $B\cup\{\infty\}$ is the multiset defined by $\partial(B\cup\{\infty\}) = \partial B \cup \{\underbrace{\infty,\infty,\ldots,\infty}_{|B|/|G_B| \text{ times}}\}$, as in §16.1. The G-orbit of $B\cup\{\infty\}$ is the set of subsets of $G\cup\{\infty\}$ defined by $Orb_G(B\cup\{\infty\}) = \{(B+s)\cup\{\infty\} \mid s\in S\}$ where S is a complete system of representatives for the right cosets of G_B in G.

16.74 Let G be a group of order $v-1$. A collection $\{B_1,\ldots,B_t\}$ of k-subsets of $G\cup\{\infty\}$ is a 1-*rotational* (v,k,λ) *difference family* if every nonidentity element of $G\cup\{\infty\}$ occurs λ times in $\partial B_1\cup\ldots\cup\partial B_t$.

16.75 Remarks

1. If $\{B_1, \ldots, B_t\}$ is a 1-rotational (v, k, λ) difference family over the group G, then $Orb_G(B_1) \cup \ldots \cup Orb_G(B_t)$ is the collection of blocks of a BIBD(v, k, λ) admitting G as an automorphism group fixing one point and acting sharply transitively on the others.
2. If $\{B_1, \ldots, B_t\}$ is a $(v, k-1, k, \lambda)$ difference family over G and relative to H, then $\{B_1, \ldots, B_t\} \cup \{\underbrace{H \cup \{\infty\}}_{\lambda \text{ times}}\}$ is a 1-rotational (v, k, λ) difference family.
3. In a 1-rotational $(v, k, 1)$ difference family over an abelian group G the block through ∞ is short and it is of the form $H \cup \{\infty\}$ with H a coset of a suitable subgroup of G of order $k-1$. Every other short block is a coset of a suitable subgroup of G of order k.

16.76 Examples

1. The five triples $B_1 = \{(0,0), (0,3), \infty\}$, $B_2 = \{(0,0), (1,0), (2,0)\}$, $B_3 = \{(0,0), (1,2), (2,4)\}$, $B_4 = \{(0,0), (0,1), (1,5)\}$, and $B_5 = \{(0,0), (0,2), (1,3)\}$ form a 1-rotational $(19, 3, 1)$ difference family over $(\mathbb{Z}_3 \times \mathbb{Z}_6) \cup \{\infty\}$.
2. Let G be the nonabelian group of order 24 with defining relations $G =< x, y \mid x^{12} = y^2 = 1; xy = yx^7 >$. Then $B_1 = \{1, x^4, x^8, \infty\}$, $B_2 = \{1, x^6, y, yx^6\}$, $B_3 = \{1, x, yx^3, yx^{10}\}$, $B_4 = \{1, x^2, x^5, yx\}$ form a 1-rotational $(25, 4, 1)$ difference family over $G \cup \{\infty\}$.
3. Let G be the nonabelian group of order 42 with defining relations $G =< x, y \mid x^3 = y^{14} = 1; yx = xy^9 >$. Then the triples
$$\begin{array}{lll} B_1 = \{1, y^7, \infty\}, & B_2 = \{1, x, x^2\}, & B_3 = \{1, xy^2, x^2y^6\}, \\ B_4 = \{1, y, xy^4\}, & B_5 = \{1, y^2, xy^9\}, & B_6 = \{1, y^3, xy^{13}\}, \\ B_7 = \{1, y^4, xy^{12}\}, & B_8 = \{1, y^5, xy^6\}, & B_9 = \{1, y^6, xy^{11}\} \end{array}$$
form a 1-rotational $(43, 3, 1)$ difference family over G.
4. Let $G = \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ and let α be the automorphism of G defined by $\alpha(x, y) = (y - x, 3x + 4y)$. Then $\alpha^2(x, y) = (3y, 9x + 7y)$, and $\alpha^3(x, y) = (x, y)$. Set $A = \{(0,0), (0,4), (0,8), \infty\}$, $B = \{(0,0), (1,0), (2,0), (3,0)\}$, $C = \{(0,0), (1,3), (2,4), (2,5)\}$. $\{A, B, \alpha(B), \alpha^2(B), C, \alpha(C), \alpha^2(C)\}$ is a 1-rotational $(49, 4, 1)$ difference family over $G \cup \{\infty\}$ in which α is a multiplier of order 3.

16.77 Theorem [384, 1740]

1. If $v \equiv 3 \pmod 6$, then a 1-rotational $(v, 3, 1)$ difference family over some group exists if and only if $v \equiv 3, 9 \pmod{24}$.
2. If $v \equiv 1 \pmod 6$, then a necessary condition for the existence of a 1-rotational $(v, 3, 1)$ STS over some group is that either $v = 24n+1$ for some n or $v = 24m+19$ with $4m+3$ having a prime factor $p \not\equiv 2 \pmod 3$. This condition is also sufficient, except possibly when $v = 24n + 1$ and all prime factors of n are congruent to 2 modulo 3.

16.78 Theorem A 1-rotational Kirkman triple system, KTS(v) is known for every v of the following forms:

1. [965] $v = 3^n$;
2. [394] $v = 2p_1p_2 \ldots p_n + 1$ with $p_i \equiv 1 \pmod{12}$ prime for $1 \le i \le n$;
3. [394] $v = 8p_1p_2 \ldots p_n + 1$ with $p_i \equiv 1 \pmod 6$ prime for $1 \le i \le n$.

16.79 Theorem A 1-rotational BIBD$((k-1)t + 1, k, 1)$ with a resolution that is invariant under the action of $\mathbb{Z}_{(k-1)t}$ exists in the following cases:

1. [391] $k = 4$, and all prime factors of $t \equiv 1 \pmod 4$.
2. [389] $k = 6$, t is a prime $\equiv 1 \pmod{12}$, and $t \neq 13, 37$.

3. [389] $k = 8$, t is a prime $\equiv 1 \pmod 8$, and $t \neq 17, 89$.

16.80 Theorem [381] Let p, q, and r be odd prime powers and s be any prime power. Then the following BIBDs designs exist:

1. A 1-rotational BIBD$(pq+1, p+1, (p+1)/2)$ for $p \equiv 3 \pmod 4$ and $q > p$.
2. A 1-rotational RBIBD$(pq+1, p+1, (p+1)/2)$ for $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod{p+1}$.
3. A 1-rotational BIBD$(pq+1, p+1, p+1)$ for $q > p$.
4. A 1-rotational RBIBD$(pq+1, p+1, p+1)$ for $q \equiv 1 \pmod{p+1}$.
5. A 1-rotational BIBD$(pqr+1, pq+1, (pq+1)/2)$ for $q = p+2$ and $r > pq$.
6. A 1-rotational RBIBD$(pqr+1, pq+1, (pq+1)/2)$ for $q = p+2$ and $r \equiv 1 \pmod{pq+1}$.
7. A 1-rotational BIBD$((2^d-1)s+1, 2^d, 2^d-1)$ for $s > 2^d$.
8. A 1-rotational RBIBD$((2^d-1)q+1, 2^d, 2^d-1)$ for $q \equiv 1 \pmod{2^d}$.
9. A 1-rotational RBIBD$((k-1)q+1, k, k+1)$ for any integer k and $q \equiv 1 \pmod k$.
10. A 1-rotational BIBD$(2^e s+1, 2^e+1, 2^{e-1}+1)$ for $s \equiv 1 \pmod{2^e+1}$.

16.81 Examples 1-rotational $(v, 3, 2)$ designs. Short blocks are shown *slanted.* The designs for $v = 12$, 18, 24, 30, 36, and 42 are resolvable.

v	Base Blocks						
6	∞ 0 1	0 2 4					
10	∞ 0 1	0 1 4	0 2 4	*0 3 6*			
12	∞ 3 6	0 1 5	2 4 8	7 9 10			
18	∞ 13 16	0 1 5	3 4 11	8 10 14	6 12 15	2 7 9	
22	∞ 0 3	0 1 7	0 1 9	0 2 5	0 2 10	0 4 9	0 4 10
	0 7 14						
24	∞ 16 20	0 7 21	1 3 11	4 5 18	6 12 17	2 10 13	8 9 14
	15 19 22						
30	∞ 2 22	0 1 19	6 8 27	9 15 16	7 10 14	11 25 28	12 18 23
	13 21 26	4 20 24	3 5 17				
34	∞ 0 1	0 1 14	0 2 7	0 2 8	0 3 13	0 3 15	0 4 12
	0 4 14	0 5 16	0 6 15	0 7 16	*0 11 22*		
36	∞ 14 29	0 1 13	2 17 25	3 6 12	4 9 28	5 21 23	7 18 32
	8 16 22	10 19 20	11 15 33	24 26 31	27 30 34		
42	∞ 7 22	0 1 20	9 15 40	18 23 36	26 30 38	8 11 35	19 21 28
	13 16 34	6 17 33	10 32 39	5 31 37	3 14 27	2 4 12	24 25 29

16.82 Examples 1-rotational $(v, 3, 6)$ designs.

v	Base Blocks							
8	∞ 0 1	∞ 0 2	∞ 0 3	0 1 2	0 2 4	0 1 3	0 2 3	0 3 6
14	∞ 0 4	∞ 0 5	∞ 0 6	0 1 2	0 2 4	0 1 3	0 3 6	0 4 8
	0 5 10	0 6 12	0 1 4	0 3 4	0 2 7	0 5 7		

16.83 Examples Resolvable 1-rotational $(v, 4, 3)$ designs. Larger examples with $v \leq 132$ can be found in [38, 873].

v	Base Blocks				
8	∞ 3 5 6	0 1 2 4			
12	∞ 3 7 9	0 1 4 10	2 5 6 8		
20	∞ 8 12 18	0 2 3 14	1 4 13 16	7 9 15 17	5 6 10 11
24	∞ 0 7 10	1 8 12 22	2 5 6 11	3 9 14 18	4 16 17 19
	13 15 20 21				
32	∞ 17 22 23	0 4 7 20	2 14 25 28	1 8 10 16	5 9 18 19
	6 11 13 21	3 12 24 30	15 26 27 29		
36	∞ 24 29 33	0 19 20 32	7 12 13 31	1 9 18 22	3 4 28 30
	6 10 27 34	11 14 16 26	5 8 15 21	2 17 23 25	

16.84 Example A 1-rotational (18,4,6) design.

∞ 0 1 4	∞ 0 4 5	1 4 13 16	1 4 13 16	3 5 12 14
3 5 12 14	2 8 9 15	2 8 9 15	6 7 10 11	

16.85 Examples 1-rotational $(v, 5, 4)$ designs. When $v = 20, 30, 40$, the designs given are resolvable.

v	Base Blocks			
10	∞ 0 1 4 6	0 1 2 4 8		
15	∞ 0 1 3 8	0 1 2 5 6	0 2 4 7 10	
20	∞ 0 2 3 14	1 5 6 10 12	4 7 8 13 16	9 11 15 17 18
30	∞ 4 8 17 18	0 1 7 24 27	2 12 15 16 23	9 11 13 21 26
	3 14 20 22 25	5 6 10 19 28		
36	∞ 8 13 22 27	0 1 10 12 13	0 2 6 8 25	0 16 20 27 33
	0 15 22 23 26	14 15 21 25 30	12 15 25 30 33	*0 7 14 21 28*
40	∞ 0 3 9 27	2 5 13 26 32	1 4 20 29 36	8 16 25 30 35
	10 11 12 14 22	7 15 17 31 33	6 21 28 34 38	18 19 23 24 37

16.86 Examples 1-rotational $(v, 6, \lambda)$ designs. The (24,6,5), (30,6,5), (36,6,2), (36,6,3) and (42,6,5) designs given are resolvable.

v, λ	Base Blocks			
14,15	∞ 0 1 5 7 10	∞ 0 2 3 4 8	∞ 0 6 9 11 12	1 3 4 9 10 12
	0 1 2 6 11 12	0 3 5 6 7 10	0 2 4 5 8 9	
15,5	∞ 0 3 5 7 13	1 6 9 10 11 12	1 2 4 8 9 11	
18,5	∞ 0 2 8 9 12	0 1 2 4 7 15	0 1 3 7 8 12	
24,5	∞ 0 1 7 15 20	2 3 4 5 10 14	6 11 13 17 19 22	8 9 12 16 18 21
27,5	∞ 0 7 11 13 21	0 3 6 14 17 24	0 9 16 18 20 25	0 1 2 8 22 23
	2 5 6 15 18 19			
30,5	∞ 5 16 19 21 22	0 1 6 7 11 14	2 9 13 15 17 26	3 10 12 20 23 24
	4 8 18 25 27 28			
34,5	∞ 0 3 10 12 32	0 3 16 18 24 32	0 9 15 23 28 30	0 3 4 12 31 32
	0 7 13 21 23 30	*0 4 11 15 22 26*	*0 5 11 16 22 27*	
36,2	∞ *0 7 14 21 28*	∞ *0 7 14 21 28*	4 15 16 20 24 26	2 3 12 15 18 20
36,3	2 4 8 12 17 20	1 2 3 6 12 18	3 12 14 15 25 30	∞ *0 7 14 21 28*
	∞ *0 7 14 21 28*	∞ *0 7 14 21 28*		
40,5	∞ 0 3 19 27 32	0 6 7 15 18 35	0 17 19 21 24 33	0 1 7 8 29 30
	0 5 9 19 23 25	10 12 15 16 24 27	*0 5 13 18 26 31*	*0 2 13 15 26 28*
42,5	∞ 15 22 24 27 35	0 3 7 13 29 30	8 17 18 25 34 36	9 10 14 20 23 28
	1 2 5 11 26 31	19 21 33 37 38 40	4 6 12 16 32 39	

16.87 Examples Resolvable 1-rotational (v, k, λ) designs.

v, k, λ	Base Blocks
15,5,8	{∞,5,6,7,10}, {0,2,4,8,11}, {1,3,9,12,13}, {∞,3,9,10,12}, {0,1,5,6,13}, {2,4,7,8,11}
28,7,6	{∞,0,5,14,15,24,25}, {1,10,17,20,22,23,26}, {2,6,8,9,13,19,21}, {3,4,7,11,12,16,18}
32,8,7	{∞,0,1,5,16,18,25,28}, {3,9,17,19,20,21,24,26}, {2,6,7,12,14,15,23,27}, {4,8,10,11,13,22,29,30}
35,7,6	{∞,7,9,23,27,28,29}, {0,2,4,8,11,14,17}, {3,6,13,16,24,25,32}, {1,5,10,15,18,22,33}, {12,19,20,21,26,30,31}
36,9,8	{∞,1,10,11,13,15,25,26,29}, {0,9,16,17,18,19,22,24,30}, {3,4,6,12,21,23,27,31,34}, {2,5,7,8,14,20,28,32,33}
40,8,7	{∞,13,17,19,23,28,31,38}, {0,1,14,16,22,26,29,35}, {3,5,8,15,24,25,36,37}, {2,6,7,9,10,11,30,33}, {4,12,18,20,21,27,32,34}

40,10,9	{∞,3,4,6,10,24,32,33,34,37}, {0,9,11,14,15,18,25,26,30,31}, {1,5,7,8,12,17,19,21,27,29}, {2,13,16,20,22,23,28,35,36,38}
42,7,6	{∞,0,3,7,13,29,30}, {8,15,17,18,25,34,36}, {9,10,14,20,22,23,28}, {1,2,5,11,26,31,35}, {19,21,24,33,37,38,40}, {4,6,12,16,27,32,39}
48,8,7	{∞,1,13,15,21,22,24,40}, {0,8,17,29,30,36,39,41}, {9,14,16,19,20,26,34,43}, {5,10,12,23,27,31,37,46}, {2,18,28,32,33,42,44,45}, {3,4,6,7,11,25,35,38}
56,8,7	{∞,3,5,14,18,25,34,39}, {0,8,13,19,20,32,50,53}, {7,10,15,23,29,30,38,48}, {4,6,33,35,36,47,51,52}, {12,16,40,42,43,46,49,54}, {1,2,22,24,28,31,41,45}, {9,11,17,21,26,27,37,44}
63,7,3	{6,14,32,44,49,51,52}, {7,8,12,30,34,36,59}, {26,35,40,46,47,56,60}, {0,2,10,17,23,50,53}, {∞,*11,24,27,42,55,58*}
63,9,4	{4,9,20,32,36,38,39,45,56}, {24,34,37,42,44,46,57,58,61}, {12,16,18,19,28,33,41,52,60}, {∞,*0,17,22,23,31,48,53,54*}

16.88 Examples 1-rotational (v, k, λ) designs.

v,k,λ	Base Blocks
20,8,14	{∞,0,4,5,6,9,16,17}, {∞,0,1,4,6,7,9,11}, {0,1,5,6,7,9,15,17}, {0,4,5,6,7,10,11,16}, {0,1,4,9,11,13,16,17}
24,8,7	{∞,0,1,4,5,7,9,17}, {0,1,9,10,15,17,20,21}, {0,3,8,9,10,12,16,21}
30,10,9	{∞,0,1,5,7,16,19,20,23,28}, {0,2,3,6,8,10,11,18,22,23}, {0,2,3,13,14,19,22,24,26,28}
34,11,10	{∞,1,6,7,11,14,22,23,25,27,29}, {0,1,3,4,6,10,18,23,24,26,32}, {0,1,2,6,9,10,13,15,23,27,32}, {*0,3,6,9,12,15,18,21,24,27,30*}
34,12,12	{∞,0,1,3,5,9,16,17,23,25,27,28,30}, {1,3,6,9,10,11,20,22,24,27,30}, {0,2,4,7,12,13,17,23,27,28,29,30}, {∞,*0,3,6,9,12,15,18,21,24,27,30*}
36,12,11	{∞,0,1,4,6,7,11,19,26,28,29,34}, {1,3,6,7,15,17,18,20,28,29,32,34}, {1,4,5,7,9,10,11,16,20,25,28,29}
39,13,12	{∞,1,7,8,9,11,12,18,20,23,25,26,30}, {0,3,4,6,13,15,21,27,28,29,31,33,37}, {1,2,7,10,11,13,14,15,19,22,29,32,34}
40,12,11	{∞,0,2,3,5,9,13,21,24,27,32,33}, {1,2,5,6,7,8,9,15,19,24,29,31}, {2,3,4,6,14,16,22,27,31,35,36,38}, {*0,1,3,9,13,14,16,22,26,27,29,35*}
44,11,10	{∞,0,2,3,4,12,15,18,22,24,29}, {0,11,12,15,18,20,22,25,27,35,42}, {0,3,4,21,22,23,29,33,34,37,38}, {0,2,3,7,9,13,18,24,26,32,40}
70,7,2	{∞,*0,2,23,25,46,48*}, {0,1,8,12,14,17,41}, {0,5,14,27,49,53,59}, {0,17,20,32,50,51,58}

16.89 Examples [1] 1-rotational $(q^2+1, q+1, (q+1)/2)$ designs over $\mathbb{F}_q \times \mathbb{F}_q \cup \{\infty\}$. For $q = 9$, x is a primitive element of $\mathbb{F}_9$ satisfying $x^2 = x + 1$.

v,k,λ	Base Blocks
26,6,3	$\{(0,0),(0,y),(0,2y),(y,y),(2y,4y),(4y,0)\}$ for $y = 1, 2$; Short blocks: $\{\infty,(0,0),(1,y),(2,2y),(3,3y),(4,4y)\}$ for $y = 0, 2, 4$.
50,8,4	$\{(0,0),(0,y),(0,2y),(y,0),(2y,2y),(4y,y),(4y,5y),(6y,6y)\}$ for $y = 1, 2, 3$; Short blocks: $\{\infty,(0,0),(1,y),(2,2y),(3,3y),(4,4y),(5,5y),(6,6y)\}$ for $y = 0, 2, 3, 6$.
82,10,5	$\{(0,0),(0,y),(xy,xy),(xy,x^3y),(xy,x^5y),(x^2y,x^6y),(x^3y,x^6y),(x^5y,x^6y),(x^6y,x^3y),(x^6y,x^4y)\}$ for $y = 1, x, x^2, x^3$; Short blocks: $\{\infty,(0,0),(1,y),(x,xy),(x^2,x^2y),(x^3,x^3y),(x^4,x^4y),(x^5,x^5y),(x^6,x^6y),(x^7,x^7y)\}$ for $y = 0, x, x^2, x^3, x^5$.
122,12,6	$\{(0,0),(0,4y),(0,7y),(y,0),(y,y),(2y,2y),(5y,y),(5y,3y),(6y,y),(6y,5y),(8y,10y),(10y,3y)\}$ for $y = 1, 2, 3, 4, 5$; Short blocks: $\{\infty,(0,0),(1,y),(2,2y),(3,3y),(4,4y),(5,5y),(6,6y),(7,7y),(8,8y),(9,9y),(10,10y)\}$ for $y = 0, 3, 5, 6, 7, 8$.
170,14,7	$\{(0,0),(0,y),(y,y),(y,5y),(2y,4y),(4y,5y),(5y,8y),(5y,12y),(6y,2y),(7y,4y),(7y,12y),(8y,5y),(8y,8y),(8y,9y)\}$ for $y = 1, 2, 3, 4, 5, 6$; Short blocks: $\{\infty,(0,0),(1,y),(2,2y),(3,3y),(4,4y),(5,5y),(6,6y),(7,7y),(8,8y),(9,9y),(10,10y),(11,11y),(12,12y)\}$ for $y = 2, 6, 7, 8, 9, 10, 11$.

16.90 Example A 1-rotational (46,6,3) difference family over $(\mathbb{Z}_5 \times \mathbb{Z}_3^2) \cup \{\infty\}$. The base blocks are

{(0,0,1),(0,0,2),(1,1,1),(1,2,2),(4,1,2),(4,2,1)}, {(0,1,0),(0,2,0),(1,1,2),(1,2,1),(4,0,1),(4,0,2)},
{(0,0,1),(0,0,2),(2,1,0),(2,2,0),(3,1,1),(3,2,2)}, {(0,1,0),(0,2,0),(2,1,2),(2,2,1),(3,1,1),(3,2,2)}

and the short block (included three times) is $\{\infty$,(0,0,0),(1,0,0),(2,0,0),(3,0,0),(4,0,0)$\}$.

16.91 Example A (51,6,2) design over $(\mathbb{Z}_5 \times \mathbb{Z}_{10}) \cup \{\infty\}$ that is 2-resolvable and has short base blocks $\{\infty, (0,5), (1,5), (2,5), (3,5), (4,5)\}$, $\{\infty, (0,8), (1,8), (2,8), (3,8), (4,8)\}$. Other base blocks are $\{(0,1), (0,3), (0,7), (1,2), (1,9), (3,4)\}$, $\{(0,2), (0,7), (2,3), (2,6), (3,0), (4,4)\}$, and $\{(0,0), (0,1), (0,9), (1,6), (2,5), (4,8)\}$.

16.92 Example A resolvable (126,6,1) design over $\mathbb{Z}_5^3 \cup \{\infty\}$. Element $(x,y,z) \in \mathbb{Z}_5^3$ is written as xyz. A short base block is $\{\infty, 000, 100, 200, 300, 400\}$. The other base blocks are {001,004,122,133,421,434}, {002,003,144,111,442,413}, {043,012,220,230,332,323}, {031,024,240,210,314,341}.

16.7 Enumeration

16.93 Two difference families $D = \{B_1, B_2, \ldots, B_m\}$ and $D' = \{B_1', B_2', \ldots, B_m'\}$ over a group G are *equivalent* if there is an automorphism α of G such that B_i' is a translate of $\alpha(B_i)$ for all i.

16.94 Remarks Equivalent difference families lead to isomorphic BIBDs, although the converse is not true in general (see Remark II.2.28). For enumeration of inequivalent difference families with block size 3, see Tables II.2.29 and II.2.30.

16.95 Table [592] The number N of inequivalent $(v,4,1)$ difference families over $\mathbb{Z}_v$.

v	13	16	25	28	37	40	49	52	61	64
N	1	0	0	0	2	10	224	206	18132	12048

16.96 Table [592] The number N of inequivalent $(v,5,1)$ difference families over $\mathbb{Z}_v$.

v	21	25	41	45	61	65
N	1	0	1	0	10	2

See Also

§II.1	Difference families generate BIBDs.
§VI.19	Difference triangle sets are generalizations of perfect difference families.
§VI.18	Difference sets are difference families with one base block.
§VI.17	Difference matrices are used in recursive constructions of difference families.
§VI.53	Skolem sequences are used to construct difference families with block size three.
[96]	A survey on cyclic and 1-rotational designs
[225]	A text covering several results in this chapter.
[379, 1200]	Papers covering recursive constructions for difference families.

References Cited: [1, 4, 23, 30, 38, 96, 225, 376, 377, 378, 379, 381, 384, 386, 389, 391, 394, 454, 457, 474, 476, 479, 481, 482, 590, 592, 719, 842, 873, 888, 957, 958, 965, 1143, 1200, 1220, 1376, 1537, 1628, 1740, 2001, 2144]

17 Difference Matrices

Charles J. Colbourn

17.1 Definition and Examples

17.1 Let $(G, \odot)$ be a group of order g. A $(g, k; \lambda)$-*difference matrix* is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G, so that for each $1 \le i < j \le k$, the multiset

$$\{d_{i\ell} \odot d_{j\ell}^{-1} : 1 \le \ell \le g\lambda\}$$

(the *difference list*) contains every element of G λ times. When G is abelian, typically additive notation is used, so that differences $d_{i\ell} - d_{j\ell}$ are employed.

17.2 Examples

1. A $(3, 6; 2)$-difference matrix and a $(15, 5; 1)$-difference matrix [1847]. For the latter, append a column of zeroes to $(B|-B)$ to get the required 5×15 matrix.

$$A = \begin{pmatrix} 0&0&0&0&0&0 \\ 1&2&0&2&0&1 \\ 1&0&2&2&1&0 \\ 0&2&2&0&1&1 \\ 2&2&0&1&1&0 \\ 2&0&2&1&0&1 \end{pmatrix} \qquad B = \begin{pmatrix} 0&0&0&0&0&0&0 \\ 1&2&3&4&5&6&7 \\ 2&5&7&9&12&4&1 \\ 6&3&14&10&7&13&4 \\ 10&6&1&11&2&7&12 \end{pmatrix}.$$

2. Theorem III.3.44 gives (implicitly) a $(12, 6; 1)$-difference matrix. Numerous other difference matrices are given in §III.3.

17.3 Remark The $(15, 5; 1)$- and $(12, 6; 1)$-difference matrices of Examples 17.2 can be used to construct four MOLS(15) and five MOLS(12), respectively.

17.4 Remark Removing any row from a $(g, k; \lambda)$-difference matrix gives a $(g, k-1; \lambda)$-difference matrix.

17.5 Theorems

1. [1221] A $(g, k; \lambda)$-difference matrix does not exist if $k > \lambda g$.
2. [748] A $(g, 3; \lambda)$-difference matrix over G does not exist if λ is odd and g is even and the Sylow 2-subgroup of G is cyclic; in particular, if λ is odd, this excludes $g \equiv 2 \pmod 4$ and also excludes $G = \mathbb{Z}_g$ for even g.

17.6 Theorem [748] The multiplication table for the finite field $\mathbb{F}_q$ is a $(q, q; 1)$-difference matrix over $\mathrm{EA}(q)$.

17.2 Related Objects

17.7 Remark An $(s, k; \lambda)$-difference matrix D over a group $(G, \odot)$ with $G = \{g_1, \ldots, g_s\}$ can be developed over G to obtain a completely resolvable $\mathrm{OA}_\lambda(k, s)$, $(g_1 D \; g_2 D \; \ldots \; g_s D)$.

17.8 Theorem A $(g, k; \lambda)$-difference matrix over G gives rise to a resolvable $\mathrm{OA}_\lambda(k, g)$ and, hence, to an $\mathrm{OA}_\lambda(k+1, g)$ and a $\mathrm{TD}_\lambda(k+1, g)$.

17.9 Theorem An $(s, 3; 1)$-difference matrix is equivalent to a complete mapping.

17.10 Theorem An $\mathrm{OA}_\lambda(k, g)$ can be viewed as a $(g, k; \lambda g)$-difference matrix over an arbitrary group of order g.

17.11 Remarks A $(g, k; \lambda)$-difference matrix over a group G of order g is a generalized Bhaskar Rao design $\mathrm{GBRD}(k, k, \lambda g; G)$. See §V.4. A *generalized Hadamard matrix* $\mathrm{GH}(g, \lambda)$ is a $(g, g\lambda; \lambda)$-difference matrix. See §V.5. Here shorter difference matrices, those with $k < g\lambda$, are treated.

17.3 Shorter Difference Matrices

17.12 Example A $(15, 7; 2)$-difference matrix over $\mathbb{Z}_{15}$. Take $(A \mid 2A \mid -A \mid -2A)$, where A is the circulant matrix with first row (2 4 10 3 13 0 9). Append two columns of zeroes.

17.13 Theorem If there is a $(g, k; \lambda_1)$-difference matrix and a $(g, k; \lambda_2)$-difference matrix over the same group G, then there is a $(g, k; \lambda_1 + \lambda_2)$-difference matrix over G.

17.14 Theorem [379]Let H be a normal subgroup of G. If there is an $(h, k; \lambda)$-difference matrix over H and a $(g/h, k; \lambda')$-difference matrix over G/H, then there is a $(g, k; \lambda\lambda')$-difference matrix over G.

17.15 Corollary Since $\{1\} \times H$ is normal in $G \times H$, if there is an $(h, k; \lambda)$-difference matrix over H and a $(g, k; \lambda')$-difference matrix over G, then there is a $(gh, k; \lambda\lambda')$-difference matrix over $G \times H$.

17.16 Theorem If a $(g, k; \lambda)$-difference matrix over a group G exists, and G' is a normal subgroup of G of index x, then an $(x, k; \lambda g/x)$-difference matrix over G/G' exists.

17.17 Theorem (*tensor or Kronecker product* [1904]) If a $(g, k; \lambda)$-difference matrix and a $(g, k'; \lambda')$-difference matrix exist over the same group G, then a $(g, kk'; g\lambda\lambda')$-difference matrix exists over G.

17.18 Theorems

1. [867] A $(g, 4; 1)$-difference matrix exists if and only if $g \geq 4$ and $g \not\equiv 2 \pmod 4$.
2. [799] A $(g, 5; 1)$-difference matrix exists over $\mathbb{Z}_v$ exists if and only if v is odd and $v \notin \{3, 9\}$, except possibly when $v = 9p$ and p is an odd prime other than 5, 7, 11, 13, 17 23, 29, 31, or 109.
3. [379] Let G be any group of order g. Then there exists a $(g, p; 1)$-difference matrix over G where p is the smallest prime dividing g.
4. [379] Let p be a prime and let G be an abelian group of order p^e and type $(n_1, n_2, ..., n_t)$. Then there exists a $(p^e, p^f; 1)$ difference matrix over G where $f = \lfloor (n_1 + n_2 + ... + n_t)/\max(n_1, n_2, ..., n_t) \rfloor$.

17.19 Theorem [1221] Let $s = q_1 q_2 \dots q_n$ be the prime power factorization of s, and let $q = \min(q_1, q_2, \dots, q_n)$. Then if there exists a transversal design $\mathrm{TD}(r, s)$, there exists a $(s, r(q-1)+1; s)$-difference matrix over $\mathrm{EA}(q_1) \times \cdots \times \mathrm{EA}(q_n)$.

17.20 Theorem [1221] Suppose there is a (v, k, λ)-difference family over G. Then if there exists an idempotent $\mathrm{TD}(r, k)$, there exists a $(v, r; \lambda)$-difference matrix over G. Similarly, if there exists a $\mathrm{TD}_\mu(r, k)$ having a parallel class and $k(\mu - 1) \leq \lambda\mu$, then there exists a $(v, r; \lambda\mu)$-difference matrix over G.

17.21 A (G, s, t)-*complementary pair* is a pair of $s \times t$ $(0, G)$-matrices A and B such that $a_{ij} = 0$ if and only if $b_{ij} \neq 0$ and for $1 \leq i < j \leq t$ there is an integer λ_{ij} such that the multiset $\{a_{ik} - a_{jk} | k = 1, \dots, t\} \cup \{b_{ik} - b_{jk} | k = 1, \dots, t\}$ contains each element of G exactly λ_{ij} times.

17.22 Example A $(\mathbb{Z}_3, 7, 7)$-complementary pair. Let A and B be the circulant matrices with respective first rows $(w^2, w, w, 0, w, 0, 0)$ and $(0, 0, 0, w^2, 0, e, w)$. An (EA(12),7,28)-complementary pair is obtained by developing the rows $(a_1w^2, a_2w, a_3w, 0, a_4w, 0, 0)$ and $(0, 0, 0, a_1w^2, 0, a_2, a_3w)$ for $(a_1, a_2, a_3, a_4) = (e, e, e, e)$, (e, a, b, ab), (e, ab, a, b), and (e, b, ab, a).

17.23 Theorem (see [647, 649]) Let a be 0 or 1. If there are a (G, k, b)-complementary pair and a $(g, 2n + a, \lambda)$-difference matrix over G, then there is a $(g, kn + a, b\lambda)$-difference matrix over G.

17.24 Theorem (see [647, 649]) Suppose g is square-free, and let a be 0 or 1. If there is a $(g, 2n+a, \lambda)$-difference matrix over $\mathbb{Z}_g$, then there is a $(g, sn+a, s\lambda)$-difference matrix whenever $s = q^t(q + 1), q \equiv 1 \pmod{g}$ is a prime power and $t = 0, 1$ or 2.

17.25 Remark See [647, 649] for the definition of mixed difference matrices and generalizations of Theorems 17.23 and 17.24. A (g, k, λ)-mixed difference matrix gives a resolvable $\mathrm{TD}_\lambda(k, g)$, and the generalization of Theorem 17.24 gives (g, k, λ)-mixed difference matrices for $(g, k, \lambda) =$ (4,20,40), (4,40,20), (4,52,26), (4,60,30), (9,81,20), (12,42,14), (12,78,26), (12,42,28), (16,144,18), (16,288,36), (18,20,20), (24,78,26), (28,61,30). Of these, some have many more rows than the analogous difference matrices.

17.26 Let $x \le \lambda$. A (g, v, λ, x)-*impulse matrix* over the group G is a $v \times (\lambda g - x)$ array $A = (a_{ij})$ of elements of G such that the multisets $\{a_{ik} - a_{jk} | k = 1, \ldots, \lambda g - x\}$ each contain the identity element $\lambda - x$ times and each nonidentity element λ times.

17.27 Theorem Let $k > 0$ be an integer. If n and $n + k$ are prime powers, then an $(n + k, n^2, n, 1 - k)$-impulse matrix over $\mathrm{EA}(n)$ exists.

17.28 Remarks

1. A (g, v, λ, x)-impulse matrix with $x = 0$ or 1 is equivalent to a (g, v, λ)-difference matrix.
2. If there is a (g, v, λ, x)-impulse matrix with $x \ge 0$, then there is a (g, v, λ)-difference matrix.
3. If there is a (g, v, λ)-difference matrix, then there is a $(g, v, \lambda x, x)$-impulse matrix.
4. If there is a (g, v, λ, t)-impulse matrix and a $(g, v, \mu, -t)$-impulse matrix, then there is a $(g, v, \lambda + \mu)$-difference matrix.

17.29 Theorem Let G be a group, and $h = g\lambda - x$. If there are a (g, v, λ, x)-impulse matrix with w zero columns over G, an (h, u, μ)-difference matrix, and a $(g, u, \mu\lambda x, y)$-impulse matrix, then there is a $(g, v(u + 1), \mu\lambda h, y - \mu x^2 + w)$-impulse matrix over G.

17.30 Theorem Let q be a prime power. If there is a $\mathrm{GH}(g, (q+1)/g)$ and a $\mathrm{GH}(g, n(q+1)/g)$ over a group G, then there is a $(g, (q + 1)(q + n - 1), nq(q + 1)/g)$-difference matrix over G.

17.31 Theorem Let $g\lambda = h + 1$.

1. If there is a $(g, v + 1, \lambda)$-difference matrix, an (h, u, μ)-difference matrix, and a $(g, u + 1, \mu\lambda)$-difference matrix, then there is a $(g, v(u + 1), \mu\lambda h, 1 - \mu)$-impulse matrix.
2. If there is a $(g, v + 1, \lambda)$-difference matrix, an (h, v, μ)-difference matrix, and a $(g, u+1, \mu\lambda)$-difference matrix, then there is a $(g, u+v^2, \mu\lambda h)$-difference matrix.

17.32 Remarks See [647] for special cases of Theorems 17.29 and 17.31. The difference matrix in Theorems 17.29 and 17.31 may be replaced by the appropriate resolvable transversal design.

17.33 Theorem [648] Let H be a finite group of odd order and let $G = \mathbb{Z}_2^s \times H$, where $s \geq 0$; Let g be the order of the group G. Then there exists an integer $N(k;G)$ such that

1. if $s \neq 1$, there is a $(g, k; \lambda)$-difference matrix over G for all $\lambda > N(k;G)$;
2. if $s = 1$, there is a $(g, k; 2\lambda)$-difference matrix over G for all $\lambda > N(k;G)$.

17.34 A set of m disjoint blocks, together containing c points of a PBD on v points is a *partial parallel class* of *width* $m + v - c$. A PBD is an (ℓ, w)-*PBD* if its blocks can be partitioned into ℓ partial parallel classes of maximum width w.

17.35 Theorem [558] If an (ℓ, w)-PBD of index λ on v points exists, then for any prime power s satisfying $w \leq s \leq \lfloor \frac{\ell}{\lambda} \rfloor$, there exists a $(s, v; \ell - \lambda)$-difference matrix over EA(s). In fact, there is a $(s, v, \ell - \lambda, l - \lambda s)$-impulse matrix over EA$(s)$.

17.36 Theorem [558] Let $v = 1 + nk$ be a prime power, with v or k even. For any odd prime power s satisfying $n + 1 \leq s \leq \lfloor \frac{v}{k-1} \rfloor$, there exists a $(s, v; \frac{v-k+1}{2})$-difference matrix.

17.37 Theorem [558] If an $\mathrm{OA}_\lambda(k, n)$ exists having λ constant columns, then, over any group G of order $n + 1$, there is a $(n + 1, k; \lambda(n - 1))$-difference matrix.

17.38 Corollary [558] Let v be a prime power with $v = 1 + nk$ for n and k integers satisfying $n \geq k-2 \geq 0$. For any group G of order $n+1$, there is a $(n+1, v; 2+(n-1)k)$-difference matrix over G.

17.39 Theorem [1559] Let H be a multiplicative group of order n and $\widehat{H} = H \cup \{0\}$ (where $0 = 0 \odot h^{-1} = h \odot 0^{-1} = 0 \odot 0^{-1}$). Suppose that there is a $v \times w$ matrix $M = [m_{i,j}]$, with entries $m_{i,j} \in \widehat{H}$, satisfying the following conditions: (1) the number of entries of each row that are different from 0 is a constant k; (2) there is a constant λ such that, in the difference list of two distinct rows, the element 1 appears $\lambda - 1$ times and each $h \in H \setminus \{1\}$ appears λ times. Further, suppose that $(n+1)(2(k+1) - (n+1)\lambda) \geq nw$. Then, for any group G of order $n + 1$, there is a difference matrix over G with v rows and $2(n + 1)(k + 1) - (n + 1)^2\lambda$ columns and of index $2(k + 1) - (n + 1)\lambda$.

17.40 Remark Tables 17.42 and 17.43 give lower bounds on the number k of rows in an $(s, k; \lambda)$-difference matrix for small values of s and λ. Authorities for each construction are given as superscripts on the table entries; when a superscript is omitted, the value is obtained from Theorem 17.13; when present, the superscript can be interpreted using Table 17.41. The group G carrying the difference matrix is not recorded.

17.41 Table Key for Tables 17.42 and 17.43. Sporadic examples are found in §III.3 and [225], with the exception of (3,5), (3,7), (4,5), (6,6), and (10,2) from [1589].

a	Theorem 17.14
c	Theorem 17.23
d	Theorem 17.24
g	Generalized Hadamard matrix
h	Hadamard matrix
i	Impulse matrix
j	Theorem 17.20
l	Theorem 17.31

m	Corollary 17.38
n	Theorem 17.37
p	Theorem 17.35
q	Theorem 17.36
r	Theorem 17.19
s	Sporadic example
t	Theorem 17.17
w	Theorem 17.30

17.42 Table Lower bounds on k in $(s, k; \lambda)$-difference matrices with $2 \le s \le 50$ and $1 \le \lambda \le 18$.

$s \setminus \lambda$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2^{g}	4^{g}	2	8^{g}	2	12^{g}	2	16^{g}	2	20^{g}	2	24^{g}	2	28^{g}	2	32^{g}	2	36^{g}
3	3^{g}	6^{g}	9^{g}	12^{g}	8^{s}	18^{g}	11^{s}	24^{g}	27^{g}	30^{g}	11	36^{g}	13^{i}	21^{c}	24^{t}	48^{g}	24	54^{g}
4	4^{g}	8^{g}	12^{g}	16^{g}	9^{s}	16^{d}	12	32^{g}	36^{g}	16	12	48^{g}	16	56^{g}	21^{i}	64^{g}	32	36
5	5^{g}	10^{g}	7^{q}	20^{g}	25^{g}	15^{p}	17^{q}	25^{d}	20	50^{g}	17	25^{l}	25	20	35^{t}	80^{g}	35^{l}	90^{g}
6	2	6^{s}	2	12^{s}	2	9^{s}	2	12	2	11^{m}	2	12	2	16^{m}	2	24^{l}	2	12
7	7^{g}	14^{g}	9^{s}	28^{g}	11^{q}	18^{i}	49^{g}	28	28^{l}	18	28	49^{d}	28	98^{g}	35^{p}	37^{q}	28	63^{l}
8	8^{g}	16^{g}	9^{s}	32^{g}	9	16	56^{g}	64^{g}	21^{p}	16	32	32	25^{i}	64^{d}	56	128^{g}	25	32
9	9^{g}	18^{g}	27^{g}	36^{g}	18	54^{g}	27	72^{g}	81^{g}	36	36^{i}	108^{g}	49^{i}	54	54	81^{d}	72	162^{g}
10	2	5^{s}	2	8^{s}	2	5	2	10^{s}	2	5	2	12^{l}	2	5	2	18^{j}	2	19^{m}
11	11^{g}	22^{g}	11	44^{g}	11	22	11	44	19^{q}	30^{i}	121^{g}	44	44^{i}	30	44	44	44	30
12	6^{s}	8^{s}	9^{s}	9^{s}	8	9	9	9	9	11^{j}	30^{d}	36^{t}	9	9	9	12^{a}	9	12^{a}
13	13^{g}	26^{g}	13	52^{g}	13	26	13	52	19^{q}	26	23^{q}	84^{i}	169^{g}	27^{p}	65^{p}	52	52	39^{p}
14	2	6^{s}	2	8^{s}	2	7^{a}	2	8	2	7	2	13^{j}	2	7	2	14^{a}	2	9^{a}
15	5^{s}	8^{s}	7^{s}	8	7	9^{a}	7	10^{a}	7	8	7	10^{a}	7	12^{i}	25^{t}	12^{a}	35^{l}	10^{a}
16	16^{g}	32^{g}	16	64^{g}	16	32	16	128^{g}	16	32	16	64	16	32	90^{i}	256^{g}	33^{p}	39^{p}
17	17^{g}	34^{g}	17	68^{g}	17	34	17	68	19^{q}	34	23^{q}	68	27^{q}	34	31^{q}	272^{g}	289^{g}	39^{p}
18	2	9^{s}	2	9	2	9	2	13^{j}	2	9	2	12^{a}	2	9	2	17^{j}	2	12^{a}
19	19^{g}	38^{g}	19	76^{g}	19	38	19	76	19	38	23^{q}	76	27^{q}	38	31^{q}	76	31	54^{i}
20	4^{a}	8^{s}	5^{a}	10^{s}	5	10^{a}	5	10	7^{a}	10	7	12^{a}	7	10	12^{a}	16^{a}	8	19^{j}
21	6^{s}	8^{s}	7^{a}	8	7	9^{a}	7	12^{a}	9^{a}	8	8	14^{a}	8	11^{a}	9	14^{a}	9	14^{a}
22	2	8^{s}	2	8	2	11^{a}	2	15^{s}	2	11^{a}	2	12^{a}	2	11	2	19^{s}	2	11
23	23^{g}	46^{g}	23	92^{g}	23	46	23	184^{g}	23	46	23	92	27^{q}	46	31^{q}	184	31	46
24	8^{s}	9^{s}	8	9	8	9	8	12^{a}	9^{a}	9	9	16^{a}	9	11^{a}	9	16^{a}	9	16^{a}
25	25^{g}	50^{g}	25	100^{g}	125^{g}	50	50	200^{g}	100	125	50	100	125	100	125	200	100	125
26	2	6^{s}	2	8^{a}	2	12^{a}	2	15^{s}	2	13^{a}	2	13^{a}	2	13^{a}	2	19^{s}	2	13
27	27^{g}	54^{g}	81^{g}	108^{g}	54	81	81	216^{g}	243^{g}	81	81	108	108	81	81	216	216	243
28	6^{s}	8^{s}	7^{a}	8	7	12^{a}	7	14^{a}	9^{a}	9^{a}	8	14^{a}	8	12	11^{a}	16^{a}	9	14^{a}
29	29^{g}	58^{g}	29	116^{g}	29	58	29	232^{g}	29	58	29	116	29	58	31^{q}	232	31	58
30	2	5^{a}	2	6^{a}	2	6^{a}	2	10^{a}	2	6	2	9^{a}	2	6	2	12^{a}	2	7^{a}
31	31^{g}	62^{g}	31	124^{g}	31	62	31	248^{g}	31	62	31	124	31	62	31	248	31	62
32	32^{g}	64^{g}	32	128^{g}	32	64	32	256^{g}	32	64	32	128	32	64	32	512^{g}	32	64
33	6^{s}	8^{s}	9^{a}	11^{a}	8	11^{a}	11^{a}	12^{a}	11^{a}	11	11	18^{a}	11	11	11	22^{a}	11	22^{a}
34	2	7^{s}	2	8^{a}	2	12^{a}	2	16^{a}	2	17^{a}	2	17^{a}	2	17^{a}	2	19^{s}	2	17^{a}
35	6^{s}	8^{s}	7^{a}	10^{a}	7	9^{a}	7	14^{a}	7	14^{a}	7	14^{a}	7	14^{a}	9^{a}	20^{a}	8	14
36	9^{s}	9	9	13^{j}	9	12^{a}	9	16^{a}	12^{a}	12	9	16^{a}	12	12	12	18^{a}	12	18^{a}
37	37^{g}	74^{g}	37	148^{g}	37	74	37	296^{g}	37	74	37	148	37	74	37	296	37	74
38	2	4^{a}	2	8^{a}	2	12^{a}	2	16^{a}	2	19^{a}	2	19^{a}	2	19^{a}	2	19^{a}	2	19^{a}
39	6^{s}	6	9^{a}	12^{a}	8^{a}	13^{a}	11^{a}	13^{a}	13^{a}	13^{a}	11	18^{a}	13^{a}	13	13	24^{a}	13	26^{a}
40	8^{s}	10^{s}	8	10	8	10	8	16^{a}	8	16^{a}	8	15^{a}	8	16^{a}	9^{a}	20^{a}	9	16
41	41^{g}	82^{g}	41	164^{g}	41	82	41	328^{g}	41	82	41	164	41	82	41	328	41	82
42	2	6^{a}	2	7^{a}	2	7^{a}	2	12^{a}	2	7	2	9^{a}	2	7	2	12	2	9^{a}
43	43^{g}	86^{g}	43	172^{g}	43	86	43	344^{g}	43	86	43	172	43	86	43	344	43	86
44	6^{s}	8^{a}	11^{a}	15^{s}	9^{a}	12^{a}	11	19^{s}	11	12	11	16^{a}	11	12	11	22^{a}	11	22^{a}
45	7^{s}	9^{a}	7	10^{a}	9^{a}	10^{a}	9	18^{a}	9	18^{a}	9	20^{a}	9	17^{a}	25^{a}	20^{a}	9	18
46	2	4^{a}	2	8^{a}	2	12^{a}	2	16^{a}	2	20^{a}	2	23^{a}	2	23^{a}	2	23^{a}	2	23^{a}
47	47^{g}	94^{g}	47	188^{g}	47	94	47	376^{g}	47	94	47	188	47	94	47	376	47	94
48	9^{s}	9	9	12^{a}	9	16^{a}	11^{a}	16^{a}	16^{a}	16^{a}	11	18^{a}	13^{a}	16	16	24^{a}	16	27^{a}
49	49^{g}	98^{g}	49	196^{g}	49	98	343^{g}	392^{g}	98	98	196	196	98	343	343	392	98	196
50	2	5^{a}	2	8^{a}	2	12^{a}	2	16^{a}	2	20^{a}	2	24^{a}	2	25^{a}	2	25^{a}	2	25^{a}

17.43 Table Lower bounds on k in $(s, k; \lambda)$-difference matrices with $2 \le s \le 50$ and $19 \le \lambda \le 36$.

$s \backslash \lambda$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2	2	40^{g}	2	44^{g}	2	48^{g}	2	52^{g}	2	56^{g}	2	60^{g}	2	64^{g}	2	68^{g}	2	72^{g}
3	27	36^{d}	33^{t}	30	24	72^{g}	27	30	81^{g}	42^{l}	27	90^{g}	30	96^{g}	36^{i}	51^{l}	28^{c}	108^{g}
4	16	36^{t}	36	32	36	96^{g}	36	48	108^{g}	64^{d}	36	56	32	128^{g}	132^{g}	36	36	144^{g}
5	20	100^{g}	25	25	35^{i}	60^{l}	125^{g}	50	35	50	25	75^{t}	35	80	36^{i}	85^{l}	85^{t}	100^{d}
6	2	25^{j}	2	30^{d}	2	36^{t}	2	31^{m}	2	42^{l}	2	16	2	48^{l}	2	16	2	24
7	49	28	63^{t}	35	37	63^{d}	49	182^{g}	63^{p}	196^{g}	35	91^{l}	49	63	49	49	77^{t}	126^{l}
8	32	32	57^{d}	64	56	72^{t}	32	36^{i}	36^{i}	80^{d}	57	105^{i}	56	256^{g}	36	56^{i}	63^{i}	64
9	49	72	81	54	54	216^{g}	81	72	243^{g}	108^{i}	72	108	54	99^{d}	81	306^{g}	72	324^{g}
10	2	10	2	8	2	27^{n}	2	10	2	12	2	12	2	36^{j}	2	37^{m}	2	19
11	44	81^{i}	44	242^{g}	44	121^{l}	55^{p}	44	44	61^{q}	46^{i}	64^{i}	81	64^{i}	121	55^{i}	121	66^{p}
12	9	22^{j}	11	32^{d}	30	48^{t}	9	11	12	21^{c}	12	12	22	22	33^{d}	36^{i}	30	54^{t}
13	52	52	52	39	52	121^{i}	84	338^{g}	65	169^{l}	52	65	67^{q}	52	52	73^{q}	89^{i}	86^{d}
14	2	14^{a}	2	8	2	26^{j}	2	27^{m}	2	14^{a}	2	30^{l}	2	16^{a}	2	9	2	14
15	8	12^{a}	9	10	10	18^{a}	10	10	10	29^{m}	12	40^{t}	12	65^{l}	12	68^{l}	12	20^{a}
16	64	64	64^{i}	39	90	128	64	39	64	64	128^{i}	95^{d}	90	512^{g}	64	64	64	96^{p}
17	65^{i}	85^{p}	68	39	65	68	68	39	65	68	68	39	68^{i}	289^{d}	272	578^{g}	68	96^{p}
18	2	18^{a}	2	9	2	18^{a}	2	12	2	18^{a}	2	20^{a}	2	34^{j}	2	12	2	24^{a}
19	361^{g}	85^{p}	76^{i}	54	76	76	76	54	76	76	76	54	76	76	76	54	76	289^{i}
20	12^{i}	19^{r}	12^{a}	10	10	16^{a}	10	10	12	16^{a}	10	16^{a}	12	20^{a}	12	16	12	38^{j}
21	8	25^{i}	36^{t}	11	9	18^{a}	9	13^{a}	9	14	12	14	9	24^{a}	14	14	11	27^{a}
22	2	20^{a}	2	11	2	24^{l}	2	11	2	22^{a}	2	11	2	22^{a}	2	11	2	22^{a}
23	31	92	43^{q}	66^{i}	529^{g}	184	46	66	92	92	46	66	184	184	69^{p}	66	92	92
24	9	16^{a}	9	23^{j}	56^{d}	64^{t}	9	13^{a}	9	16	9	16	12	24^{a}	9	16	16	27^{a}
25	100	125	125	100	125	216^{i}	625^{g}	125	100	125	125	125	200^{i}	200	200	125	125	125
26	2	20^{a}	2	13	2	25^{j}	2	13	2	28^{l}	2	13	2	26^{a}	2	13	2	26^{a}
27	81	108	108	108	81	216	216	216	729^{g}	108	108	156^{p}	108	216	216	243^{i}	216	243
28	9	14	12^{a}	12	11	16^{a}	9	27^{j}	30^{d}	36^{t}	12	14	11	28^{a}	12	14	14	28^{a}
29	31	116	43^{q}	58	47^{q}	232	47	58	47	196^{i}	841^{g}	156^{p}	116^{i}	232	116	116	232^{i}	196
30	2	12^{a}	2	6	2	12^{a}	2	7	2	29^{j}	2	9^{a}	2	32^{l}	2	7	2	12
31	31	124	43^{q}	62	47^{q}	248	47	62	47	124	59^{q}	156^{p}	961^{g}	496^{p}	496^{l}	124	124	186^{p}
32	32	128	32	64	32	256	32	64	32	128	32	64	992^{g}	1024^{g}	69^{p}	128^{i}	128	186^{p}
33	11	22^{a}	11	11	11	22^{a}	11	13^{a}	11	21^{a}	11	22^{a}	32^{j}	30^{d}	36^{t}	22	11	27^{a}
34	2	20^{a}	2	17	2	24^{a}	2	17	2	28^{a}	2	17	2	32^{a}	2	17	2	34^{a}
35	9	25^{a}	9	14	9	18^{a}	11^{a}	14	9	20^{a}	10	18^{a}	9	25^{a}	11	15^{i}	36^{t}	20
36	12	16	12	13	12	27^{a}	12	16	27^{a}	18^{a}	12	18^{a}	13	32^{a}	12	18	56^{i}	81^{t}
37	37	148	43^{q}	74	47^{q}	296	47	74	47	148	59^{q}	74	59	296	67^{q}	74	71^{q}	360^{i}
38	2	20^{a}	2	19	2	24^{a}	2	19	2	28^{a}	2	19	2	32^{a}	2	19	2	37^{j}
39	13	26^{a}	13	13	13	26^{a}	13	13	13	21^{a}	13	24^{a}	13	26^{a}	13	24	13	27^{a}
40	9	25^{a}	9	16	9	16	9	16	9	20^{a}	9	16	9	25^{a}	9	16	25^{a}	20
41	41	164	43^{q}	82	47^{q}	328	47	82	47	164	59^{q}	82	59	328	67^{q}	82	71^{q}	164
42	2	11^{a}	2	7	2	12	2	9	2	14^{a}	2	9	2	14^{a}	2	9	2	12
43	43	172	43	86	47^{q}	344	47	86	47	172	59^{q}	86	59	344	67^{q}	86	71^{q}	172
44	11	16	11	15	11	22^{a}	11	19	12^{a}	22^{a}	11	21^{a}	12	32^{a}	12	22	12	36^{a}
45	10	25^{a}	17^{a}	18	18	25^{a}	18	18	20	20	17	27^{a}	20	25^{a}	18	18	25	25^{a}
46	2	23^{a}	2	23^{a}	2	24^{a}	2	23	2	28^{a}	2	23	2	32^{a}	2	23	2	36^{a}
47	47	188	47	94	47	376	47	94	47	188	59^{q}	94	59	376	67^{q}	94	71^{q}	188
48	16	30^{a}	16	16	16	32^{a}	16	16	16	21^{a}	16	24^{a}	16	32^{a}	16	24	16	32^{a}
49	196	196	343	343	343	392	196	196	196	343	343	343	343	392	196	196	343	343
50	2	25^{a}	2	25^{a}	2	25^{a}	2	25^{a}	2	28^{a}	2	25	2	32^{a}	2	25	2	36^{a}

17.4 Quasi-Difference Matrices

17.44 Let G be an abelian group of order n. A $(n, k; \lambda, \mu; u)$-*quasi-difference matrix* (QDM) is a matrix $Q = (q_{ij})$ with k rows and $\lambda(n-1+2u)+\mu$ columns, with each entry either empty (usually denoted by $-$) or containing a single element of G. Each row contains exactly λu empty entries, and each column contains at most one empty entry. Furthermore, for each $1 \le i < j \le k$, the multiset

$$\{q_{i\ell} - q_{j\ell} : 1 \le \ell \le \lambda(n-1+2u)+\mu, \text{ with } q_{i\ell} \text{ and } q_{j\ell} \text{ not empty}\}$$

contains every nonzero element of G λ times and contains 0 μ times.

17.45 Examples A (3,4;1,0;1)-QDM and an (11,4;1,0;3)-QDM (see [225]).

$-$	0	1	2
0	$-$	2	1
1	2	$-$	0
2	1	0	$-$

0	6	4	1	$-$	2	6	0	$-$	8	9	0	$-$	1	4	0
1	0	6	4	0	$-$	2	6	0	$-$	8	9	0	$-$	1	4
4	1	0	6	6	0	$-$	2	9	0	$-$	8	4	0	$-$	1
6	4	1	0	2	6	0	$-$	8	9	0	$-$	1	4	0	$-$

17.46 Examples $(19, 7; \lambda, \lambda; 1)$-QDM for $\lambda = 2, 3$. Let A and C be the circulant matrices with first rows $(-\ 4\ 9\ 6\ 6\ 9\ 4)$ and $(0\ 2\ 14\ 11\ 3\ 7\ 1)$, respectively. Then $(A \mid 2A \mid C \mid -C \mid 7C \mid -7C)$ is a $(19, 7; 2, 2; 1)$-QDM, and $(3A \mid 6A \mid 8A \mid C \mid -C \mid 3C \mid -3C \mid 4C \mid -4C)$ is a $(19, 7; 3, 3; 1)$-QDM.

17.47 Construction [2150] If a $(n, k; \lambda, \mu; u)$-QDM exists and $\mu \le \lambda$, then an $\mathrm{ITD}_\lambda(k, n+u; u)$ exists. Start with a $(n, k; \lambda, \mu; u)$-QDM A over the group G. Append $\lambda - \mu$ columns of zeroes. Then select u elements $\infty_1, \ldots, \infty_u$ not in G, and replace the empty entries $(-)$, each by one of these infinite symbols, so that ∞_i appears exactly once in each row, for $1 \le i \le u$. Develop the resulting matrix over the group G (leaving infinite symbols fixed), to obtain a $k \times \lambda(n^2 + 2nu)$ matrix T. Then T is an incomplete orthogonal array with k rows and index λ, having $n+u$ symbols and one hole of size u. The technique in Remark III.3.10 then gives an $\mathrm{ITD}_\lambda(k, n+u; u)$.

17.48 Let q be a prime power and let $q = mt + 1$ for m, t integer. Let ω be a primitive element of $\mathbb{F}_q$. A *V(m,t) vector* is a vector $(a_1, \ldots, a_{m+1})$ for which, for each $1 \le k < m$, the differences $\{a_{i+k} - a_i : 1 \le i \le m+1, i+k \ne m+2\}$ represent the m cyclotomic classes of $\mathbb{F}_{mt+1}$ (compute subscripts modulo $m+2$). In other words, for fixed k, if $a_{i+k} - a_i = \omega^{mx+\alpha}$ and $a_{j+k} - a_j = \omega^{my+\beta}$, then $\alpha \not\equiv \beta \pmod m$.

17.49 Construction A quasi-difference matrix from a $V(m, t)$ vector. Starting with a $V(m, t)$ vector $(a_1, \ldots, a_{m+1})$, form a single column of length $m+2$ whose first entry is empty, and whose remaining entries are $(a_1, \ldots, a_{m+1})$. Form t columns by multiplying this column by the tth roots, the powers of ω^m. From each of these t columns, form $m+2$ columns by taking the $m+2$ cyclic shifts of the column. The result is a $(q, m+2; 1, 0; t)$-QDM.

17.50 Theorem [863] Suppose that a $V(m, t)$ vector exists and write $q = mt+1$. If $(m, n) = 1$, then a $V(m, \frac{q^n-1}{m})$ exists.

17.51 Theorem [484] Let m and t be two positive integers, not both even, for which $mt+1$ is a prime power. Let $u = \lfloor (m+1)/2 \rfloor$, $F = (u-1)m^u$, and $E = (m-1)F - m^{u-1} - 1$. Then whenever $mt + 1 > ((E + \sqrt{E^2 + 4F})/2)^2$, there exists a $V(m, t)$ vector.

17.52 Theorem A $V(m, t)$ vector exists if m and t are not both even and $t \ge m-1$,

1. whenever $m \le 8$ and $mt+1$ is a prime power, except for $(m, t) \in \{(3, 5), (7, 9)\}$, and possibly when $(m, t) \in \{(8, 3^6), (8, 3^{12})\}$ (see [484]);
2. whenever $mt + 1 \le 5000$, $m \in \{9, 10, 11\}$ and $mt+1$ is prime, and $(m, t) \notin \{(9, 8), (11, 18)\}$, as no $V(9, 8)$ or $V(11, 18)$ exists [5, 527];

3. when $m = 12$, $12t + 1$ is prime, and $829 \le 12t + 1 \le 5000$ [6]. (There is no $V(12, t)$ with $t \le 15$.)

17.53 Remarks For $m \le 8$, these sufficient conditions are necessary. While the condition that m and t not both be even holds for every m, the condition that $t \ge m - 1$ is only a conjectured necessary condition in general. See [484].

17.54 Table Some $V(m, t)$ vectors with $3 \le m \le 10$, $mt + 1$ prime.

Solutions for $V(m, t)$, $m = 3$, $v = mt + 1$

t	v	Vector	t	v	Vector	t	v	Vector
2	7	(0 1 3 6)	4	13	(0 1 3 9)	6	19	(0 1 3 7)
10	31	(0 1 4 13)	12	37	(0 1 3 10)	14	43	(0 1 4 13)
20	61	(0 1 3 13)	22	67	(0 1 3 7)	24	73	(0 1 3 15)
26	79	(0 1 3 8)	32	97	(0 1 3 9)	34	103	(0 1 3 7)

Solutions for $V(m, t)$, $m = 4$, $v = mt + 1$

t	v	Vector	t	v	Vector	t	v	Vector
3	13	(0 1 3 7 2)	7	29	(0 1 3 7 19)	9	37	(0 1 3 2 8)
13	53	(0 1 3 7 19)	15	61	(0 1 3 7 5)	25	101	(0 1 3 2 31)

Solutions for $V(m, t)$, $m = 5$, $v = mt + 1$

t	v	Vector	t	v	Vector	t	v	Vector
6	31	(0 1 3 7 30 17)	8	41	(0 1 3 22 14 18)	12	61	(0 1 3 7 23 50)
14	71	(0 1 3 9 25 54)	20	101	(0 1 3 10 43 91)	26	131	(0 1 3 6 48 15)

Solutions for $V(m, t)$, $m = 6$, $v = mt + 1$

t	v	Vector	t	v	Vector
5	31	(0 1 7 30 12 21 15)	7	43	(0 1 3 16 35 26 36)
11	67	(0 1 3 14 7 24 27)	13	79	(0 1 3 7 55 47 34)
17	103	(0 1 3 2 14 99 29)	21	127	(0 1 4 13 66 93 45)

Solutions for $V(m, t)$, $m = 7$, $v = mt + 1$

t	v	Vector	t	v	Vector
6	43	(0 1 12 27 37 16 30 35)	10	71	(0 1 3 45 9 50 28 16)
16	113	(0 1 3 7 82 72 93 39)	18	127	(0 1 3 6 97 114 99 26)

Solutions for $V(m, t)$, $m = 8$, $v = mt + 1$

t	v	Vector	t	v	Vector
9	73	(0 1 20 70 23 59 3 8 19)	11	89	(0 1 6 56 22 35 47 23 60)
17	137	(0 1 3 2 133 126 47 109 74)	29	233	(0 1 4 11 94 60 85 16 198)

Solutions for $V(m, t)$, $m = 9$, $v = mt + 1$

t	v	Vector	t	v	Vector
8	73	none	12	109	(0 1 4 19 56 22 83 95 52 96)
14	127	(0 1 11 25 37 8 100 23 95 42)	18	163	(0 1 3 7 36 30 158 94 52 70)
20	181	(0 1 3 19 145 70 173 159 18 85)	22	199	(0 1 3 31 99 190 174 46 87 127)
30	271	(0 1 3 8 197 68 119 13 215 105)	34	307	(0 1 3 13 140 81 74 131 303 238)
42	379	(0 1 3 6 66 258 186 346 104 152)	44	397	(0 1 4 11 144 103 216 77 160 363)

Solutions for $V(m,t)$, $m = 10$, $v = mt + 1$

t	v	Vector	t	v	Vector
13	131	(0 1 5 10 22 6 14 9 53 129 84)	15	151	(0 1 45 146 51 97 70 137 85 133 18)
19	191	(0 1 3 96 143 156 182 142 4 189 25)	21	211	(0 1 6 188 205 39 101 113 30 32 42)
25	251	(0 1 3 85 140 178 195 22 48 179 188)	27	271	(0 1 3 82 109 241 36 112 141 263 126)
31	311	(0 1 3 57 128 247 289 239 70 271 96)	33	331	(0 1 3 67 319 44 249 146 302 282 90)
43	431	(0 1 6 29 170 207 385 290 375 32 336)	49	491	(0 1 3 8 406 72 335 197 324 383 395)

See Also

§III.3	Difference matrices generate transversal designs.
§III.4	Quasi-difference matrices generate incomplete transversal designs.
§III.6	Difference and quasi-difference matrices generate orthogonal arrays and incomplete orthogonal arrays.
§IV.6	Linear spaces are used to construct difference matrices.
§VI.16	Difference matrices are used to construct difference families and graph decompositions [390].
§V.4	A $(g, k; \lambda)$-difference matrix over G is a GBRD$(k, k, g\lambda; G)$.
§V.5	A generalized Hadamard matrix is a difference matrix with the maximum number of rows.
[225]	Develops the theory of difference and quasi-difference matrices and gives numerous examples.
[1074]	Studies difference matrices under the name "difference schemes" and gives connections to orthogonal arrays.

References Cited: [5, 6, 225, 379, 390, 484, 527, 558, 647, 648, 649, 748, 799, 863, 867, 1074, 1221, 1559, 1589, 1847, 1904, 2150]

18 Difference Sets

Dieter Jungnickel
Alexander Pott
Ken W. Smith

18.1 Basics

18.1 Let G be an additively written group of order v. A k-subset D of G is a $(v, k, \lambda; n)$-*difference set* of *order* $n = k - \lambda$ if every nonzero element of G has exactly λ representations as a difference $d - d'$ with elements from D. The difference set is *abelian*, *cyclic*, or the like if the group G has the respective property. The redundant parameter n is sometimes omitted; therefore, the notion of (v, k, λ)-difference sets is also used.

18.2 Remark The term difference set indicates that the groups are written additively. However, it is also possible to write the groups multiplicatively, in which case the difference $d - d'$ must be replaced by $d \cdot d'^{-1}$. Additive notation is used in the case of abelian groups, and multiplicative notation in the nonabelian case as well as in more theoretical investigations, see §18.3.

18.3 Example

1. The set $\{1,3,4,5,9\}$ is an $(11,5,2;3)$-difference set in the group $\mathbb{Z}_{11}$.
2. Let $G = Q \times \mathbb{Z}_2$, where $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group, where the generators satisfy $i^2 = j^2 = k^2 = 1$, $ij = jk = ki = -1$. Then the set $D = \{(1,0),(i,0),(j,0),(k,0),(1,1),(-1,1)\}$ is a nonabelian $(16,6,2;4)$-difference set.

18.4 Remarks

1. The group G itself and $G\backslash\{g\}$ for an arbitrary $g \in G$ are $(v,v,v,0)$- and $(v, v-1, v-2; 1)$-difference sets. In the tables these *trivial* difference sets are excluded.
2. The complement of a $(v,k,\lambda;n)$-difference set is again a difference set with parameters $(v, v-k, v-2k+\lambda; n)$. Therefore, assume that $k \leq v/2$ (the case $k = v/2$ is actually impossible).
3. A thorough investigation of difference sets is in [225]. A more recent survey is [2173]. If not stated otherwise, proofs for all the theorems and results throughout this chapter can be found in [225].

18.5 The *development* of a difference set D is the incidence structure *dev(D)* whose points are the elements of G and whose blocks are the translates $gD = \{gd : d \in D\}$.

18.6 Theorem The existence of a $(v,k,\lambda;n)$-difference set is equivalent to the existence of a symmetric (v,k,λ)-design $\mathcal{D}$ admitting G as a point regular automorphism group; that is, for any two points p and q, there is a unique group element g that maps p to q. The design $\mathcal{D}$ is isomorphic with *dev(D)*. The design is cyclic when the difference set is cyclic.

18.7 Remarks

1. Many symmetric designs do not have difference set representations.
2. Since difference sets yield symmetric designs, the parameters v, k and λ must satisfy the trivial necessary conditions for the existence of a symmetric design ($\lambda(v-1) = k(k-1)$) as well as the Bruck–Ryser–Chowla condition. (See §II.6.2.)
3. The parameters of difference sets must also satisfy some further necessary conditions, see Theorem 18.22.
4. For $(v,k,\lambda;n)$-difference sets, the inequality $4n-1 \leq v \leq n^2+n+1$ holds, since this inequality holds for symmetric designs. Difference sets with $v = 4n-1$ are *Paley-type difference sets*, those with $v = n^2+n+1$ are *planar*.
5. There are examples of designs that admit nonabelian regular automorphism groups (difference sets), but no abelian ones. These difference sets are *genuinely nonabelian*, see Example 18.56 and Remark 18.61.

18.8 Two difference sets D_1 (in G_1) and D_2 (in G_2) are *equivalent* if there is a group isomorphism φ between G_1 and G_2 such that $D_1^\varphi = \{d^\varphi : d \in D_1\} = gD_2$ for a suitable $g \in G$. The difference sets are *isomorphic* if the designs *dev(D_1)* and *dev(D_2)* are isomorphic. This does not necessarily imply that G_1 and G_2 are isomorphic.

18.9 Remark Equivalent difference sets are isomorphic; however, there are examples of isomorphic difference sets that are not equivalent, see Table 18.77, for instance. In the cyclic case, in all known examples, isomorphic difference sets are also equivalent.

18.10 Remark The main problem concerning difference sets is to give necessary and sufficient conditions for their existence. These conditions sometimes depend only on the parameters $(v,k,\lambda;n)$, sometimes also on the structure of the underlying group G. Another problem is to classify all $(v,k,\lambda;n)$-difference sets in certain groups.

18.2 Multipliers

18.11 A *multiplier* of a difference set D in G is an automorphism φ of G such that $D^\varphi = gD$ for some $g \in G$. If G is abelian and φ is the automorphism that maps h to h^t, then t is a *numerical* multiplier.

18.12 Theorem If φ is a multiplier of the difference set D, then there is at least one translate gD of D that is fixed by φ. If D is abelian and $\gcd(v,k) = 1$, then there is a translate fixed by all multipliers.

18.13 Remarks

1. Multipliers play an important role, in particular in the theory of abelian difference sets.
2. The content of the multiplier theorems is the assertion that certain automorphisms (integers) have to be (numerical) multipliers of an abelian difference set depending only on the parameters v, k and λ. Theorem 18.14 is the *first multiplier theorem*.

18.14 Theorem Let D be an abelian $(v,k,\lambda;n)$-difference set. If p is a prime that satisfies $\gcd(p,v) = 1$, $p|n$ and $p > \lambda$, then p is a numerical multiplier.

18.15 Conjecture Every prime divisor p of n that is relatively prime to v is a multiplier of a $(v,k,\lambda;n)$-difference set; that is, the condition $p > \lambda$ in Theorem 18.14 is not necessary.

18.16 Remarks

1. Multipliers are useful in constructing difference sets and in proofs of nonexistence. In particular, if $\lambda = 1$, it is conjectured that n must be a prime power; using multipliers, it has been shown that this holds for all values of $n \leq 2{,}000{,}000$ (see [168]).
2. Several attempts have been made to weaken the assumption "$p > \lambda$" in Theorem 18.14 (2nd multiplier theorem, McFarland's multiplier theorem; see [225, 1397]).

18.17 Example Multipliers may be used to construct nonabelian difference sets: The set $D = \{3,6,7,12,14\}$ is a $(21,5,1;4)$-difference set in $(\mathbb{Z}_{21},+)$ with multiplier 4. Denote the automorphism $x \mapsto x+3$ by a, and the automorphism $x \mapsto 4x+1$ by b. Then $G = \langle a,b | a^7 = b^3 = 1, b^{-1}ab = a^4\rangle$ acts regularly on the points of *dev(D)*. A difference set D' in G corresponding to this action is $D' = \{a, a^2, a^4, a^4b, a^5b\}$. This is an illustration of Theorem 18.68.

18.3 Difference Sets: An Algebraic Approach

18.18 Remark Let $\mathbb{F}$ be a field and G a multiplicatively written group. The group algebra $\mathbb{F}[G]$ is the set $\{\sum_{g\in G} \lambda_g \cdot g : \lambda_g \in \mathbb{F}\}$ equipped with an addition and multiplication in the natural way. A subset $D \subseteq G$ is identified with $D = \sum_{g\in D} g$; moreover, $D^{(-1)} = \sum_{g\in D} g^{-1}$.

18.19 Theorem A k-subset $D \subseteq G$ of a group G of order v with identity element e_G is a $(v,k,\lambda;n)$-difference set if and only if $D \cdot D^{(-1)} = n \cdot e_G + \lambda \cdot G$ in $\mathbb{C}[G]$.

18.20 Remark A representation of $\mathbb{F}[G]$ is a homomorphism $\Psi : \mathbb{F}[G] \to GL(m,\mathbb{F})$. Theorem 18.19 shows $\Psi(D)\Psi(D^{(-1)}) = n \cdot \mathbf{I}_n$ if Ψ is nontrivial ($\mathbf{I}_m$ is the identity matrix of order m). If G is abelian, there are $|G|$ different 1-dimensional representations χ

(*characters*). Most nontrivial necessary conditions on the existence of difference sets follow from this group algebra approach in connection with algebraic number theory.

18.21
1. A prime p is *self-conjugate* modulo v if $p^f \equiv -1 \bmod v$.
2. The *exponent* of a group G is the smallest integer v^* such that $g^{v^*} = e_G$ for all $g \in G$.

18.22 Theorem Let D be a $(v, k, \lambda; n)$-difference set in an abelian group G. If a prime p dividing n is self-conjugate modulo the exponent of G, then n must be a square. If p is self-conjugate modulo the exponent of some subgroup of G, then p divides n to an even power.

18.23 Remark Much more powerful nonexistence results follow from Schmidt's field descent method, see [1851]. This approach avoids the self-conjugacy assumption that is crucial in many previous nonexistence results.

18.24 Remark It has been conjectured by Ryser that no cyclic $(v, k, \lambda; n)$-difference sets may exist if $\gcd(v, n) > 1$. This conjecture includes the conjecture about the nonexistence of circulant Hadamard matrices (see Conjecture 18.63). An interesting generalization of this is given next.

18.25 Conjecture (Lander's conjecture [1397]) Let G be an abelian group of order v containing a $(v, k, \lambda; n)$-difference set. If p is a prime dividing n and v, then the Sylow p-subgroup of G cannot be cyclic.

18.26 Theorem [1428] Lander's conjecture is true for $(v, k, \lambda; n)$-difference sets if n is the power of a prime $p \neq 2, 3$.

18.4 Difference Sets with Classical Parameters

18.27 The points and hyperplanes of the projective geometry $\mathrm{PG}(m-1, q)$ form a symmetric design with parameters

$$\left(\frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}, \frac{q^{m-2}-1}{q-1}; q^{m-2}\right)$$

(see §VII.2 or [225]). These parameters are the *classical parameters* $[q, m]$. The parameters of the complementary difference sets are denoted $[q, m]'$

18.28 Construction Let α be a generator of the multiplicative group of $\mathbb{F}_{q^m}$. Then the set of integers $\{i : 0 \leq i < (q^m-1)/(q-1), \mathrm{trace}_{m/1}(\alpha^i) = 0\}$ modulo $(q^m-1)/(q-1)$ form a (cyclic) difference set with the classical parameters $[q, m]$. Here the *trace* denotes the usual trace function $\mathrm{trace}_{m/1}(\beta) = \sum_{i=0}^{m-1} \beta^{q^i}$ from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$. These difference sets are *Singer difference sets*.

18.29 Construction The construction of Singer difference sets with parameters $[q, m]$ is straightforward if a primitive polynomial $f(x) = x^m + \sum_{i=1}^{m} a_i x^{m-i}$ of degree m in $\mathbb{F}_q$ is known. Consider the recurrence relation $\gamma_n = -\sum_{i=1}^{m} a_i \gamma_{n-i}$. Take arbitrary start values, for instance $\gamma_0 = 1, \gamma_1, \ldots, \gamma_{m-1} = 0$. Then the set of integers $\{0 \leq i < \frac{q^m-1}{q-1} : \gamma_i = 0\}$ is a Singer difference set. For instance, $x^4 + x^3 + 2$ is a primitive polynomial over $\mathbb{F}_3$. The recurrence relation $\gamma_n = 2\gamma_{n-1} + \gamma_{n-4}$ yields the sequence

$$1000121220111222202021120102100221202200200 0\ldots$$

which gives the cyclic (40,13,4;9)-difference set {1,2,3,9,17,19,24,26,29,30,35,38,39}.

18.30 Remark See VII.8.8 for a list of primitive polynomials that can be used to construct Singer difference sets using 18.29.

18.31 Construction Let D be an arbitrary cyclic difference set in G with the classical parameters $[q, s]'$. Let G be embedded into $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, which is possible if $s|m$. Let α be a primitive element in $\mathbb{F}_{q^m}$. Then the set of integers $\{0 \le i < \frac{q^m-1}{q-1} : \mathrm{trace}_{m/s}(\alpha^i) \in D\}$ is a difference set with classical parameters $[q, m]'$. Here $\mathrm{trace}_{m/s}(\beta) = \sum_{i=0}^{(m/s)-1} \beta^{q^{si}}$ denotes the relative trace with respect to the subfield $\mathbb{F}_{q^s}$. The difference sets are *Gordon–Mills–Welch difference sets* corresponding to D. Different embeddings of the same difference set D may result in inequivalent difference sets, see [167].

18.32 Remark If D is a Singer difference set with parameters $[q, m]'$, Construction 18.31 may be reformulated: If s divides m and r is relatively prime to $q^s - 1$, then the set of integers $\{0 \le i < (q^m - 1)/(q - 1) : \mathrm{trace}_{s/1}(\mathrm{trace}_{m/s}(\alpha^i)^r) = 0\}$ is a Gordon–Mills–Welch difference set denoted by $\mathrm{GMW}(q, m, s, r)$.

18.33 Remark There are many more constructions of difference sets with parameters $[2, m]$. For instance, it is possible that the Paley difference sets of Construction 18.48 also have classical parameters. There is a construction using monomial hyperovals, see [1532]. A very general and powerful construction is given next.

18.34 Construction (Dillon–Dobbertin construction) Let α be a generator of the multiplicative group of $\mathbb{F}_{2^m}$, and let $t < m/2$ be an integer relatively prime to m, and $k = 4^t - 2^t + 1$. Then the set $D = \{(x + 1)^k + x^k + 1 : x \in \mathbb{F}_{2^m}, x \ne 0, 1\} \subseteq \mathbb{F}_{2^m}^*$ is a difference set with the classical parameters $[2, m]$, a *Dillon–Dobbertin difference set* or a $\mathrm{DD}(m, t)$. If $m = 3t \pm 1$, then the set $D = \mathbb{F}_{2^m}^* \setminus \{(x + 1)^k + x^k : x \in \mathbb{F}_{2^m}\} \subseteq \mathbb{F}_{2^m}^*$ is also a difference set with parameters $[2, m]$. These difference sets are abbreviated by $\mathrm{NCY}(m)$ since the validity of the construction has been conjectured by No, Chung, and Yun. Proofs are contained in [706, 707].

18.35 Remark The series of GMW-difference sets and DD-difference sets show that the number of inequivalent difference sets grows rapidly. In these two series, inequivalent difference sets are in general also nonisomorphic, see [1261] for the GMW case and [733] for the Dillon–Dobbertin case.

18.36 Remark There are additional constructions of difference sets with classical parameters $[3^e, m]$. They can be described using the canonical epimorphism $\rho : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$.

18.37 Construction [111] Let $R = \{a \in \mathbb{F}_{3^m}^* : a = x + x^6$ has 4 solutions with $x \in \mathbb{F}_{3^m}\}$ with $m > 1$. Then the set $\rho(R)$ is a difference set with parameters $[3, m]'$.

18.38 Construction [1090] Let $q = 3^e$, $e \ge 1$, $m = 3k$, $d = q^{2k} - q^k + 1$. If $R = \{x \in \mathbb{F}_{q^m} : \mathrm{trace}_{m/1}(x + x^d) = 1\}$, then $\rho(R)$ is a difference set with parameters $[3^e, m]'$.

18.39 Conjecture Let $m \ge 3$ be an odd integer, and let $d = 2 \cdot 3^{(m-1)/2} + 1$. If $R = \{x \in \mathbb{F}_{q^m} : \mathrm{trace}_{m/1}(x + x^d) = 1\}$, then $\rho(R)$ is a difference set with parameters $[3, m]'$.

18.40 Remarks

1. As pointed out in [2173], Conjecture 18.39 has been proven recently.
2. The construction 18.37 explains one of the three difference sets with parameters $(121, 40, 13; 27)$ listed in Baumert's book as sporadic [167], see also Table 18.83.

18.5 Other Series of Difference Sets

18.41 Construction Let q be a prime power and d a positive integer. Let G be a group of order $v = q^{d+1}(q^d + \cdots + q^2 + q + 2)$ that contains an elementary abelian subgroup E of order q^{d+1} in its center. View E as the additive group of $\mathbb{F}_q^{d+1}$. Put $r = (q^{d+1} - 1)/(q - 1)$ and let $H_1, \ldots, H_r$ be the hyperplanes of order q^d of E. If $g_0, \ldots, g_r$

are distinct coset representatives of E in G then $D = (g_1+H_1)\cup(g_2+H_2)\cup\cdots\cup(g_r+H_r)$ is a *McFarland difference set* denoted $\mathrm{MF}(q,d)$ with parameters

$$\left(q^{d+1}(1+\tfrac{q^{d+1}-1}{q-1}), q^d\cdot\tfrac{q^{d+1}-1}{q-1}, q^d\cdot\tfrac{q^d-1}{q-1}; q^{2d}\right).$$

18.42 Construction Let E be the elementary abelian group of order 3^{d+1} and let G be a group of order $v = 3^{d+1}(3^{d+1}-1)/2$ containing E in its center. Put $m = (3^{d+1}-1)/2$ and let $H_1,\ldots,H_m$ denote the subgroups of E of order 3^d. If $g_1,\ldots,g_m$ are distinct coset representatives of E in G, then $D = (g_1+(E\backslash H_1))\cup(g_2+H_2)\cup(g_3+H_3)\cup\cdots\cup(g_m+H_m)$ is a *Spence difference set* denoted $\mathrm{Sp}(d)$. It has parameters

$$\left(3^{d+1}\cdot\tfrac{3^{d+1}-1}{2}, 3^d\cdot\tfrac{3^{d+1}+1}{2}, 3^d\cdot\tfrac{3^d+1}{2}; 3^{2d}\right).$$

18.43 Remarks

1. The parameters that occur in Constructions 18.41 and 18.42 are McFarland and Spence parameters, respectively. There are difference sets with McFarland parameters not constructed from 18.41.
2. There are many inequivalent McFarland and Spence difference sets.
3. If $q = 2$, the McFarland construction yields Hadamard difference sets, see §18.6.
4. If $q = 2$ and G is elementary abelian, then the difference sets with McFarland parameters are also known as *bent functions*.

18.44 Theorem Necessary and sufficient conditions about difference sets with McFarland parameters.

1. An abelian group G contains a difference set with parameters $\mathrm{MF}(2^t,1)$ if and only if G contains an elementary abelian subgroup of order 2^{t+2}, see [109].
2. Let $q = p^f$ for some odd prime p, and let G be an abelian group such that p is self-conjugate modulo the exponent of G. Then G contains a difference set with parameters $\mathrm{MF}(q,d)$ if and only if G contains an elementary abelian subgroup of order q^{d+1}, see [1492].

18.45 Let q be a prime power, and let t be any positive integer. Difference sets with parameters

$$\left(4q^{2t}\cdot\tfrac{q^{2t}-1}{q^2-1}, q^{2t-1}\cdot\tfrac{2q^{2t}+q-1}{q+1}, q^{2t-1}(q-1)\cdot\tfrac{q^{2t-1}+1}{q+1}; q^{4t-2}\right)$$

are *Davis–Jedwab–Chen* difference sets.

18.46 Remark If $t = 1$, Davis–Jedwab–Chen difference sets are Hadamard difference sets.

18.47 Theorem [225, 1851] A Davis–Jedwab–Chen difference set in an abelian group G exists when:

1. $q = 3^f$, the Sylow 3-subgroup of G is elementary abelian;
2. $q = p^{2f}$, p odd, the Sylow p-subgroup of G is elementary abelian;
3. $q = 2^f$, the Sylow 2-subgroup of G has rank $\geq 2f+1$; or
4. $q = 2$, $\exp(G) \leq 4$.

18.48 Construction The subsets of $\mathbb{F}_q$ that are difference sets in the additive subgroup of $\mathbb{F}_q$ (some with classical parameters). These are *cyclotomic difference sets*.

- $\mathbb{F}_q^{(2)} = \{x^2 : x\in\mathbb{F}_q\backslash\{0\}\}, q\equiv 3 \pmod 4$ (quadratic residues, *Paley difference sets*);
- $\mathbb{F}_q^{(4)} = \{x^4 : x\in\mathbb{F}_q\backslash\{0\}\}, q = 4t^2+1, t$ odd;
- $\mathbb{F}_q^{(4)}\cup\{0\}, q = 4t^2+9, t$ odd;
- $\mathbb{F}_q^{(8)} = \{x^8 : x\in\mathbb{F}_q\backslash\{0\}\}, q = 8t^2+1 = 64u^2+9, t, u$ odd;
- $\mathbb{F}_q^{(8)}\cup\{0\}, q = 8t^2+49 = 64u^2+441, t$ odd, u even;

- $H(q) = \{x^i : x \in \mathbb{F}_q \backslash \{0\}, i \equiv 0, 1 \text{ or } 3 \pmod 6\}$ $q = 4t^2 + 27, q \equiv 1 \pmod 6$ (*Hall difference sets*).

18.49 Construction Let q and $q+2$ be prime powers. Then the set $D = \{(x, y) : x, y$ are both nonzero squares or both nonsquares or $y = 0\}$ is a *twin prime power difference set* (TPP(q)) with parameters

$$\left(q^2 + 2q, \tfrac{q^2+2q-1}{2}, \tfrac{q^2+2q-3}{4}; \tfrac{q^2+2q+1}{4}\right)$$

in the group $(\mathbb{F}_q, +) \oplus (\mathbb{F}_{q+2}, +)$, see [225].

18.6 Difference Sets and Hadamard Matrices

18.50 Remark A Hadamard matrix of size $4n$ gives rise to a symmetric $(4n-1, 2n-1, n-1; n)$-design. If the matrix is regular (it has constant row sum), then it also yields a symmetric $(4u^2, 2u^2 - u, u^2 - u; u^2)$-design. Both types of design can sometimes be represented by difference sets. (See §V.1)

18.51 Difference sets with $v = 4n - 1$ are *Paley-type difference sets.*

18.52 Remarks The Paley difference sets and the twin prime power difference sets are examples of Paley-type difference sets. Other difference sets of Paley-type are the difference sets with classical parameters $[2, m]$. Parametrically, these are the only known constructions of Paley-type difference sets. There are many nonexistence results that rule out the existence of Paley-type difference sets.

18.53 Theorem Small orders n for which the existence of a cyclic Paley-type difference set is undecided (see [168]): $n \in \{860, 1089, 2148, 2209, 2284, 2304, 2356\}$.

18.54 A $(4u^2, 2u^2 - u, u^2 - u; u^2)$-difference set is a *Hadamard difference set.*

18.55 Theorem [225] Let $G \cong H \times EA(w^2)$ be an abelian group of order $4u^2$ with $u = 2^a 3^b w^2$ where w is the product of not necessarily distinct primes $p \equiv 3 \pmod 4$ and $EA(w^2)$ denotes the group of order w^2, which is the direct product of groups of prime order. If H is of type $(2^{a_1})(2^{a_2}) \dots (2^{a_s})(3^{b_1})^2 \dots (3^{b_r})^2$ with $\sum a_i = 2a+2$ $(a \geq 0, a_i \leq a+2)$, $\sum b_i = 2b$ $(b \geq 0)$, then G contains a Hadamard difference set of order u^2.

18.56 Example The set

$$\begin{aligned} D = {} & (1 + a + a^4) + (1 + a)b + (1 + a^2 + a^3 + a^4)b^2 + (1 + a + a^2 + a^3)b^3 \\ & + (1 + a^4)b^4 + [(a^2 + a^4) + a^4 b + a^3 b^2 + (1 + a^2)b^3 + (a + a^2 + a^3 + a^4)b^4]c \\ & + [a^4 + (a + a^2 + a^4)b + (a + a^4)b^2 + (1 + a^2 + a^4)b^3 + a^3 b^4]c^2 \\ & + [(a^3 + a^4) + (1 + a^4)b + a^3 b^2 + (a + a^2 + a^3 + a^4)b^3 + ab^4]c^3 \end{aligned}$$

is a $(100, 45, 20)$-difference set in the nonabelian group

$$\langle a, b, c : a^5 = b^5 = c^4 = [a, b] = cac^{-1}a^{-2} = cbc^{-1}b^{-2} = 1\rangle.$$

No abelian difference sets with these parameters can exist, see [1565, 1931].

18.57 Theorem [225] An abelian group of order 2^{2a+2} contains a Hadamard difference set if and only if the exponent of G is at most 2^{a+2}.

18.58 Example The set $D = (1 + x^{16})[1 + x^4 + x(1 + x^8) + y(1 + x^{12})] +$
$(1 + x^8)[(x^{-2} + x^2) + (x^{13} + x^3) + y(x^{-2} + x^{18}) + y(x^{-3} + x^3)]$
is a $(64, 28, 12)$-difference set in the nonabelian group $\langle x, y : x^{32} = y^2 = yxyx^{-17} = 1\rangle$ [637]. This group has exponent 32. It is the first example in an infinite family of nonabelian difference sets with exponent higher than allowed by Theorem 18.57 for abelian groups.

18.59 Remark Many constructions of Hadamard difference sets are known. In particular in the case of elementary abelian groups, the number of inequivalent difference sets grows rapidly. Theorem 18.60 produces many nonabelian Hadamard difference sets.

18.60 Theorem (Dillon [705]) Let H_1 and H_2 be two groups with Hadamard difference sets. Then any group G that can be written as the product of H_1 and H_2 also has a Hadamard difference set.

18.61 Remark The only known genuinely nonabelian difference sets (see 18.7) are Hadamard difference sets with parameters $(4u^2, 2u^2 - u, u^2 - u)$ with u a multiple of 2, 3, or 5, or occur as difference sets with parameters $(96, 20, 4)$, see [52].

18.62 Theorem [1161] Suppose p is a prime greater than 3 and G is a group of order $4p^2$ containing a Hadamard difference set. Then either G has an irreducible representation of degree 4 or $p \equiv 1 \pmod 4$ and G is the single group

$$G = \langle x, y, z : x^p = y^p = z^4 = [x, y] = [x, z] = zyz^{-1}y = 1\rangle.$$

18.63 Conjecture There is no cyclic Hadamard difference set of order $n > 1$.

18.64 Remarks

1. The trivial $(4, 1, 0)$-difference set provides an example of a circulant Hadamard matrix of order 1.
2. The existence of a cyclic Hadamard difference set of order n^2 is equivalent to the existence of a circulant Hadamard matrix of size $4n^2$.

18.65 Theorem [1430] There is no circulant Hadamard matrix of order $v = 4u^2$ $(4 < v < 10^{11})$ with the only possible exceptions $u \in \{11715, 82005\}$.

18.66 Remark The abelian groups for which the existence of a Hadamard difference set of order u^2 with $u < 20$ is still undecided are $\mathbb{Z}_2^2 \times \mathbb{Z}_{16} \times \mathbb{Z}_9$, $\mathbb{Z}_4 \times \mathbb{Z}_{16} \times \mathbb{Z}_9$, $\mathbb{Z}_8^2 \times \mathbb{Z}_9$, $\mathbb{Z}_4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5^2$, and $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3^2 \times \mathbb{Z}_9$.

18.7 Nonabelian Difference Sets

18.67 Remark This section includes additional results on nonabelian difference sets that are not covered in the previous sections.

18.68 Theorem Let D be a cyclic difference set with $\lambda = 1$ and $k \equiv 2 \pmod 3$. Then there exists a nonabelian difference set with the same parameters. The associated projective planes are isomorphic.

18.69 Theorem [705] Let G be an abelian group with subgroup H of index 2. Let $\hat{G}$ be the dihedral extension of H; that is, $\hat{G} = \langle H, \theta\rangle$, $\theta^2 = 1$, and for all $h \in H, \theta h\theta = h^{-1}$. Then the existence of a difference set in $\hat{G}$ forces the existence of one in G.

18.70 Corollary Let G be a group of order 2^{2d+2}. If there exists a normal subgroup K of index at least 2^{d+3} such that G/K is cyclic or dihedral, then G does not have a difference set.

18.71 Remark Corollary 18.70 gives a necessary and sufficient condition for the existence of a difference set in groups of order 64. It is an open question as to whether this is true for all 2-groups.

18.72 Theorem [1429] There are no dihedral difference sets of order $1 < n \leq 10^6$ with the only possible exception $n = 540\,225$.

18.8 Tables of Difference Sets with Small Parameters

18.73 Table Abelian difference sets of order $n \leq 30$. In this table, one difference set for each abelian group is listed. In general, there are many more examples! There are no other groups or parameters with $n \leq 30$ for which the existence of a difference set is undecided (see also Remark 18.84). In the column "group" the decomposition of the group is given as a product of cyclic subgroups. If the group is cyclic, the integers modulo the group order are used to describe the difference set.

n	v	k	λ	Group	Difference Set	Comment
2	7	3	1	(7)	1 2 4	PG(2, 2)
3	13	4	1	(13)	0 1 3 9	PG(2, 3)
3	11	5	2	(11)	1 3 4 5 9	Paley
4	21	5	1	(21)	3 6 7 12 14	PG(2, 4)
4	16	6	2	(8)(2)	(00) (10) (11) (20) (40) (61)	MF(2, 1)
				$(4)^2$	(00) (01) (10) (12) (20) (23)	MF(2, 1)
				$(4)(2)^2$	(000) (010) (100) (101) (200) (211)	MF(2, 1)
				$(2)^4$	(0000) (0010) (1000) (1001) (1100) (1111)	MF(2, 1)
4	15	7	3	(3)(5)	0 1 2 4 5 8 10	PG(3, 2)
5	31	6	1	(31)	1 5 11 24 25 27	PG(2, 5)
5	19	9	4	(19)	1 4 5 6 7 9 11 16 17	Paley
6	23	11	5	(23)	1 2 3 4 6 8 9 12 13 16 18	Paley
7	57	8	1	(3)(19)	1 6 7 9 19 38 42 49	PG(2, 7)
7	37	9	2	(37)	1 7 9 10 12 16 26 33 34	$\mathbb{F}_{37}^{(4)}$
7	27	13	6	$(3)^3$	(001) (011) (021) (111) (020) (100) (112) (120) (121) (122) (201) (202) (220)	Paley
8	73	9	1	(73)	1 2 4 8 16 32 37 55 64	PG(2, 8)
8	31	15	7	(31)	1 2 3 4 6 8 12 15 16 17 23 24 27 29 30	PG(4, 2)
9	91	10	1	(7)(13)	0 1 3 9 27 49 56 61 77 81	PG(2, 9)
9	45	12	3	$(3)^2(5)$	(000) (001) (002) (003) (010) (020) (101) (112) (123) (201) (213) (222)	MF(3, 1)
9	40	13	4	(8)(5)	1 2 3 5 6 9 14 15 18 20 25 27 35	PG(3, 3)
9	36	15	6	$(4)(3)^2$	(010) (011) (012) (020) (021) (022) (100) (110) (120) (200) (211) (222) (300) (312) (321)	Sp(1)
				$(2)^2(3)^2$	(0010) (0011) (0012) (0020) (0021) (0022) (0100) (0110) (0120) (1000) (1011) (1022) (1100) (1112) (1121)	Sp(1)
9	35	17	8	(5)(7)	0 1 3 4 7 9 11 12 13 14 16 17 21 27 28 29 33	TPP(5)
11	133	12	1	(7)(19)	1 11 16 40 41 43 52 60 74 78 121 128	PG(2, 11)
11	43	21	10	(43)	1 4 6 9 10 11 13 14 15 16 17 21 23 24 25 31 35 36 38 40 41	Paley
12	47	23	11	(47)	1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42	Paley
13	183	14	1	(3)(61)	0 2 3 10 26 39 43 61 109 121 130 136 141 155	PG(2, 13)
15	59	29	14	(59)	1 3 4 5 7 9 12 15 16 17 19 20 21 22 25 26 27 28 29 35 36 41 45 46 48 49 51 53 57	Paley
16	273	17	1	(3)(7)(13)	1 2 4 8 16 32 64 91 117 128 137 182 195 205 234 239 256	PG(2, 16)

n	v	k	λ	Group	Difference Set	Comment
16	96	20	4	$(2)(4)^2(3)$	(0000) (0001) (0002) (0020) (0101) (0031) (0132) (0200) (0212) (0220) (0111) (0302) (1012) (1101) (1132) (1201) (1211) (1222) (1131) (1322)	[112]
				$(2)^3(4)(3)$	(00001) (00002) (00010) (00011) (00012) (00021) (00101) (00121) (01002) (01030) (01131) (01112) (10002) (10031) (10110) (10132) (11002) (11032) (11130) (11111)	MF$(4,1)$
				$(2)^5(3)$	(000001) (000002) (000010) (000011) (000012) (000101) (001001) (001101) (010002) (010110) (011012) (011111) (100002) (100111) (101010) (101112) (110002) (110112) (111011) (111110)	MF$(4,1)$
16	85	21	5	(5)(17)	0 1 2 4 7 8 14 16 17 23 27 28 32 34 43 46 51 54 56 64 68	PG$(3,4)$
16	64	28	12	(4)(16)	(0 9) (0 11) (0 13) (0 15) (1 4) (1 5) (1 6) (1 9) (1 11) (1 12) (1 14) (1 15) (2 2) (2 3) (2 6) (2 7) (2 9) (2 10) (2 13) (2 14) (3 2) (3 3) (3 4) (3 5) (3 7) (3 9) (3 10) (3 12)	18.57
				$(2)^2(16)$	(0 0 1) (0 0 2) (0 0 3) (0 0 4) (0 0 5) (0 0 6) (0 0 7) (0 0 10) (0 0 12) (0 0 14) (0 1 1) (0 1 4) (0 1 5) (0 1 11) (0 1 12) (0 1 15) (1 0 1) (1 0 2) (1 0 3) (1 0 10) (1 0 13) (1 0 15) (1 1 1) (1 1 6) (1 1 7) (1 1 11) (1 1 13) (1 1 14)	MF$(2,2)$
				$(8)^2$	(14) (15) (16) (17) (22) (23) (26) (27) (32) (34) (35) (37) (41) (43) (45) (47) (51) (53) (54) (56) (61) (62) (65) (66) (71) (72) (73) (74)	18.57
				$(2)^3(8)$	(0001) (0002) (0003) (0004) (0005) (0006) (0007) (0012) (0014) (0016) (0101) (0104) (0105) (0113) (0114) (0117) (1001) (1002) (1003) (1012) (1015) (1017) (1101) (1106) (1107) (1113) (1115) (1116)	MF$(2,2)$
				$(4)^3$	(001) (010) (011) (012) (021) (033) (100) (101) (102) (110) (111) (112) (120) (121) (122) (133) (201) (210) (211) (212) (221) (233) (303) (313) (323) (330) (331) (332)	MF$(2,2)$
				$(2)^2(4)^2$	(0001) (0002) (0003) (0010) (0011) (0012) (0013) (0021) (0022) (0023) (0102) (0110) (0112) (0122) (0131) (0133) (1001) (1010) (1011) (1021) (1032) (1033) (1103) (1110) (1113) (1123) (1131) (1132)	MF$(2,2)$
				$(2)^4(4)$	(00001) (00002) (00003) (00010) (00011) (00012) (00013) (00101) (00102) (00103) (01002) (01010) (01012) (01102) (01111) (01113) (10001) (10010) (10011) (10101) (10112) (10113) (11003) (11010) (11013) (11103) (11111) (11112)	MF$(2,2)$

n	v	k	λ	Group	Difference Set	Comment
16	64	28	12	$(2)^6$	(000001) (000010) (000011) (000100) (000101) (000110) (000111) (001010) (001100) (001110) (010001) (010100) (010101) (011011) (011100) (011111) (100001) (100010) (100011) (101010) (101101) (101111) (110001) (110110) (110111) (111011) (111101) (111110)	MF(2, 2)
16	63	31	15	(9)(7)	0 1 2 3 4 6 7 8 9 12 13 14 16 18 19 24 26 27 28 32 33 35 36 38 41 45 48 49 52 54 56	PG(5, 2)
				$(3)^2(7)$	(000) (001) (002) (003) (004) (005) (006) (011) (012) (014) (021) (022) (024) (103) (105) (106) (113) (115) (116) (121) (122) (124) (203) (205) (206) (211) (212) (214) (223) (225) (226)	TPP(7)
17	307	18	1	(307)	0 1 3 30 37 50 55 76 98 117 129 133 157 189 199 222 293 299	PG(2, 17)
17	67	33	16	(67)	1 4 6 9 10 14 15 16 17 19 21 22 23 24 25 26 29 33 35 36 37 39 40 47 49 54 55 56 59 60 62 64 65	Paley
18	71	35	17	(71)	1 2 3 4 5 6 8 9 10 12 15 16 18 19 20 24 25 27 29 30 32 36 37 38 40 43 45 48 49 50 54 57 58 60 64	Paley
19	381	20	1	(3)(127)	0 1 19 28 96 118 151 153 176 202 240 254 290 296 300 307 337 361 366 369	PG(2, 19)
19	101	25	6	(101)	1 5 16 19 24 25 31 36 37 52 54 56 58 68 71 78 79 80 81 84 87 88 92 95 97	$\mathbb{F}_{101}^{(4)}$
20	79	39	19	(79)	1 2 4 5 8 9 10 11 13 16 18 19 20 21 22 23 25 26 31 32 36 38 40 42 44 45 46 49 50 51 52 55 62 64 65 67 72 73 76	Paley
21	109	28	7	(109)	0 1 3 5 7 9 15 16 21 22 25 26 27 35 38 45 48 49 63 66 73 75 78 80 81 89 97 105	$\mathbb{F}_{109}^{(4)}$
21	83	41	20	(83)	1 3 4 7 9 10 11 12 16 17 21 23 25 26 27 28 29 30 31 33 36 37 38 40 41 44 48 49 51 59 61 63 64 65 68 69 70 75 77 78 81	Paley
23	553	24	1	(7)(79)	1 23 52 90 108 120 152 163 173 178 186 223 232 272 359 407 411 431 438 512 513 515 529 548	PG(2, 23)
25	651	26	1	(3)(7)(31)	1 5 25 42 71 107 125 201 210 217 354 355 357 387 399 412 434 462 468 473 483 521 535 561 625 633	PG(2, 25)
25	175	30	5	$(5)^2(7)$	(001) (002) (003) (004) (005) (006) (011) (021) (031) (041) (106) (112) (124) (133) (145) (206) (213) (222) (235) (244) (306) (314) (325) (332) (343) (406) (415) (423) (434) (442)	MF(5, 1)
25	156	31	6	(4)(3)(13)	0 1 5 11 13 25 28 39 46 55 58 65 68 74 76 86 87 91 111 117 118 119 122 123 125 127 134 140 142 143 147	PG(3, 5)

n	v	k	λ	Group	Difference Set	Comment
25	133	33	8	(7)(19)	1 4 5 14 16 19 20 21 25 38 54 56 57 64 66 70 76 80 83 84 91 93 95 98 100 101 105 106 114 123 125 126 131	
25	99	49	24	$(3)^2(11)$	(0 0 0) (0 1 0) (0 1 1) (0 1 3) (0 1 4) (0 1 5) (0 1 9) (0 2 0) (0 2 1) (0 2 3) (0 2 4) (0 2 5) (0 2 9) (1 0 0) (1 0 2) (1 0 6) (1 0 7) (1 0 8) (1 0 10) (1 1 0) (1 1 2) (1 1 6) (1 1 7) (1 1 8) (1 1 10) (1 2 0) (1 2 1) (1 2 3) (1 2 4) (1 2 5) (1 2 9) (2 0 0) (2 0 2) (2 0 6) (2 0 7) (2 0 8) (2 0 10) (2 1 0) (2 1 1) (2 1 3) (2 1 4) (2 1 5) (2 1 9) (2 2 0) (2 2 2) (2 2 6) (2 2 7) (2 2 8) (2 2 10)	TPP(9)
26	103	51	25	(103)	1 2 4 7 8 9 13 14 15 16 17 18 19 23 25 26 28 29 30 32 33 34 36 38 41 46 49 50 52 55 56 58 59 60 61 63 64 66 68 72 76 79 81 82 83 91 92 93 97 98 100	Paley
27	757	28	1	(757)	0 1 3 9 27 43 81 129 173 220 243 310 387 404 409 445 455 466 470 505 519 578 608 641 653 660 673 729	PG$(2, 27)$
27	121	40	13	(121)	1 3 4 7 9 11 12 13 21 25 27 33 34 36 39 44 55 63 64 67 68 70 71 75 80 81 82 83 85 89 92 99 102 103 104 108 109 115 117 119	PG$(4, 3)$
27	107	53	26	(107)	1 3 4 9 10 11 12 13 14 16 19 23 25 27 29 30 33 34 35 36 37 39 40 41 42 44 47 48 49 52 53 56 57 61 62 64 69 75 76 79 81 83 85 86 87 89 90 92 99 100 101 102 105	Paley
29	871	30	1	(13)(67)	1 24 29 69 151 167 216 234 259 263 295 321 329 414 488 543 582 599 645 659 683 689 696 716 731 819 820 822 831 841	PG$(2, 29)$

18.74 Remark Table 18.73 does not contain inequivalent difference sets. In general, it is not known how many inequivalent difference sets exist. The next tables list all difference sets (up to equivalence) with $k < 20$. The cases $(16, 6, 2; 4)$ and $(36, 15, 6; 9)$ are treated in Tables 18.77 and 18.78.

18.75 Table (Kibler [1295]) Difference sets with parameters (v, k, λ), $k < 20$, $(v, k, \lambda) \neq (16, 6, 2), (36, 15, 6)$ that are not already covered by Table 18.73.

parameters	group
$(21, 5, 1)$	$a^7 = b^3 = 1,\ ba = a^2b$
	$a + a^2 + b + a^4 + b^2$
$(57, 8, 1)$	$a^{19} = b^3 = 1, a^7b = ba$
	$(1 + a + a^3 + a^8) + (1 + a^4 + a^{13})b + a^{18}b^2$
	$(1 + a + a^3 + a^8) + b + (a^5 + a^9 + a^{18})b^2$
$(45, 12, 3)$	$a^{15} = b^3 = 1$, abelian
	$1 + a^2 + a^3 + a^4 + a^7 + a^{12} + (1 + a^8 + a^{14})b + (1 + a^9 + a^{13})b^2$
$(40, 13, 4)$	$a^5 = b^8 = a^4ba^{-1}b^{-1} = 1$
	$(1 + a + a^2) + (1 + a^3)b + (a + a^3 + a^4)b^2 + ab^4 + (a + a^2)b^5 + ab^6 + a^4b^7$
$(27, 13, 6)$	$a^9 = b^3 = a^4ba^{-1}b^{-1} = 1$
	$(1 + a + a^2 + a^4 + a^5 + a^7) + (1 + a + a^2 + a^5)b + (a^5 + a^6 + a^8)b^2$
	$(1 + a + a^2 + a^4 + a^5 + a^7) + (1 + a^5 + a^8)b + (a^2 + a^4 + a^5 + a^6)b^2$

parameters group
$(183, 14, 1)$ $a^{61} = b^3 = a^{13}ba^{-1}b^{-1} = 1$
$(1 + a + a^3 + a^{20} + a^{26} + a^{48} + a^{57}) + (1 + a^8 + a^{18} + a^{29})b + (a^{17} + a^{32} + a^{44})b^2$
$(1 + a + a^3 + a^{20} + a^{26} + a^{48} + a^{57}) + (1 + a^{12} + a^{46})b + (a^9 + a^{17} + a^{27} + a^{38})b^2$
$(31, 15, 7)$ $a^{31} = 1$, abelian
$a + a^2 + a^4 + a^5 + a^7 + a^8 + a^9 + a^{10} + a^{14} + a^{16} + a^{18} + a^{19} + a^{20} + a^{25} + a^{28}$
$(273, 17, 1)$ $a^{13} = b^7 = c^3 = a^3ca^{-1}b^{-1} = b^2cb^{-1}c^{-1} = aba^{-1}b^{-1} = 1$
$(a + b + a^2b + a^4b^2 + a^{11}b^2 + a^5b^4 + a^{10}b^4$
$+(a^4 + a^9b + a^{12}b + a^2b^2 + a^6b^2 + a^{10}b^4)c + (b^3 + b^5 + b^6)c^2$
$(273, 17, 1)$ $a^{13} = b^7 = c^3 = a^{12}ca^{-1}b^{-1} = b^2cb^{-1}c^{-1} = aba^{-1}b^{-1} = 1$
$(a + b + a^2b + a^4b^2 + a^{11}b^2 + a^5b^4 + a^{10}b^4$
$+(a^4 + a^9b + a^{12}b + a^2b^2 + a^6b^2 + a^{10}b^4)c + (b^3 + b^5 + b^6)c^2$

18.76 Remarks In Table 18.75, the designs corresponding to difference sets with $\lambda = 1$ are isomorphic.

18.77 Table (Kibler [1295]) (16,6,2) difference sets. There are 14 groups of order 16. The cyclic and dihedral groups do not have difference sets. The four noncyclic abelian groups have a total of eight difference sets (cases D_1 to D_8). The set D_8 in the elementary abelian group of order 16 gives a $(16, 6, 2)$ design with a very large automorphism group. The nonabelian difference sets all give a design isomorphic to that one except for D_{11} and D_{14}. These give isomorphic $(16, 6, 2)$ designs that are not isomorphic to the other. The third $(16, 6, 2)$ design can be obtained from the abelian difference set D_1 (see [1295]). All 27 difference sets are listed in [1295]. The three designs are given in Table II.1.32.

$G = \langle a, b : a^8 = b^2 = [a, b] = 1\rangle$.
$D_1 = 1 + a + a^2 + a^4 + ab + a^6b$ $D_2 = 1 + a + a^2 + a^5 + b + a^6b$
$G = \langle a, b : a^4 = b^4 = [a, b] = 1\rangle$.
$D_3 = 1 + a + a^2 + b + ab^2 + a^2b^3$ $D_4 = 1 + a + a^2 + b + b^3 + a^3b^2$
$D_5 = 1 + a + b + a^2b + ab^2 + a^2b^2$
$G = \langle a, b, c : a^4 = b^2 = c^2 = [a, b] = [a, c] = [b, c] = 1\rangle$.
$D_6 = 1 + a + a^2 + b + c + a^3bc$ $D_7 = 1 + a + a^2 + ab + ac + a^3bc$
$G = \langle a, b, c, d : a^2 = b^2 = c^2 = d^2 = [a, b] = [a, c] = [a, d] = [b, c] = [b, d] = [c, d] = 1\rangle$.
$D_8 = 1 + a + b + c + d + abcd$
$G = \langle a, b, c : a^4 = b^2 = c^2 = baba = [a, c] = [b, c] = 1\rangle$.
$D_9 = 1 + a + a^2 + b + ac + a^2bc$ $D_{10} = 1 + a + b + a^2b + c + a^3c$
$G = \langle a, b, c : a^4 = c^2 = b^2a^2 = a^3ba^{-1}b^{-1} = [a, c] = [b, c] = 1\rangle$.
$D_{11} = 1 + a + a^2 + b + c + abc$ $D_{12} = 1 + a + a^2 + b + ac + a^2bc$
$G = \langle a, b, c : a^4 = c^4 = b^4 = a^2b^2 = b^2c^2 = a^3ba^{-1}b^{-1} = [a, c] = [b, c] = 1\rangle$.
$D_{13} = 1 + a + a^2 + b + ac + bc$ $D_{14} = 1 + a + b + ab + c + a^2c$
$G = \langle a, b, c : a^4 = b^2 = bc^2 = a^3bca^{-1}c^{-1} = [a, b] = 1\rangle$.
$D_{15} = 1 + a + a^2 + ab + c + a^2bc$ $D_{16} = 1 + a + a^2 + ab + ac + a^3bc$
$D_{17} = 1 + a + b + a^3b + ac + a^3c$ $D_{18} = 1 + a + a^2 + a^3b + ac + abc$
$G = \langle a, b : a^4 = b^4 = a^3ba^{-1}b^{-1} = 1\rangle$.
$D_{19} = 1 + a + a^2 + b + ab^2 + a^2b^3$ $D_{20} = 1 + a + a^2 + b + b^3 + a^3b^2$
$D_{21} = 1 + a + b + a^2b + b^2 + a^3b^2$
$G = \langle a, b : a^8 = b^2 = a^5ba^{-1}b^{-1} = 1\rangle$.
$D_{22} = 1 + a + a^2 + a^5 + a^4b + a^2b$ $D_{23} = 1 + a + a^3 + a^4 + a^3b + a^5b$
$G = \langle a, b : a^8 = b^4 = a^4b^2 = a^3ba^{-1}b^{-1} = 1\rangle$.
$D_{24} = 1 + a + a^2 + a^5 + b + a^2b$ $D_{25} = 1 + a + a^3 + a^4 + ab + a^3b$
$G = \langle a, b : a^8 = b^4 = a^4b^2 = a^7ba^{-1}b^{-1} = 1\rangle$.
$D_{26} = 1 + a + a^2 + a^5 + b + a^2b$ $D_{27} = 1 + a + a^3 + a^4 + b + a^2b$

18.78 Table (Kibler [1295]) (36,15,6) difference sets. There are 14 groups of order 36. Five do not have difference sets. Two abelian groups have seven difference sets giving seven nonisomorphic designs. Seven nonabelian groups have 28 difference sets but 26 of these arise as automorphism groups of the seven designs constructible by abelian groups. (These seven designs occur as follows. There are three designs with 3-rank equal to 12, given by the families of difference sets from the table: $\{D_5, D_8, D_{17}, D_{20}, D_{34}\}$, $\{D_6, D_{18}\}$, $\{D_7, D_{19}, D_{33}\}$. There are four designs with 3-rank equal to 14, given by the four families: $\{D_3, D_{12}, D_{24}, D_{32}, D_{35}\}$, $\{D_1, D_{13}, D_{21}, D_{25}, D_{27}, D_{29}\}$, $\{D_2, D_{14}\}$, $\{D_4, D_{11}, D_{15}, D_{16}, D_{22}, D_{23}, D_{26}, D_{28}, D_{30}, D_{31}\}$.) Two difference sets ($D_9$ and D_{10}) are genuinely nonabelian; the designs constucted from D_9 and D_{10} are dual to each other and have 3-rank 16. All 35 difference sets are given. (D_{35} does not occur in Kibler's work.)

$G = \langle a^3 = b^3 = c^4 = [a,b] = [a,c] = [b,c] = 1\rangle$ (abelian)

$D_1 = (1+a+a^2)(1+b) + (1+b+b^2)c + (1+ab+a^2b^2)c^2 + (1+a^2b+ab^2)c^3$

$D_2 = (1+a+a^2)(1+b) + (1+b+b^2)c + (1+ab+a^2b^2)c^2 + (a+b+a^2b^2)c^3$

$D_3 = (1+a+a^2)(1+b) + (1+b+b^2)c + (1+ab+a^2b^2)c^2 + (a^2+ab+b^2)c^3$

$D_4 = (1+a+a^2)(1+b) + (1+b+b^2)c + (a+a^2b+b^2)c^2 + (a^2+ab+b^2)c^3$

$G = \langle a,b,c : a^3 = b^3 = c^4 = [a,b] = [a,c] = b^2cb^{-1}c^{-1} = 1\rangle$.

$D_5 = (1+a+a^2)+(1+a+a^2)b+(1+ab+a^2b^2)c+(1+b+b^2)c^2+(1+a^2b+ab^2)c^3$

$D_6 = (1+a+a^2)+(1+a+a^2)b+(1+ab+a^2b^2)c+(1+b+b^2)c^2+a(1+a^2b+ab^2)c^3$

$D_7 = (1+a+b)+(ab+b^2+ab^2)+(1+ab+a^2b^2)c+(1+a+a^2)c^2+(1+a^2b+ab^2)c^3$

$D_8 = (1+a+b)+(ab+b^2+ab^2)+(1+ab+a^2b^2)c+(1+a+a^2)c^2+a(1+a^2b+ab^2)c^3$

$G = \langle a,b,c : a^3 = b^3 = c^4 = [a,b] = [a,c] = b^2cb^{-1}c^{-1} = 1\rangle$.

$D_9 = (1+a+b)+(a+b+ab)ab+(1+a+a^2)c+(1+ab+a^2b^2)c^2+(1+b+b^2)c^3$

$D_{10} = (1+a+b)+(a+b+ab)ab+(1+a+a^2)c+(1+ab+a^2b^2)c^2+(1+b+b^2)ac^3$

$G = \langle a,b,c : a^3 = b^3 = c^4 = [a,b] = a^2ca^{-1}c^{-1} = b^2cb^{-1}c^{-1} = 1\rangle$.

$D_{11} = (1+a+a^2)+(1+a+a^2)b+(a^2+b+ab^2)c+(1+b+b^2)c^2+(1+a^2b+ab^2)c^3$

$G = \langle a,b,c : a^3 = b^3 = c^4 = [a,b] = bca^{-1}c^{-1} = a^2cb^{-1}c^{-1} = 1\rangle$.

$D_{12} = (1+a+a^2)+(1+a+a^2)b+(a^2+b+ab^2)c+(1+b+b^2)c^2+(1+a^2b+ab^2)c^3$

$D_{13} = (1+a+a^2)+(1+a+a^2)b+(a^2+b+ab^2)c+(1+b+b^2)c^2+a(1+a^2b+ab^2)c^3$

$D_{14} = (1+a+a^2)+(1+a+a^2)b+(a^2+b+ab^2)c+(1+b+b^2)c^2+a^2(1+a^2b+ab^2)c^3$

$D_{15} = (1+a+a^2)+(1+a+a^2)b+(a^2+b+ab^2)c+a(1+b+b^2)c^2+(1+a^2b+ab^2)c^3$

$D_{16} = (1+a+a^2)+(1+a+a^2)b+(a^2+ab+b^2)c+(1+b+b^2)c^2+(1+ab+a^2b^2)c^3$

$G = \langle a^3 = b^3 = c^2 = d^2 = [a,b] = [c,d] = [a,c] = [a,d] = [b,c] = [b,d] = 1\rangle$ (abelian)

$D_{17} = (1+a+a^2)+(1+a^2+b+a^2b+b^2+a^2b^2)c+(a+a^2b+b^2)d+(a+b+a^2b^2)cd$

$D_{18} = (1+a+a^2)+(1+a^2+b+a^2b+b^2+a^2b^2)c+(a^2+ab+b^2)d+(1+ab+a^2b^2)cd$

$D_{19} = (1+a+a^2)+(1+a^2+ab+a^2b+b^2+ab^2)c+(1+b+b^2)d+(1+ab+a^2b^2)cd$

$G = \langle a,b,c,d : a^3 = b^3 = c^2 = d^2 = [a,b] = [c,d] = [a,d] = [b,d] = 1, a^2c = ca, b^2c = cb\rangle$.

$D_{20} = (1+a+a^2)+(1+a+a^2)b+(1+b+b^2)c+(1+ab+a^2b^2)d+(1+a^2b+ab^2)cd$

$G = \langle a,b,c,d : a^3 = b^3 = c^2 = d^2 = [a,b] = [c,d] = [a,d] = [b,c] = [b,d] = a^2ca^{-1}c^{-1} = 1\rangle$.

$D_{21} = (1+a+a^2)+(1+a+a^2)b+(1+ab+a^2b^2)c+(1+b+b^2)d+(1+a^2b+ab^2)cd$

$D_{22} = (1+a+a^2)+(1+a+a^2)b+(1+ab+a^2b^2)c+(1+b+b^2)d+a(1+a^2b+ab^2)cd$

$D_{23} = (1+a+b)+(ab+b^2+ab^2)+(1+ab+a^2b^2)c+(1+a+a^2)d+(1+a^2b+ab^2)cd$

$D_{24} = (1+a+b)+(ab+b^2+ab^2)+(1+ab+a^2b^2)c+(1+a+a^2)d+a(1+a^2b+ab^2)cd$

$D_{25} = (1+a+b)+a(ab+b^2+ab^2)+(1+a+a^2)c+(1+ab+a^2b^2)d+(1+b+b^2)cd$

$D_{26} = (1+a+b)+a(ab+b^2+ab^2)+(1+a+a^2)c+a^2(1+ab+a^2b^2)d+(1+b+b^2)cd$

$G = \langle a,b,c,d : a^3 = b^3 = c^2 = d^2 = [a,b] = [c,d] = [a,d] = [b,c] = 1, b^2d = db, a^2c = ca\rangle$.

$D_{27} = (1+a+a^2)+(b+ab+a^2b)+(c+abc+a^2b^2c)+(d+a^2bd+ab^2d)+(cd+bcd+b^2cd)$

$D_{28} = (1+a+a^2)+(1+a+a^2)b+(1+ab+a^2b^2)c+(1+a^2b+ab^2)d+a^2(1+b+b^2)cd$

$D_{29} = (1+a+b)+(a^2b+ab^2+a^2b^2)+(c+ac+a^2c)+(d+bd+b^2d)+(cd+abcd+a^2b^2cd)$

$D_{30} = (1+a+b)+(a^2b+ab^2+a^2b^2)+(1+a+a^2)c+a^2(1+b+b^2)d+(1+ab+a^2b^2)cd$
$D_{31} = (1+a+b)+(a^2b+ab^2+a^2b^2)+(1+b+b^2)c+(1+a+a^2)d+(1+ab+a^2b^2)cd$
$D_{32} = (1+a+b)+(a^2b+ab^2+a^2b^2)+(1+b+b^2)c+(1+a+a^2)d+a(1+ab+a^2b^2)cd$
$G = \langle a, b, c, d : a^3 = b^3 = c^2 = d^2 = [a, b] = [c, d] = [b, c] = [d, b] = 1, da = ac, cda = ad\rangle$.
$D_{33} = (1+c+d+cd+a+ca+da^2)+(c+ca+cda+cda^2)b+(c+ca+da+a^2)b^2$
$D_{34} = (1+c+d+cda+a+ca^2+cda^2)+(a+da+ca^2+da^2)b+(a+ca+ca^2+a^2)b^2$
$D_{35} = 1+a+b+d+c+a^2+ac+b^2+abd+abc+a^2bc+ab^2c+abdc+b^2dc+a^2bdc$

18.79 Remarks

1. The multipliers of the difference sets with $k < 20$ are also known, see [1295].
2. Tables 18.75, 18.77, and 18.78 contain all difference sets, up to equivalence, with $k < 20$.
3. There are over 2500 inequivalent $(96, 20, 4)$ difference sets in 94 groups.

18.80 Table A complete list (up to equivalence) of cyclic $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$-difference sets with $m \leq 9$ (see Table 18.81 for the case $m = 10$). All of these difference sets are fixed by the multiplier 2; see Theorem 18.12. The table contains only one representative from each orbit under the multiplier group generated by the multiplier 2; the first difference set is $\{1, 2 \cdot 1, 2^2 \cdot 1\}$. The difference sets in this table describe nonisomorphic designs. In most cases, this can be seen by the different ranks over $\mathbb{F}_2$ of the corresponding incidence matrices. If the ranks coincide, one may consider the intersection numbers of three or four blocks of *dev(D)*. (See [167, 132].)

m	Difference Set	$\mathbb{F}_2$-rank	Comment
3	1	4	Singer
4	0 1 5	5	Singer
5	1 3 15	6	Singer
	1 5 7	16	Paley
6	0 1 3 7 9 13 27	7	Singer
	0 1 3 5 9 23 27	13	GMW(2,6,3,-1)
7	1 3 7 9 15 27 29 31 47	8	Singer
	1 9 11 13 15 19 21 31 47	64	Paley
	1 3 5 7 19 23 27 47 63	22	Hall
	1 3 7 9 13 19 27 31 47	36	DD(7,2)
	1 3 5 9 15 19 27 29 55	36	NCY(7)
	1 3 5 11 19 21 27 29 63	22	DD(7,3)
8	0 1 3 7 13 17 19 23 25 27 31 37 45 51 59 85 111 119 127	9	Singer
	0 7 11 13 17 19 23 27 39 43 47 51 53 55 63 85 95 111 119	33	GMW(2,8,4,-1)
	0 1 3 7 13 15 17 25 29 37 39 43 47 51 53 61 63 85 119	41	DD(8,3)
	0 7 9 11 15 17 19 25 29 31 37 43 51 53 61 63 85 87 119	41	NCY(8)
9	1 7 13 17 21 23 31 35 37 39 51 53 55 59 61 75 77 79 83 85 91 95 103 109 123 183 187 219 223	10	Singer
	1 5 23 27 29 31 37 39 41 47 55 59 63 75 77 79 85 87 95 109 117 123 171 175 183 191 219 223 255	28	GMW(2,9,3,-1)
	1 3 5 7 13 15 19 21 23 25 27 37 39 45 55 57 59 63 77 83 91 107 117 123 183 191 219 239 255	64	hyperoval

m	Difference Set	$\mathbb{F}_2$-rank	Comment
9	1 3 5 7 9 11 17 29 31 43 53 55 57 61 63 75 77 91 95 109 117 123 125 171 175 183 219 239 255	28	DD(9,4)
	1 7 9 11 25 27 31 35 37 39 47 53 55 61 77 83 85 87 107 109 111 119 171 175 183 187 191 219 223	82	DD(9,2)

18.81 Table Difference sets with parameters $(1023, 511, 255)$. Let D be a difference set with the Singer parameters $[2, m]$ and multiplier 2. Let α be a primitive element in $\mathbb{F}_{2^m}$. Then there is a subset T of integers $0 \le t < 2^m - 1$ such that $D = \{0 \le i < 2^m - 1 : \sum_{t\in T} \mathrm{trace}(\alpha^{it}) = 0\}$ for any primitive element α in $\mathbb{F}_{2^m}$. In [849], all cyclic difference sets with the classical parameters $[2, 10]$ have been determined. The set T (a more condensed way to describe the difference set) is given.

No.	T	$\mathbb{F}_2$-rank	Comment
1.	1	11	Singer
2.	1 219	21	GMW
3.	1 63	21	GMW
4.	1 39 157 221	41	GMW
5.	1 101 159 187	41	GMW
6.	1 39 47 95 101 159 171 187	81	GMW
7.	1 5 7 9 19 25 69	71	GMW with Paley
8.	1 5 25 45 69 87 101 107 121 159 187 237 245 479	141	GMW with Paley
9.	1 9 57 73 121	51	DD(9,3)
10.	1 10 11 12 13 14 15 138 139 140 141 142 143	131	NCY(10)

18.82 Table Cyclic difference sets with $\lambda = 1$ of prime power order n (cyclic $(n^2+n+1, n+1, 1)$ difference sets) for $31 \le n \le 97$. From each orbit under the multilier n, only one element is listed. For example, the element 220 in the first row represents the elements $220, 31 \cdot 220, 31^2 \cdot 220$ modulo $31^2 + 31 + 1$, the elements $220, 862, 904$.

n	Difference Set
31	1 98 220 280 331 360 491 662 738 748 939 945
37	1 144 157 159 469 566 609 635 805 898 938 1046 1279 1298
41	1 152 271 345 421 638 672 761 879 897 1011 1207 1542 1612
43	1 79 214 414 474 482 562 606 631 875 896 1215 1262 1747 1757 1831
47	1 199 269 389 669 806 1125 1258 1380 1441 1647 1698 1707 1718 1906 2055
53	1 148 209 271 645 826 899 907 1075 1085 1176 1444 1807 2054 2067 2519 2681 2731
59	1 135 373 820 938 1421 1530 1701 1919 2187 2312 2342 2471 2477 2728 2827 3198 3236 3302 3459
61	1 279 401 415 980 1066 1261 1707 1790 1949 2087 2205 2522 2544 2562 2579 2594 2704 3310 3582 3653 3657
67	1 18 29 269 421 529 551 646 685 1519 1790 2199 2415 2668 2676 2931 3038 3315 3577 3623 3671 3814 4111 4377
71	1 222 499 510 829 1502 1732 1885 1901 1906 2143 2580 2856 2869 3325 3635 3714 3845 3989 4162 4268 4719 4921 4930
73	1 186 979 985 1291 1801 2076 2093 2271 2303 2535 2728 2852 3149 3297 3336 3371 3464 3480 3491 3602 4084 4148 4466 5067 5397
79	1 13 335 359 808 1309 1419 1613 1943 2107 2517 2596 2694 2754 2768 2944 3140 3404 3475 3675 3783 3961 4127 4178 4214 5084 5400 6016
83	1 502 690 786 796 1275 1431 1891 1989 2424 2706 2839 4129 4283 4446 4578 4591 4592 4768 5190 5215 5385 5665 5809 5878 6146 6280 6452

n	Difference Set
89	1 390 693 1261 1355 2372 2564 2833 3024 3194 3374 3464 3472 3624 3661 3811 4163 4484 5073 5079 5402 5570 5711 5732 5841 6949 7085 7405 7425 7863
97	1 657 670 1070 1071 1073 1107 1378 1402 1984 2225 2748 2793 3000 3169 3186 3211 4257 4536 4745 5588 6124 6246 6338 6566 6596 7221 7609 7829 7848 8091 8233 9098 9374

18.83 Table Baumert's cyclic difference sets with $k \leq 100$. Baumert [167] listed all known cyclic difference sets with $k \leq 100$. The following examples are in his table but are not covered by Table 18.73 or 18.80. As in Table 18.80, only one representative from each orbit under the multiplier group is listed. The three $(121, 40, 13)$-difference sets are not isomorphic. They may be distinguished by the $\mathbb{F}_3$-ranks of the incidence matrices. The rank of the classical Singer difference set with this parameters is 16.

n	v	k	λ		Multipliers	Comment
11	43	21	10	1 2 3	$\langle x \to 4x \rangle$	H(43), see 18.48
27	121	40	13	2 5 10 13 71 72 76 91	$\langle x \to 3x \rangle$	18.37, $\mathbb{F}_3$-rank 41
27	121	40	13	2 10 11 17 68 71 72 78	$\langle x \to 3x \rangle$	$\mathbb{F}_3$-rank 31
27	121	40	13	2 5 19 67 68 69 72 73	$\langle x \to 3x \rangle$	$\mathbb{F}_3$-rank 26
36	143	71	35	0 1 13	$\langle x \to 2x \rangle$	TPP(11), see 18.49
37	197	49	12	1	$\langle x \to 16x \rangle$	biquadratic residues

18.84 Remark Existence status for abelian difference sets with $k \leq 100$. For all abelian groups of order v, it is known whether they may contain $(v, k, \lambda; n)$-difference sets. In the first edition of this book, several cases were still open. In addition to the references in [225], refer to the papers [110, 1162, 1492, 1849] for new nonexistence results, and to [108] for a new existence result. In particular, there are no open cases in the range of the tables of Kopilovich [1323] and of Lander [1397].

See Also

§II.6	Every difference set yields a symmetric design (Theorem 18.6).
§V.1	Some difference sets yield Hadamard designs; see §18.6.
§VI.16	Difference families are a generalization of difference sets.
§VII.1	The code generated by *dev(D)* is an ideal in a group algebra.
§VII.8	The quadratic residues can be difference sets. Primitive polynomials can be used to construct Singer difference sets (18.29)
§VII.2	Singer difference sets correspond to classical geometries and the cyclic property of the designs can be used to construct ovals, arcs, and the like.
[225]	Contains most of the material used here (nonexistence and existence results).
[1397]	Develops the classical nonexistence theory nicely.
[1851]	Explains the field descent method, the most powerful technique to prove nonexistence of difference sets.
[2173]	Survey containing many new theorems on difference sets.
[168, 1481]	Contain more tables about the parameters of putative abelian difference sets, including some small open cases, see also Theorems 18.53 and 18.65 and Remark 18.66.

References Cited: [52,108,109,110,111,112,132,167,168,225,637,705,706,707,733,849,1090,1161, 1162,1261,1295,1323,1397,1428,1429,1430,1481,1492,1532,1565,1849,1851,1931,2173]

19 Difference Triangle Sets

James B. Shearer

19.1 Definition and Example

19.1 An (n,k)-*difference triangle set*, or (n,k)-DΔS, is a set $\mathcal{X} = \{X_1, \ldots, X_n\}$, where for $1 \le i \le n$, $X_i = \{a_{i0}, a_{i1}, \ldots, a_{ik}\}$, with a_{ij} an integer, and the differences

$$a_{i\ell} - a_{ij} : 1 \le i \le n,\ 0 \le j \ne \ell \le k$$

are all distinct and nonzero. It is *normalized* if, for every $1 \le i \le n$,

$$0 = a_{i0} < a_{i1} < \cdots < a_{ik}.$$

19.2 **Example** A $(3,3)$-DΔS. $\{\{0,3,15,19\},\{0,6,11,13\},\{0,8,17,18\}\}$.

19.3 **Remark** The "difference triangle" nomenclature arises from writing the differences obtained in triangular format: From Example 19.2 one obtains,

3			12			4			6			5			2			8			9			1
		15			16					11			7					17			10		
				19								13								18			

19.4 The *scope* of a (normalized) (n,k)-DΔS $\mathcal{X} = \{X_1, \ldots, X_n\}$ is

$$m(\mathcal{X}) = \max(\max(x \ :\ x \in X_i) \ :\ X_i \in \mathcal{X}).$$

Then m_{nk} denotes $\min(m(\mathcal{X}) :\ \mathcal{X}$ is a (n,k)-DΔS$)$.

19.5 **Example** The scope of the $(3,3)$-DΔS in Example 19.2 is 19.

19.6 **Remark** Difference triangle sets have applications in the construction of error correcting codes, in the allocation radio frequencies to reduce interference [131] and various other areas. In these applications, in general, better results are obtained from difference triangle sets having smaller scope. Hence, the determination of m_{nk} is of interest.

19.2 Golomb Rulers

19.7 **Remark** An important special case occurs when $n = 1$.

19.8 A *Golomb ruler* is a ruler with k marks and length L that measures every distance from 1 to L as a distance between two marks on the ruler in at most one way. A *optimal Golomb ruler* with k marks is a Golomb ruler (with k marks) of minimum length.

19.9 **Proposition** A Golomb ruler with k marks is a $(1, k-1)$-DΔS of minimum scope.

19.10 Examples $(1,k)$-DΔS of minimum scope (Golomb rulers with $k+1$ marks) for $k \le 19$.

k	Block
3	0 1 4 6
4	0 1 4 9 11
5	0 1 4 10 12 17
6	0 1 4 10 18 23 25
7	0 1 4 9 15 22 32 34
8	0 1 5 12 25 27 35 41 44
9	0 1 6 10 23 26 34 41 53 55
10	0 1 4 13 28 33 47 54 64 70 72
11	0 2 6 24 29 40 43 55 68 75 76 85
12	0 2 5 25 37 43 59 70 85 89 98 99 106
13	0 4 6 20 35 52 59 77 78 86 89 99 122 127
14	0 4 20 30 57 59 62 76 100 111 123 136 144 145 151
15	0 1 4 11 26 32 56 68 76 115 117 134 150 163 168 177
16	0 5 7 17 52 56 67 80 81 100 122 138 159 165 168 191 199
17	0 2 10 22 53 56 82 83 89 98 130 148 153 167 188 192 205 216
18	0 1 6 25 32 72 100 108 120 130 153 169 187 190 204 231 233 242 246
19	0 24 30 43 55 71 75 89 104 125 127 162 167 189 206 215 272 275 282 283

19.3 Modular Golomb Rulers

19.11 A *(v,k) modular Golomb ruler* is a set of k marks, $\{a_1, a_2, \ldots, a_k\}$, such that all of the differences, $\{a_i - a_j | 1 \le i \ne j \le k\}$, are distinct and nonzero modulo v.

19.12 Remarks Generally one is interested in dense rulers: for fixed k one wants v to be as small as possible. By simple counting, $v \ge k(k-1)+1$.

19.13 A *perfect difference set* is a (k^2-k+1, k) modular Golomb ruler.

19.14 Remark Perfect difference sets are special cases of difference sets. See §VI.18.

19.15 Theorem [1920] For every prime power q, there is a $(q^2+q+1, q+1)$ modular Golomb ruler.

19.16 Examples $(q^2+q+1, q+1)$ modular Golomb rulers for $2 \le q \le 16$.

q	v	k	Block
2	7	3	0 1 3
3	13	4	0 1 4 6
4	21	5	0 2 7 8 11
5	31	6	0 1 4 10 12 17
7	57	8	0 4 5 17 19 25 28 35
8	73	9	0 2 10 24 25 29 36 42 45
9	91	10	0 1 6 10 23 26 34 41 53 55
11	133	12	0 2 6 24 29 40 43 55 68 75 76 85
13	183	14	0 4 6 20 35 52 59 77 78 86 89 99 122 127
16	273	17	0 5 15 34 35 42 73 75 86 89 98 134 151 155 177 183 201

19.17 Theorem [302] For every prime power q, there is a (q^2-1, q) modular Golomb ruler. The missing differences are the $q-1$ multiples of $q+1$.

19.18 Examples (q^2-1, q) modular Golomb rulers for $3 \le q \le 17$.

q	v	k	Block
3	8	3	0 1 3
4	15	4	0 1 3 7
5	24	5	0 1 4 9 11
7	48	7	0 5 7 18 19 22 28
8	63	8	0 2 8 21 22 25 32 37
9	80	9	0 1 12 16 18 25 39 44 47
11	120	11	0 1 4 9 23 30 41 43 58 68 74
13	168	13	0 3 11 38 40 47 62 72 88 92 93 105 111
16	255	16	0 10 11 31 33 58 70 73 77 86 122 127 151 157 165 183
17	288	17	0 5 7 17 52 56 67 80 81 100 122 138 159 165 168 191 199

19.19 Theorem [1835] For every prime p, there is a $(p^2-p, p-1)$ modular Golomb ruler. The missing differences are the $2p-2$ multiples of p or $p-1$.

19.20 Examples $(p^2-p, p-1)$ modular Golomb rulers for $3 \le q \le 17$.

q	v	k	Block
3	6	2	0 1
5	20	4	0 1 3 9
7	42	6	0 1 3 11 16 20
11	110	10	0 13 16 17 25 31 52 54 59 78
13	156	12	0 1 3 10 18 32 38 43 59 89 93 112
17	272	16	0 13 14 23 42 53 86 89 107 111 113 148 156 163 168 194

19.21 Theorem If $\{a_1, \ldots, a_k\}$ is a (v, k) modular Golomb ruler, m and b are integers with $\gcd(m, v) = 1$, then $\{ma_1 + b, \ldots, ma_k + b\}$ is also a (v, k) modular Golomb ruler.

19.22 Remarks Modular Golomb rulers are also Golomb rulers. Theorem 19.21 can be used to obtain short rulers from Theorem 19.15 or Theorem 19.17 . All of the best rulers known for $k > 15$ are obtained in this way (or by truncating rulers obtained in this way). For $15 < k < 24$, computer searches have verified that there are no better rulers, and this is likely true for most larger values as well.

19.4 Difference Packings

19.23 A $(v, k; n)$-*difference packing*, or n-DP(v, k), is a set $\mathcal{X} = \{X_1, \ldots, X_n\}$, where for $1 \le i \le n$, $X_i = \{a_{i1}, \ldots, a_{ik}\}$ such that all of the differences, $\{a_{ij} - a_{il} | 1 \le i \le n, 1 \le j \ne l \le k\}$, are distinct and nonzero modulo v.

19.24 Remarks A (v, k)-modular Golomb ruler is a 1-DP(v, k).

19.25 Theorem A $(v, k, 1)$-cyclic difference family is a $\frac{v-1}{k(k-1)}$-DP(v, k). A $(v, k, 1)$-partial cyclic difference family is a $\frac{v-k}{k(k-1)}$-DP(v, k) (see §VI.16). A difference set of order q and index one is a 1-DP$(q^2+q+1, q+1)$ (see §VI.18).

19.26 Theorem An $(n, k-1)$-DΔS of scope m is an n-DP(v, k) for all $v \ge 2m+1$.

19.27 Theorem An n-DP(v,k) is an $(n,k-1)$-DΔS, whose scope is the largest element of a set of the difference packing.

19.28 Remarks In Theorem 19.27, one can often reduce the scope as follows. For the difference packing $\mathcal{X}=\{X_1,\ldots,X_n\}$, choose integers $a_1,\ldots,a_n$ and an integer m relatively prime to v. Then $\{m\cdot X_i+a_i \pmod v : i=1,\ldots,n\}$ is a difference packing whose largest element may differ from that of the original. This translation can also be used in conjunction with the following generalization of Theorem 19.27.

19.29 Theorem [1313] Let $\mathcal{X}=\{X_1,\ldots,X_n\}$ be an n-DP(v,k), where $X_i=\{b_{i1},\ldots,b_{ik}\}$ and $b_{i1}<b_{i2}<\cdots<b_{ik}$. For each $1\le i\le n$, let $\{B_{i1},\ldots,B_{is_i}\}$ be a packing of pairs by $(\ell+1)$-sets on the elements $\{1,\ldots,k\}$. Let $B_{ij}=\{c_{ij0},\ldots,c_{ij\ell}\}$ with $c_{ij0}<c_{ij1}<\cdots<c_{ij\ell}$. Then $\{\{b_{ic_{ijm}}-b_{ic_{ij0}} : 0\le m\le \ell\} \ : \ 1\le i\le n,\ 1\le j\le s_i\}$ is a $(\sum_{i=1}^n s_i,\ell)$-DΔS whose scope is $\max(b_{ic_{ij\ell}}-b_{ic_{ij0}} : \ 1\le i\le n,\ 1\le j\le s_i)$.

19.30 Theorem [488] If there exists an n-DP(v,k) and a $(g,k;1)$-difference matrix over $\mathbb{Z}_g$, then there exists a gn-DP(gv,k). If an n'-DP(g,k) also exists, then there exists a $gn+n'$-DP(gv,k).

19.5 Difference Triangle Sets: Variants

19.31 Let c and m be positive integers. A family of sets $\mathcal{B}=\{B_1,\ldots,B_m\}$ with $B_i=\{b_{i0},\ldots,b_{iv_i}\}$, $b_{i0}=0$, and $b_{i\ell}>b_{ik}$ when $\ell>k$, is a *perfect system of difference sets* with *threshold* c when

$$\bigcup_{i=1}^m\{b_{i\ell}-b_{ik} : 0\le k<\ell\le v_i\} \ = \ \{c,c+1,\ldots,c-1+\sigma\},$$

where $\sigma=\sum_{i=1}^m \frac{v_i(v_i+1)}{2}$.

19.32 Remark Perfect systems of difference sets restrict to *consecutive* sets of differences but permit *varying* block sizes. When all block sizes are equal, they are special types of difference triangle sets. There is a large literature on perfect systems of difference sets; see, for example, [1815] and references therein. Perfect difference families are perfect systems of difference sets with threshold 1 and all blocks having the same size; see §VI.16.3.

19.33 Remark Perfect difference families are (n,k)-DΔS having scope $n\binom{k+1}{2}$, the minimum possible.

19.34 Remark *Synch-sets* [1913] are analogues of $(1,k)$-DΔS in which each difference is permitted to occur at most some fixed number λ of times.

19.6 Difference Triangle Sets: Bounds

19.35 Theorem There exists an $(n,1)$-DΔS with scope n for all $n\ge 1$. There exists an $(n,2)$-DΔS with scope $3n$ whenever $n\equiv 0,1 \pmod 4$, and scope $3n+1$ whenever $n\equiv 2,3 \pmod 4$; these scopes are minimum.

19.36 Remarks $(n,2)$-DΔS can be constructed from Skolem sequences and hooked Skolem sequences (see §VI.53). The minimum scope of (n,k)-DΔS is unknown for all $k\ge 3$, except for some values of n. Upper bounds on m_{nk} are primarily obtained by computer search or by constructions [488, 1313, 1328, 1469, 1807] using the constructions for modular Golomb rulers. Lower bounds are obtained by computer search or derived by linear programming [1896] .

19.37 Table Bounds for m_{nk} [487, 488, 850, 1313, 1469, 1895, 1896, 1897]. Exact values are shown in **bold**; when no exact value is known, the upper bound is given above the lower bound.

$k\backslash n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
2	**3**	**7**	**10**	**12**	**15**	**19**	**22**	**24**	**27**	**31**	**34**	**36**	**39**	**43**	**46**
3	**6**	**13**	**19**	**24**	**30**	**36**	**42**	**48**	**54**	**60**	**66**	**72**	**78**	**84**	**90**
4	**11**	**22**	**32**	**41**	**51**	**60**	**71**	**80**	**91**	**100**	**111**	122 120	133 131	144 140	154 151
5	**17**	**34**	**49**	**64**	**79**	96 92	113 108	130 123	148 138	166 153	183 168	199 183	215 199	233 214	250 229
6	**25**	**51**	**72**	**94**	119 113	146 136	171 158	197 181	223 203	249 225	274 248	300 270	327 292	353 315	379 337
7	**34**	**70**	**100**	135 124	171 155	210 186	251 217	282 247	318 278	352 309	393 339	431 370	464 401	499 431	524 462
8	**44**	**94**	135 124	187 164	238 205	288 245	339 286	395 327	447 367	497 408	532 448	589 489	604 529	659 570	735 610
9	**55**	**121**	184 158	253 209	317 261	386 313	456 365	521 417	585 469	631 521	672 572	746 624	755 676	906 728	915 780
10	**72**	**153**	238 197	329 261	412 326	492 391	587 456	672 520	761 585	840 650	877 715	892 780	989 844	998 909	1268 974
11	**85**	195 161	311 240	416 320	527 399	638 478	740 558	844 637	956 716	1067 796	1097 875	1102 954	1113 1034	1301 1113	1316 1193
12	**106**	250 194	370 289	520 385	660 480	797 576	935 671	1076 767	1213 862	1348 958	1392 1054	1402 1149	1413 1245	1484 1340	1978 1436
13	**127**	288 229	447 343	599 456	800 569	967 683	1124 796	1318 909	1430 1023	1598 1136	1782 1249	1906 1363	1953 1476	2205 1589	2220 1703
14	**151**	334 268	526 401	690 534	866 667	1134 800	1319 933	1510 1066	1745 1198	1879 1331	2132 1464	2272 1597	2534 1730	2630 1863	2874 1996
15	**177**	365 311	593 464	820 618	1043 772	1257 926	1492 1080	1713 1234	2005 1388	2165 1542	2410 1696	2627 1850	2953 2003	3082 2157	3092 2311
16	**199**	450 356	678 533	937 709	1183 886	1436 1062	1689 1239	1929 1415	2259 1592	2389 1768	2698 1945	3003 2121	3195 2298	3422 2475	3442 2651
17	**216**	497 405	765 606	1058 807	1306 1007	1570 1208	1915 1409	2144 1610	2587 1811	2781 2012	3063 2213	3353 2413	3871 2614	4156 2815	4246 3016
18	**246**	559 457	861 684	1192 910	1522 1137	1853 1364	2111 1591	2508 1818	2767 2044	3083 2271	3615 2498	3741 2725	4315 2952	4483 3178	5020 3405
19	**283**	623 512	959 767	1288 1021	1699 1276	2022 1530	2474 1784	2683 2039	3074 2293	3584 2548	3854 2802	4141 3057	4744 3311	4770 3565	5508 3820
20	**333**	686 571	1083 855	1467 1139	1846 1422	2259 1706	2712 1990	3140 2274	3391 2557	3883 2841	4127 3125	4587 3409	5285 3692	5358 3976	5953 4260
21	**356**	768 633	1159 948	1598 1263	2081 1577	2418 1892	2979 2207	3420 2522	3768 2837	4222 3151	4687 3466	5231 3781	5686 4096	6242 4410	6398 4725
22	**372**	826 699	1285 1046	1781 1394	2308 1742	2747 2089	3198 2437	3645 2784	4300 3132	4543 3480	5026 3827	5517 4175	6071 4522	6728 4870	6987 5217
23	**425**	919 768	1418 1150	1962 1532	2530 1914	2984 2296	3546 2678	3941 3060	4618 3442	5171 3824	5758 4206	6184 4588	6643 4971	7139 5353	7795 5735
24	480 427	991 841	1549 1259	2092 1677	2667 2095	3277 2514	3762 2932	4555 3350	4915 3769	5518 4187	6365 4605	6542 5024	7107 5442	8229 5860	8310 6279
25	492 460	1076 917	1689 1373	2279 1829	2921 2286	3573 2742	4255 3198	4840 3655	5442 4111	5819 4567	6694 5024	7244 5480	8168 5936	8649 6392	9218 6849

See Also

§VI.16	Perfect difference families are (n, k)-DΔS having scope $n\binom{k+1}{2}$, the minimum possible.
§VI.17	Difference matrices are used in constructing difference packings.

References Cited: [131, 302, 487, 488, 850, 1313, 1328, 1469, 1807, 1815, 1835, 1895, 1896, 1897, 1913, 1920]

20 Directed Designs

Frank E. Bennett
Alireza Mahmoodi

20.1 Definitions and Examples

20.1 An ordered set $A = (a_1, a_2, \ldots, a_m)$ is *contained* in an ordered set $B = (b_1, b_2, \ldots, b_n)$ if $a_i = b_{\ell_i}, i = 1, 2, \ldots, m$, and $\ell_i < \ell_j$ for $i < j$.

20.2 A *directed t-design* of type t-(v, k, λ), denoted t-(v, k, λ) DD, is a pair $(X, \mathcal{B})$ where X is a v-element set of points and $\mathcal{B}$ is a collection of *ordered* k-subsets of X (*blocks*) with the property that every *ordered* t-subset of X is contained in exactly λ blocks.

20.3 Example Let $X = \{0, 1, 2, 3\}$ and let $\mathcal{B} = \{$ $(0, 1, 2, 3)$, $(1, 0, 3, 2)$, $(2, 0, 3, 1)$, $(3, 0, 2, 1)$, $(2, 1, 3, 0)$, $(3, 1, 2, 0)\}$. Then $(X, \mathcal{B})$ forms a 3-$(4, 4, 1)$ DD. The block $(0, 1, 2, 3)$ contains the four ordered triples $(0, 1, 2)$, $(0, 1, 3)$, $(0, 2, 3)$, and $(1, 2, 3)$.

20.4 A t-(v, k, λ) directed design is also denoted by $DB_t(k, \lambda; v)$ or $T_\lambda(t, k, v)$ with the subscript dropped when $t = 2$ and $\lambda = 1$, respectively.

20.5 A 2-(v, k, λ) DD is a *directed* BIBD (DBIBD for short) and is denoted by (v, k, λ) DD. A $(v, 3, \lambda)$ DD is referred to as a *directed triple system* and is denoted by DTS(v, λ).

20.6 Example The blocks $(0, 1, 2), (0, 2, 4), (0, 3, 1), (0, 4, 3)$ when developed modulo 5 form a DTS$(5, 3)$.

20.7 The *converse* of a directed design $(X, \mathcal{B})$, is $(X, \mathcal{B}^{-1})$ where $\mathcal{B}^{-1} = \{(a_k, \ldots, a_2, a_1) : (a_1, a_2, \ldots, a_k) \in \mathcal{B}\}$. A directed design is *self-converse* if it is isomorphic to its converse.

20.8 A *directed group divisible design*, (k, λ)-DGDD of type $m^{v/m}$, is a $(k, 2\lambda)$-GDD of type $m^{v/m}$ whose blocks are transitively ordered so that every ordered pair not contained in the same group appear in exactly λ blocks.

20.9 Remark A 2-(v, k, λ) DD is equivalent to a decomposition of the complete symmetric directed multigraph, λK_v^*, into transitive tournaments of size k. Directed designs are sometimes termed *transitive* designs.

20.2 Elementary Properties

20.10 Theorem A t-(v, k, λ) DD is also a t-$(v, k, \lambda t!)$ design.

20.11 The corresponding t-design of a directed design is its *underlying design.*

20.12 Theorem The existence of a t-(v, k, λ) DD implies the existence of a $(t-1)$-$(v-1, k-1, t\lambda)$ DD.

20.13 Theorem Every t-(v, k, λ) DD is a $(t-1)$-(v, k, λ') DD, where $\lambda' = \frac{\lambda t(v-t+1)}{(k-t+1)}$.

20.14 Corollary Every t-(v, k, λ) DD is an s-(v, k, λ_s) DD, for $0 \le s \le t-1$ where

$$\lambda_s = \lambda(\tbinom{v-s}{t-s}t!)/(\tbinom{k-s}{t-s}s!)$$

20.15 Proposition Corollary 20.14 implies that a necessary condition for the existence of a t-(v, k, λ) DD is that λ_s must be an integer for $s = 0, 1, \ldots, t-1$.

20.3 Existence

20.16 Example Let $(X, \mathcal{B})$ be any (v, k, λ) design with some arbitrary but fixed ordering imposed on the elements of each block. Then $(X, \mathcal{B} \cup \mathcal{B}^{-1})$ is a (v, k, λ) DD. Listed are some small (v, k, λ) DD where a (v, k, λ) design does not exist.

(v, k, λ)	Construction
$(6, 3, 1)$	Develop $(0, \infty, 4)$ and $(0, 1, 3)$ modulo 5
$(8, 3, 3)$	Develop $(0, 4, 1)$, $(0, 4, 2)$, $(0, 4, 3)$, $(0, 1, 7)$, $(0, 2, 1)$, $(0, 5, 3)$, and $(0, 2, 5)$ modulo 8
$(7, 4, 1)$	Develop $(0, 1, 4, 6)$ modulo 7
$(19, 4, 1)$	Develop $(0, 3, 12, 1)$, $(13, 1, 0, 5)$, and $(9, 4, 6, 0)$ modulo 19
$(6, 5, 2)$	Blocks: $(0, 1, 2, 3, 4)$, $(0, 1, 2, 3, 5)$, $(2, 1, 0, 4, 5)$, $(3, 4, 5, 1, 0)$, $(5, 4, 3, 2, 0)$, $(5, 4, 3, 2, 1)$
$(11, 5, 1)$	Develop $(0, 2, 1, 6, 9)$ modulo 11
$(16, 6, 1)$	Develop $(0, 1, x^3, x^6, x^9, x^{12})$ modulo 16, where x is a primitive root of $\mathbb{F}_{16}$, and $x^4 = x + 1$

20.17 Remark Directed triple systems have been studied extensively and they are closely related to ordinary triple systems (Theorem II.2.114). See [576, 578], where an excellent bibliography is given. Since directed BIBDs are equivalent to perfect deletion-correction codes, additional information can be found in §VI.14.2 and §VI.14.3. Theorem 20.18 summarizes the existence results for DBIBDs (see [200, 576]).

20.18 Theorem A 2-(v, k, λ) DD exists for $k \in \{3, 4, 5, 6\}$ if and only if $(v, k, \lambda) \neq (15, 5, 1)$ or $(21, 6, 1)$, $v(v-1)2\lambda \equiv 0 \pmod{k(k-1)}$, and $(v-1)2\lambda \equiv 0 \pmod{k-1}$.

20.19 Remark See [2115] for a determination of the existence of 2-$(v, 7, 1)$ DDs with the genuine exception of $v = 22$ and 68 possible exceptions.

20.20 Theorem [1249] A self-converse $(v, 3, 1)$ DD exists if and only if $v \equiv 0, 1 \pmod 3$ and $v \neq 6$.

20.21 Theorem [199, 1841, 1842, 2185] A (k, λ)-DGDD of type $m^{v/m}$ exists for $k \in \{3, 4, 5\}$ if and only if $v \geq km$, $v \equiv 0 \pmod m$, $(v-m)2\lambda \equiv 0 \pmod{k-1}$, and $v(v-m)2\lambda \equiv 0 \pmod{k(k-1)}$, except possibly when $k = 5$, $v/m = 15$, and $m = 9$ or $m \equiv 1, 5 \pmod 6$ but $m \not\equiv 0 \pmod 5$.

20.22 Theorem [946] A 3-$(v, 4, \lambda)$ DD exists if and only if $v\lambda \equiv 0 \pmod 2$.

20.23 Remark The necessary conditions for the existence of a 3-$(v, 5, 1)$ DD are $v \equiv 0, 1, 2 \pmod 5$. These designs do not exist for $v \in \{5, 6, 7\}$, but do exist for $v \in \{17, 26, 37\}$, as well as for the infinite class in Theorem 20.24.

20.24 Theorem [313] There exists a 3-$(25^n + 1, 5, 1)$ DD for all $n \geq 1$.

20.25 Remark The necessary condition for the existence of a 4-$(v, 5, 1)$ DD is $v \equiv 0, 1, 2, 3 \pmod 5$. No 4-$(6, 5, 1)$ DD exists, but for $v \in \{5, 7, 8, 13, 18, 48\}$, a 4-$(v, 5, 1)$ DD exists [313]; the design with $v = 7$ is used to establish Theorem 20.26.

20.26 Theorem [313] There exists a 4-$(2^n - 1, 5, 1)$ DD for all $n \geq 3$.

20.27 Theorem [1437] The set of permutations of length k, S_k, can be partitioned into k directed designs with parameters $(k-1)$-$(k, k, k-1)$ (or using the other notation, into $T(k-1, k, k)$). See Theorem VI.14.28.

20.28 Remark The only known example of a $T(t,k,k)$ when $k-t \geq 2$ is a $T(4,6,6)$ [1554].

20.29 Remark Replacing each block of an $S(k-1,k,v)$ with a $T(k-1,k,k)$ yields a $T(k-1,k,v)$, and hence $T(4,5,v)$ and $T(5,6,v+1)$ exist for $v = 11, 23, 47, 71, 83, 107, 131,$ and 167. Also, $T(4,6,6)$ together with $S(4,6,27)$ produce a $T(4,6,27)$ (see §II.5).

20.4 Directability and Consequences

20.30 Since a t-(v,k,λ) DD is also a t-$(v,k,\lambda t!)$ design, it is natural to ask whether a t-(v,k,λ) DD can be constructed from a t-$(v,k,\lambda t!)$ design by ordering the elements in each block. Such a process is referred to as *directing*, and when the directing process is successful the t-design is *directable*.

20.31 Theorem (Colbourn and Harms (see [576])) Every $(v,3,2\lambda)$ block design is directable.

20.32 Remark Theorem 20.31 together with the existence results for $(v,3,2\lambda)$ designs provide an existence proof for directed triple systems. An important consequence of the directability theorem is that results on one type of design can be carried over to the other type. There are numerous results concerning triple systems, which are thus applicable to directed triple systems (see [576]). Theorems 20.33 and 20.34 are applications of Theorem 20.31.

20.33 Theorem Let $v \geq 2w+1, v, w \neq 2$. If $\lambda \equiv 0 \pmod{\gcd(v-2,3)}$ and $\lambda \equiv 0 \pmod{\gcd(w-2,3)}$, then a DTS$(v,\lambda)$ exists having a sub-DTS(w,λ).

20.34 Theorem For $v \geq 3$, $\lambda \equiv 0 \pmod{\gcd(v-2,3)}$, and $\lambda \leq (v-2)/2$ there exists a DTS(v,λ) whose underlying design is simple.

20.35 Remark There are two known optimal algorithms for directing triple systems that are quite different from each other. Colbourn and Rosa (see [576]) present an optimal algorithm for directing triple systems of index two that preserves an automorphism group of the underlying design when certain necessary conditions are met.

20.36 Remarks Computational investigations [1512] have shown that none of the known biplanes (symmetric $(v,k,2)$ designs) with $v \geq 37$ is directable, and hence, the directability theorem for triple systems does not hold for BIBDs in general. The smallest known design that cannot be directed is a 2-$(28,7,2)$ design. Theorems 20.37 and 20.38 are consequences of the directing algorithm by Harms and Colbourn.

20.37 Theorem Every partial triple system of index 2λ underlies a partial directed triple system of index λ.

20.38 Theorem Every simple $(v,3,2\lambda)$ block design underlies at least four disjoint $(v,3,\lambda)$ DD.

20.39 Conjecture (Harms and Colbourn) Every simple $(v,3,2\lambda)$ block design underlies six disjoint $(v,3,\lambda)$ DD.

20.5 Automorphism, Isomorphism, and Large Sets

20.40 Theorem A DTS(v,λ) having a cyclic automorphism exists if and only if

1. $\lambda \equiv 1,5 \pmod 6$ and $v \equiv 1,4,7 \pmod{12}$;
2. $\lambda \equiv 2,4 \pmod 6$ and $v \equiv 1 \pmod 3$;
3. $\lambda \equiv 3 \pmod 6$ and $v \equiv 0,1,3 \pmod 4$; or
4. $\lambda \equiv 0 \pmod 6$ and $v \neq 2$.

20.41 Remark A similar theorem by Cho, Chae, and Hwang settles existence for k-rotational DTS(v,1)s.

20.42 Theorem For v sufficiently large, $v \equiv 0, 1 \pmod 3$, the number of nonisomorphic DTS$(v, 1)$ is $\exp[(v^2 \ln v/3)(1 + o(1)]$.

20.43 Remark [1708] The number of nonisomorphic DTS$(v, 1)$ is $1, 3, 32, 2368, 596893386$, and 3753619614456 for $v = 3, 4, 6, 7, 9, 10$, respectively.

20.44 Theorem For all $v \equiv 0, 1 \pmod 3$, there is a large set of disjoint DTS$(v, 1)$ (see [576] for references).

20.45 Remark A large set of $T(k - 1, k, k)$ exists for every positive integer k (see Theorem VI.14.28). Also, a large set of $T(4, 6, 6)$ exists [1554].

20.6 Intersection and Other Results

20.46 Theorem For $v \equiv 0, 1 \pmod 3$, there exist two DTS$(v, 1)$ on the same element set intersecting in s triples if and only if $s \in \{0, 1, \ldots, v(v - 1)/3\}$, $s \neq v(v - 1)/3 - 1$.

20.47 Theorem [1515] For $v \equiv 1 \pmod 3$ there exist two 2-$(v, 4, 1)$ DD on the same element set intersecting in s blocks if and only if either $s \in \{0, 1, \ldots, v(v-1)/6\} \backslash \{v(v-1)/6-1\}$ and $v \neq 7$, or $s \in \{0, 1, 7\}$ and $v = 7$.

20.48 Theorem [1514] For any even v, there exist two 3-$(v, 4, 1)$ DD on the same element set intersecting in s blocks if and only if $s \in \{0, 1, \ldots, v(v - 1)(v - 2)/4\} \setminus \{v(v - 1)(v - 2)/4 - 3, v(v - 1)(v - 2)/4 - 1\}$

20.49 Theorem [119, 118] For $k \leq 5$, a directed packing of order v with b blocks of size k and index λ exists whenever a $(v, k, 2\lambda)$ packing with b blocks exists, except possibly when $k = 5$ and $(v, \lambda) \in \{(19, 1), (27, 1), (43, 3)\}$.

20.50 Theorem [116, 119] For $k \leq 5$, a directed covering of order v with b blocks of size k and index λ exists whenever v is even or λ is even, and a $(v, k, 2\lambda)$-covering with b blocks exists.

See Also

§II.2	(Undirected) triple systems.
§VI.14	Directed BIBDs are equivalent to perfect deletion-correction codes.
§VI.35	Mendelsohn designs correspond to a different ordering of pairs within each block.
[576]	A survey of directed triple systems with proofs and original references.
[578]	Chapter 24 concerns directed triple systems.

References Cited: [116, 118, 119, 199, 200, 313, 576, 578, 946, 1249, 1437, 1512, 1514, 1515, 1554, 1708, 1841, 1842, 2115, 2185]

21 Factorial Designs

Deborah J. Street

21.1 Definitions and Examples

21.1 A *factor* is any attribute of the experimental units that may affect the response observed in the experiment. A *treatment factor* is allocated by the experimenter to the units. A *block factor* is an inherent attribute of the units. They are used to allocate the units into homogeneous sets that form the blocks. In either case, each factor may take one of several values. These values are the *levels* of the factor. If there are k treatment factors and factor i has s_i levels, $1 \leq i \leq k$, then it is a $s_1 \times s_2 \times \ldots \times s_k$ *factorial design*. If $s_1 = s_2$, say, then one writes ${s_1}^2 \times s_3 \times \ldots \times s_k$.

21.2 Example Stolle et al. [1981] outline a possible experiment in the psycholegal area, which would require a factorial design approach. They want to investigate mock-juror perception of child witnesses. The factors of interest (and the corresponding factor levels) were witness age (with 2 or 3 levels), form of testimony (in open court or via closed-circuit television), communication style (powerful or powerless), style of prosecuting attorney's questions (leading or nonleading), defendant (guilty or innocent), and deliberation by mock-jury (do deliberate or do not deliberate). Only some combinations of factor levels can be completed on each day and so "day" becomes a blocking factor, and one must be sure that all levels of each factor appear on each day. If this does not happen, then it is impossible to distinguish "day" effects from the effects of the levels of that factor. [1767] is an annotated bibliography of application papers.

21.3 Remark The aim of a factorial design is to determine the effect of each of the treatment factors on the response observed and to determine whether there are any interactions between two, or more, of the treatment factors. The block factors are regarded as nuisance factors whose effects must be allowed for in the analysis but which are not of interest *per se*.

21.4 Each of the possible combinations of treatment factor levels is a *treatment combination*. These are usually represented by k-tuples, with the ith entry being from a set of s_i symbols.

21.5 Example A $2 \times 2 \times 3$ factorial design has treatment combinations

{(000), (001), (002), (010), (011), (012), (100), (101), (102), (110), (111), (112)}.

21.6 If all the treatment factors have the same number of levels then the factorial design is *symmetrical* (or *pure*); otherwise, the design is *asymmetrical* (or *mixed*).

21.7 Remarks

1. The factor levels can be represented by any finite set of the elements. If the number of levels is a prime or a prime power, then it is usual to use the elements of a finite field of the appropriate order.
2. Symmetrical factorial designs in which the number of levels is a prime or a prime power are related to finite geometries (§VI.2) [1984].
3. When the experiment is conducted, a response is observed on each occasion that a treatment combination appears in the design. The responses are typically represented by y subscripted by the treatment combination and, if necessary,

the appropriate blocking factor(s). The analysis of factorial designs is discussed in [1623, 1365, 1021].

21.8 A factorial design may have each possible treatment combination appearing an equal number of times, in which case it is *complete*, or only a subset of the possible treatment combinations may appear, in which case the design is *incomplete*. Each occurrence of a treatment combination in a design is a *run*. Designs in which each treatment combination appears exactly once are *single replicate designs*. Incomplete factorial designs are also known as *fractional factorial designs*.

21.9 Remark Fractional factorial designs are sometimes referred to as 1/2 replicates (if half of the possible treatment combinations appear in the experiment), 1/3 replicates, and so on. A 1/2 replicate of a $2 \times 2 \times 3$ factorial design could have treatment combinations {(000), (110), (101), (011), (102), (012)}.

21.10 A factorial design, whether complete or incomplete, may have one, or more, blocking factors associated with each unit. If each treatment combination appears exactly once in each block, then the blocks are *complete* and each block constitutes a complete replicate of the factorial design. Otherwise, the blocks are *incomplete*.

21.11 Remarks

1. A complete factorial design can be conducted in either complete or incomplete blocks. The same is true for fractional factorial designs.
2. It is possible for blocks to have more units than there are distinct treatment combinations in the experiment. Then the blocks constitute either two, or more, complete replicates of the treatment combinations in the experiment or they can be viewed as a union of one or more complete blocks and an incomplete block.
3. Tables factorial designs and fractional factorial designs with up to 9 factors, with incomplete blocks indicated, for 2^k, 3^k, and $2^k 3^n$ designs can be found in §21.6. More extensive tables can be found in [1581, 1623, 276, 472]. An algorithm to construct fractional factorial designs is available at

   `http://support.sas.com/techsup/technote/ts723.html`.

21.2 Symmetrical Prime Power Factorial Designs

21.12 Let s be a prime or a prime power. Then the treatment combinations in a symmetrical s^k factorial design are k-tuples with each entry coming from $\mathbb{F}_s$. Usually one uses a k-tuple to represent both the treatment combination and the response observed when that treatment combination is applied to an experimental unit.

21.13 Example Suppose that s=3 and k=2. Then the treatment combinations are

{(00), (01), (02), (10), (11), (12), (20), (21), (22)}.

21.14 In an s^k factorial design, the *main effect* of, say, factor A compares the responses among the s sets $T_\theta = \{(x_1, x_2, \ldots, x_k) | x_a = \theta\}$, $\theta \in \mathbb{F}_s$. The sets T_θ partition the s^k treatment combinations into s sets each of size s^{k-1}. Denote this partition by $\mathcal{P}(A)$.

21.15 The *interaction effect* of say, factors A and B compares the responses among the sets within the $s-1$ partitions given by $\{(x_1, x_2, \ldots, x_k) | x_a + \theta x_b = \gamma\}$, $\theta, \gamma \in \mathbb{F}_s, \theta \neq 0$. For fixed θ, denote these partitions by $\mathcal{P}(AB^\theta)$. Higher order interactions are defined similarly. For instance, the three factor interaction between the factors A, B, and C compares the responses among the sets within the $(s-1)^2$ partitions given by $\mathcal{P}(AB^\theta C^\delta)$, $\theta, \delta \in \mathbb{F}_s, \theta \neq 0, \delta \neq 0$.

21.16 Example Suppose that $s = 3$ and $k = 2$. Then letting the factors be A and B, $\mathcal{P}(A) = \{\{(x_1, x_2)|x_1 = \theta\}, \theta \in \mathbb{F}_3\} = \{\{(00), (01), (02)\}, \{(10), (11), (12)\}, \{(20), (21), (22)\}\}$. The two partitions associated with the interactions between factors A and B are $\mathcal{P}(AB) = \{\{(x_1, x_2)|x_1 + x_2 = \theta\}, \theta \in \mathbb{F}_3\}$ and $\mathcal{P}(AB^2) = \{\{(x_1, x_2)|x_1 + 2x_2 = \theta\}, \theta \in \mathbb{F}_3\}$. Thus, $\mathcal{P}(AB) = \{\{(00), (12), (21)\}, \{(01), (10), (22)\}, \{(02), (11), (20)\}\}$, and $\mathcal{P}(AB^2) = \{\{(00), (11), (22)\}, \{(02), (10), (21)\}, \{(01), (12), (20)\}\}$

21.17 Table Partitions for the effects in a $2 \times 2 \times 2$ factorial design.

Effect	Partition	
A	{(000), (001), (010), (011)}	{(100), (101), (110), (111)}
B	{(000), (001), (100), (101)}	{(010), (011), (110), (111)}
C	{(000), (010), (100), (110)}	{(001), (011), (101), (111)}
AB	{(000), (001), (110), (111)}	{(100), (101), (010), (011)}
AC	{(000), (010), (101), (111)}	{(100), (110), (001), (011)}
BC	{(000), (100), (011), (111)}	{(010), (110), (001), (101)}
ABC	{(000), (011), (101), (110)}	{(100), (111), (001), (010)}

21.18 Remarks

1. The sets of the partitions are the pencils of the corresponding affine plane [1984].
2. The first nonzero coefficient in each equation can be made to equal 1.

21.19 Order the treatment combinations lexicographically and let τ_i represent the expected response of the ith treatment combination. Then a *contrast* is a linear function $\sum_i \lambda_i \tau_i$ with $\sum_i \lambda_i = 0$. If treatment combination i appears n_i times in the design, then two contrasts with coefficients λ_i and μ_i are *orthogonal* if and only if $\sum_i \lambda_i \mu_i / n_i = 0$.

21.20 Example The unique orthogonal contrasts for an equi-replicated $2 \times 2 \times 2$ factorial design.

Effect	(000)	(001)	(010)	(011)	(100)	(101)	(110)	(111)
A	−1	−1	−1	−1	1	1	1	1
B	−1	−1	1	1	−1	−1	1	1
C	−1	1	−1	1	−1	1	−1	1
AB	1	1	−1	−1	−1	−1	1	1
AC	1	−1	1	−1	−1	1	−1	1
BC	1	−1	−1	1	1	−1	−1	1
ABC	−1	1	1	−1	1	−1	−1	1

21.21 Example Possible orthogonal contrasts for an equi-replicated 3×3 factorial design. (These are not unique.)

Effect	(00)	(01)	(02)	(10)	(11)	(12)	(20)	(21)	(22)
A	−1	−1	−1	0	0	0	1	1	1
A	−1	−1	−1	2	2	2	−1	−1	−1
B	−1	0	1	−1	0	1	−1	0	1
B	−1	2	−1	−1	2	−1	−1	2	−1
AB	−1	0	1	0	1	−1	1	−1	0
AB	−1	2	−1	2	−1	−1	−1	−1	2
AB^2	−1	1	0	0	−1	1	1	0	−1
AB^2	−1	1	2	2	−1	−1	−1	2	−1

21.22 Consider a factorial design with t treatment combinations and with observed responses $y_{ij}, 1 \le i \le t, 1 \le j \le n_i$. If a contrast has coefficients $\lambda_i, 1 \le i \le t$, then the *sum of squares* associated with the contrast is given by $(\sum_i \sum_j \lambda_i y_{ij}/n_i)^2/(\sum_i \lambda_i^2/n_i)$.

21.23 The set of all treatment contrasts forms a vector space of dimension $t-1$, the *treatment contrast space*. Thus, any set of $t-1$ orthogonal contrasts is maximal. Adding the sums of squares associated with each contrast in a maximal set gives a unique sum of squares, the *treatment sum of squares*. The dimension of the space is the number of *degrees of freedom* of the corresponding sum of squares.

21.24 Let $T_1, T_2, \ldots, T_m$ be a partition of the treatment combinations. Then a *contrast among the* T_i is one in which all the treatment combinations in each T_i have the same coefficient in the contrast. This is written as $\sum_i \lambda_i T_i$, where necessarily $\sum_i \lambda_i |T_i| = 0$.

21.25 Example The first two contrasts in Example 21.21 are orthogonal contrasts on $\mathcal{P}(A)$. The third and fourth contrasts in Example 21.21 are orthogonal contrasts on $\mathcal{P}(B)$, the next two are orthogonal contrasts on $\mathcal{P}(AB)$, and the final two are orthogonal contrasts on $\mathcal{P}(AB^2)$.

21.26 Remarks

1. The main effects and interaction effects define orthogonal subspaces of the treatment contrast space.
2. Any basis of orthogonal contrasts can be used to calculate the sum of squares associated with any effect.
3. The coefficients of orthogonal polynomials of degree s provide one set of $s-1$ orthogonal contrasts. These can be used as the coefficients for the sets in the corresponding partitions. The various contrasts are the linear effect, the quadratic effect, the linear $\times$ quadratic interaction, and so on. Related matters are discussed in [1317, 1310, 1363].
4. If the aim of an experiment is to model a polynomial response, then response surface designs are more appropriate. See [1661].
5. In practice, interactions involving several factors can be regarded as negligible.

21.27 Denote the blocks by $B_1, B_2, \ldots, B_b$. These form a partition of the treatment combinations. Contrasts among the B_i are elements of the *block contrast space*, a $(b-1)$-dimensional subspace of the treatment contrast space. The corresponding sum of squares is the *block sum of squares*.

21.28 A main (or interaction) effect is *confounded with blocks* if the inner product of a block contrast and an effect contrast is nonzero. If every contrast in an effect subspace is in the block contrast space, then that effect is *completely confounded with blocks*. If some contrasts in an effect subspace are in the block contrast space and some are not, then that effect is *partly confounded with blocks*.

21.29 Example Consider a $2 \times 2 \times 2$ complete factorial design conducted in two blocks of size four. If the two blocks correspond to any of the partitions in Table 21.17, then the corresponding effect is completely confounded with blocks. For example, if the blocks are {(000), (011), (101), (110)} and {(100), (111), (001), (010)}, then the three factor interaction is completely confounded with blocks. If the two blocks do not correspond to any of these partitions, then two, or more, effects are partly confounded. For instance, suppose that the blocks are {(000), (100), (110), (101)} and {(010), (001), (011), (111)}. Then the block contrast has coefficients (using lexicographic order

for the treatment combinations) $(-1,-1,1,-1,1,-1,1,1)$, which is orthogonal to the contrasts corresponding to each of the two factor interactions but not to the other four effects. Thus, the three main effects and the three factor interaction are all partly confounded with blocks.

21.30 Remarks

1. It is usual for all blocks to be of the same size, which must then be s^m, $m \le k$.
2. It is usual for all blocks to be obtained from intersections of sets in $\mathcal{P}$s. The corresponding effects are then confounded with blocks, and the blocks constitute a subspace of dimension m and its cosets.

21.31 If the blocks in an incomplete factorial design constitute a subspace and its cosets, then the subspace is the *principal block* (or *intrablock subgroup*). The set of coset representatives forms the *interblock subgroup*.

21.32 Theorem [1984] Consider an s^k factorial design in s^{k-m} blocks of size s^m where the blocks are given by a principal block and its cosets. Then there are $(s^{k-m}-1)/(s-1)$ effects confounded with blocks.

21.33 Example Let $s=3$, $k=3$, and $m=1$. Hence, there are nine blocks of size 3. Suppose one decides to confound $\mathcal{P}(111)$ and $\mathcal{P}(112)$ (which are both part of the three factor interaction). Then the subspace is $\{(x_1,x_2,x_3)|x_1+x_2+x_3=0, x_1+x_2+2x_3=0\}$=$\{(000),(120),(210)\}$. There are $(3^{3-1}-1)/(3-1)=4$ effects, each corresponding to two degrees of freedom, confounded in total. In addition to the two effects that were chosen to confound, one has also confounded $\mathcal{P}(001)$ (since $2(x_1+x_2+x_3)+(x_1+x_2+2x_3)=x_3=0$) and $\mathcal{P}(110)$ (since $2(x_1+x_2+x_3)+2(x_1+x_2+2x_3)=x_1+x_2=0$). Thus, one has confounded part of a main effect and part of a two-factor interaction; so in practice this is not a good allocation.

21.34 There are $(k-m)$ independent confounded effects. The remaining confounded effects, which are determined as a linear combination of these, are the *generalized interactions*.

21.35 Remarks

1. The independent confounded effects are usually interactions involving several factors, as these are least likely to be significant. It is necessary to be careful that none of the generalized interactions that are confounded is of interest, but there is no simple way to calculate all the generalized interactions.
2. The blocks can be determined most easily by evaluating the principal block and then obtaining all its cosets.
3. [511] gives an algorithm to decide if two fractions of a design with binary attributes are isomorphic. Other results on the isomorphism of fractional factorial designs appear in [1490].
4. The order of runs in an experiment may be important. Changing some factor levels may be very difficult and so should happen as infrequently as possible. Changing levels frequently gives a design that is robust against trend. See [126, 491, 485] for a discussion of some of the issues involved.

21.36 If several replicates of a complete factorial are conducted and the same effects are confounded in each replicate, then these effects are *totally confounded*; effects confounded in some replicates but not others are *partially confounded*.

21.3 Fractional Symmetrical Prime Power Factorial Designs

21.37 A $1/(s^m)$ replicate of an s^k factorial design has s^{k-m} distinct treatment combinations appearing in it. Assume that these constitute the principal block of some incomplete block design. The set of confounded effects gives the defining equations for the treatment combinations in the fractional replicate. In this setting the effects are the *defining contrasts*. Two effects are *aliased* if, in the fractional replicate, the $\mathcal{P}$ corresponding to the two effects (and hence the estimates) are indistinguishable. An s^{k-m} design is often written to mean a $1/s^m$ replicate of an s^k factorial design.

21.38 Example Consider a 1/2 replicate of a 2^3 factorial design with treatment combinations {(000), (110), (101), (011)}. These are all the solutions of the equation $x_1+x_2+x_3 = 0$ and so the defining contrast is $\mathcal{P}(111)$, the three factor interaction. For $\mathcal{P}(100)$, for example, the partition in this 1/2 replicate is {(000), (011)} and {(110), (101)}. This is the same as the partition $\mathcal{P}(011)$. Hence, the main effect of A and the two factor interaction of B and C are aliased. All the partitions for this case appear in the next table.

Effects	Partition
A, BC	{(000), (011)}, {(110), (101)}
B, AC	{(000), (101)}, {(110), (011)}
C, AB	{(000), (110)}, {(101), (011)}

21.39 Remarks

1. The defining contrasts in a fractional factorial design determine both the effects about which no information is available and the aliasing structure of the design.
2. The defining contrasts should all correspond to higher order interactions, as should the generalized interactions of these.
3. The aliasing should be such that all main effects can be estimated independently of each other and preferably of two-factor interactions. The higher the order of the interactions aliased with main effects, the more desirable is the design. See §21.4.
4. Sometimes irregular fractions are used. Typically these include the principal block and some of the cosets. See [1623].

21.40 Example Let $s = 5$, $k = 4$, and $m = 2$. Suppose that the effects corresponding to the partitions $\mathcal{P}(a, b, c, d)$ and $\mathcal{P}(w, x, y, z)$ are the defining contrasts. Then the generalized interactions are calculated as $\alpha(a, b, c, d) + \beta(w, x, y, z)$, $\alpha, \beta \in \mathbb{F}_5$, α, β not both 0. Hence, it is not possible for all of the defining contrasts to involve all four factors. Suppose $a = b = c = 1$, $d = 0$. Then the generalized interactions are of the form $(\alpha + \beta w,\ \alpha + \beta x,\ \alpha + \beta y,\ \beta z)$. Thus, one wants z to be nonzero. One does not want w, x, and y all to be zero; otherwise, there is a confounding of the main effect of the fourth factor. So assume that $w = 1$. Then $\alpha + \beta w = \alpha + \beta$. If $\alpha + \beta = 0$, then one would like $\alpha + \beta x$ and $\alpha + \beta y$ to be nonzero (so that the contrast involves three factors). Hence, one wants $\beta(x - 1) \neq 0$ and $\beta(y - 1) \neq 0$. Thus $x, y \neq 1$. Try $z = 1$, $x = y = 2$. Then the defining contrasts are $(1, 1, 1, 0)$, $(1, 2, 2, 1)$, and their generalized interactions $(0, 0, 1, 1) = 4(1, 1, 1, 0) + (1, 2, 2, 1)$ and $(1, 0, 0, 4) = 2(1, 1, 1, 0) + 4(1, 2, 2, 1)$. Both involve confounding part of a two-factor interaction. Can one avoid this? Try $z = 1$, $x = 2$, $y = 3$. The defining contrasts are now $(1, 1, 1, 0)$, $(1, 2, 3, 1)$ and the generalized interactions $(1, 0, 4, 4) = 2(1, 1, 1, 0) + 4(1, 2, 3, 1)$ and $(0, 1, 2, 1) = 4(1, 1, 1, 0)+(1, 2, 3, 1)$. This is a satisfactory arrangement. The treatment combinations to be used in the experiment are then $\{(x_1, x_2, x_3, x_4) | x_1 + x_2 + x_3 =$

$\theta, x_1 + 2x_2 + 3x_3 + x_4 = \eta\}$ for some arbitrary but fixed θ, η in F_5. The confounded effects may be written as $I \equiv ABC \equiv ABC^2D^3 \equiv AC^4D^4 \equiv BC^2D$.

21.41 Remarks

1. The designs advocated by Taguchi are, in fact, fractional factorial designs constructed as described here. For instance, the L_4 is a 2^{3-1}; the L_8 is a 2^{7-4}; the L_9 is a 3^{4-2}; the L_{12} is a Plackett–Burman Design (see §21.5). See [314, 1240] for a more complete discussion.
2. A computer program for determining defining contrasts for two-level designs with $3 \le k \le 12$ is given in [2078].
3. Another systematic method, suitable for computer implementation, for the determination of defining contrasts and confounded effects is given in [830].

21.4 Ways To Compare Factorial Designs

21.42 A fractional factorial design is of *resolution* R if no p factor interaction is aliased with another effect containing less than $R - p$ factors. $R_s(k, m)$ denotes the maximum resolution of an s^{k-m} design.

21.43 Remarks

1. The resolution is usually written in roman numerals.
2. In a resolution III design, no main effects (1-factor interactions) are aliased with each other.
3. In a resolution V design, no main effects are aliased with 1-, 2-, or 3-factor effects and no 2-factor effects are aliased with each other.
4. An orthogonal array of strength t is a fractional factorial design with resolution $t + 1$. See §III.7.

21.44 Example Consider the 2^{3-1} design with treatment combinations {(000), (011), (101), (110)}. The design is of resolution III because main effects are aliased with two-factor interactions. In the 2^{3-1} design with treatment combinations {(000), (001), (110), (111)}, the main effects of A and B are aliased so the design is not of resolution III but of resolution II.

21.45 Theorem

1. [91] Suppose that $s_1 < s_2 < \ldots < s_k$. In a $s_1^{n_1} \times \ldots \times s_k^{n_k}$ design of resolution IV, a lower bound on the number of runs required is $s_k(\sum_i (s_i - 1)n_i - (s_k - 2))$.
2. [473] $R_s(k + (s^m - 1)/(s - 1), m) \ge R_s(k, m) + s^{m-1}$.

21.46 Remarks

1. The only designs known that meet this bound are 2^k designs, $2^2 \times 2a$ designs, and some two-factor resolution V designs. See [91].
2. An algorithm for partitioning 2^k designs into 2^m mutually exclusive 2^{k-m} fractional factorial designs, each of resolution III, $5 \le k \le 20$, is given in [1641].

21.47 In an $s_1 \times s_2 \times \ldots \times s_k$ factorial design, use the integers modulo s_i to denote the s_i levels of factor i, $1 \le i \le k$. Let $\mathbb{Z}_{s_i}$ be the integers modulo s_i and let G_t be the abelian group of treatment combinations with addition defined componentwise. A single replicate factorial design in incomplete blocks is a *generalized cyclic design* if one block, say B_0, is a subgroup of G_t and the other blocks are the cosets of B_0 in G_t. B_0 is the *principal block* of the design. If B_0 can be generated by g treatment combinations then the generalized cyclic design is a *g-generator design*.

21.48 Example In a 2^3 design in which the three-factor interaction is confounded, B_0 = {(000), (011), (110), (101)} and any two of the nonzero treatment combinations generate B_0. Hence $g = 2$.

21.49 Let $a = \text{lcm}(s_1, s_2, \ldots, s_k)$. Let the abelian group $G_c = \{(c_1, \ldots, c_k) | c_i \in \mathbb{Z}_{s_i}\}$ with addition defined componentwise. Define the bilinear form $[\mathbf{c}, \mathbf{t}] = \sum_i (c_i t_i a / s_i) \pmod a$. Then the *annihilator* of B_0, $(B_0)^0$, is $\{\mathbf{c} | \mathbf{c} \in G_c, [\mathbf{c}, \mathbf{t}] = 0 \ \forall \mathbf{t} \in B_0\}$. The *confounding scheme* of the design constructed from B_0 is completely specified by the elements in $C = (B_0)^0$ in the sense that each element $\mathbf{c} \in C$ corresponds to a single degree of freedom from the interaction of the factors corresponding to the nonzero entries of $\mathbf{c}$. C is the *defining contrasts subgroup*.

21.50 Remark Either B_0 or C can be used to completely specify the design since $B_0 = C^0$.

21.51 Example Let $s = k = 3$, $g = 1$ and let B_0 be generated by (120). Then B_0={(120), (210), (000)} (see Example 21.33). Thus, $a = \text{lcm}(3) = 3$ and so $C = \{\mathbf{c} | c_1 + 2c_2 = 0\}$ ={(000), (001), (002), (110), (220), (111), (112), (221), (222)}. Hence, in this design two degrees of freedom of the main effect of the third factor, two degrees of freedom of the two factor interaction between factors 1 and 2, and four degrees of freedom of the three factor interaction are confounded, as found in Example 21.33.

21.52 Let $\mathbf{c} \in C$, the defining contrasts subgroup of an s^{k-m} fractional factorial design. The *wordlength* of $\mathbf{c}$ is the number of nonzero entries in $\mathbf{c}$. Let a_i be the number of vectors in C with wordlength i, $1 \le i \le k$. Then $\mathbf{w}$=$(a_1, \ldots, a_k)$ is the *wordlength pattern* of the design with principal block C^0. The resolution of a design is the smallest i such that a_i is positive. If two designs, d_1 and d_2, are both resolution r and if a_r for d_1 is less than a_r for d_2 then d_1 has *less aberration* than d_2. An s^{k-m} design has *minimum aberration* if no other s^{k-m} design has less aberration. The *s^m-lag* of the vector $\mathbf{w}$ is the juxtaposition of a zero vector of length s^m and the vector $\mathbf{w}$. This is written as $lag(\mathbf{w}, s^m)$. (See [833, 473].)

21.53 Example The wordlength pattern of the design in Example 21.51 is (2, 2, 4).

21.54 Theorem [473] For any s^{k-m} fractional factorial design with wordlength pattern $\mathbf{w}$ there exists an $s^{(k+(s^m-1)/(s-1))-m}$ design with wordlength pattern $lag(\mathbf{w}, s^{m-1})$.

21.55 Theorem [473] Let $F_1, \ldots, F_k$ denote the k factors in the design.

1. The minimum aberration 2^{k-1} designs have defining contrast subgroup $C = \langle (11 \ldots 1) \rangle$ (equivalently $I \equiv F_1 F_2 \ldots F_k$).
2. Let $k - 2 = 3a + r, 0 \le r < 3$. Then a minimum aberration 2^{k-2} design has defining contrasts
   $I \equiv F_1 \ldots F_{2a} F_{k-1} \equiv F_{a+1} \ldots F_{3a} F_k$, if $r = 0$;
   $I \equiv F_1 \ldots F_{2a+1} F_{k-1} \equiv F_{a+1} \ldots F_{3a+1} F_k$, if $r = 1$;
   $I \equiv F_1 \ldots F_{2a+1} F_{k-1} \equiv F_{a+1} \ldots F_{3a+2} F_k$, if $r = 2$.
3. Let $k = 7a + r, 0 \le r \le 6$. For $i = 1, \ldots, 7$, define
   $B_i = \{(ia - a + 1), (ia - a + 2), \ldots, (ia), (7a + i)\}$ when $i \le r$, and
   $B_i = \{(ia - a + 1), (ia - a + 2), \ldots, (ia)\}$, otherwise.
   The elements of B_i are the subscripts of the Fs, and they subdivide the k letters into seven approximately equal blocks. Then a minimum aberration 2^{k-3} design has defining contrast $I \equiv B_7 B_6 B_4 B_3 \equiv B_7 B_5 B_4 B_2 \equiv B_6 B_5 B_4 B_1$.
4. Let $k = 15a + r, 0 \le r \le 15$. For $i = 1, \ldots, 15$, let
   $B_i = \{(ia - a + 1), (ia - a + 2), \ldots, (ia), (15a + i)\}$, for $i \le r$, and
   $B_i = \{(ia - a + 1), (ia - a + 2), \ldots, (ia)\}$, otherwise.
   Then a minimum aberration 2^{k-4} design has defining contrast

$$I \equiv B_{15}B_{14}B_{12}B_9B_8B_7B_6B_1 \equiv B_{15}B_{13}B_{11}B_9B_8B_7B_5B_2$$
$$\equiv B_{15}B_{14}B_{11}B_{10}B_8B_6B_5B_3 \equiv B_{15}B_{13}B_{12}B_{10}B_7B_6B_5B_4, \text{ if } r \neq 5.$$

If $r = 5$, then interchange B_{15} and B_5 in the defining contrast.

21.56 Example Let $k = 6$. To construct a 2^{6-3} minimum aberration design, observe that $6 = 7\times0+6$, so $a = 0$ and $r = 6$. Then $B_1 = \{1\}, B_2 = \{2\}, B_3 = \{3\}, B_4 = \{4\}, B_5 = \{5\}, B_6 = \{6\}, B_7 = \emptyset$. The defining contrast is $\mathrm{I} \equiv F_3F_4F_6 \equiv F_2F_4F_5 \equiv F_1F_4F_5F_6$, and hence, the principal block is $\{(x_1, x_2, x_3, x_4, x_5, x_6) | x_3+x_4+x_6 = 0, x_2+x_4+x_5 = 0, x_1+x_4+x_5+x_6 = 0\}$ ={(000000), (001110), (010101), (011011), (100111), (101001), (110010), (111100)}. The wordlength pattern for this design is (0, 0, 4, 3, 0, 0) and so the design is resolution II.

21.57 Remarks [473]

1. Resolution has a periodic property for fractions with $m \leq 4$. This is why the recursive-type constructions work. For other m, one needs to find the least k above for which the periodicity holds.
2. Minimum aberration has been extended to irregular fractions by [490]. Tables of minimum aberration designs for designs with levels a power of 2 or 3 are given in [1642].

21.58 Theorem [473]

1. For any fixed m, there exists a positive integer K_m such that for $k > K_m$, $R_s(k + (s^m - 1)/(s - 1), m) = R_s(k, m) + s^{m-1}$.
2. For any fixed m, there exists a positive integer M_m such that for $k > M_m$, the minimum aberration property is periodic (that is, if a minimum aberration s^{k-m} design has the wordlength pattern $\mathbf{w}$, then there exists a minimum aberration $s^{(k+(s^m-1)/(s-1))-m}$ design with wordlength pattern lag($\mathbf{w}$, s^{m-1}).

21.59 Consider an s^{k-m} fractional factorial design, d_1, with wordlength pattern $\mathbf{w} = (a_1, a_2, \ldots, a_k)$. The ith *moment of the design* is defined to be $M_i(d_1) = \sum_j j^i a_j$. Consider two designs d_1 and d_2. Let f be the first i such that $M_i(d_1) \neq M_i(d_2)$ and suppose $M_f(d_1) < M_f(d_2)$. Then d_2 has *better moments* if f is odd, and d_1 has *better moments* if f is even. A design has *optimal moments* if no other design has better moments. (See [829].)

21.60 Example The design in Example 21.56 has M_1=24 and M_2=84.

21.61 Remark The optimal moments criterion has a periodic property for any s^{k-m} design. See [473].

21.5 Miscellaneous Topics

21.62 In a 2^{k-m} factorial design a *fold-over design* refers to one in which, if treatment combination $(x_1, x_2, \ldots, x_k)$ is in the fraction, so is the treatment combination $(1 + x_1, 1 + x_2, \ldots, 1 + x_k)$.

21.63 Remark Folding over a design of resolution III gives a design of resolution IV.

21.64 Example Folding over the design in Example 21.56 gives the design with the additional treatment combinations {(111111), (110001), (101010), (100100), (011000), (010110), (001101), (000011)}. Hence, the defining contrasts are $I \equiv F_1F_4F_5F_6 \equiv F_2F_3F_5F_6 \equiv F_1F_2F_3F_4$, and the wordlength pattern is (0, 0, 0, 3, 0), so the design is resolution IV.

21.65 In a *saturated design* the number of effects to be estimated is equal to the number of experimental runs. In a *supersaturated design*, the number of effects to be estimated is greater than the number of experimental runs. These designs are used when there is a large number of factors that might influence the outcome but only a few of them are likely to be active in practice. So these designs are used to screen for the active factors. Constructions are given in [805, 1477, 2175].

21.66 *Plackett–Burman designs* are saturated two-level fractional factorial designs that exist when the number of runs is a multiple of 4.

21.67 Example A 12-run Plackett–Burman design is given on the right.

1	0	1	0	0	0	1	1	1	0	1
1	1	0	1	0	0	0	1	1	1	0
0	1	1	0	1	0	0	0	1	1	1
1	0	1	1	0	1	0	0	0	1	1
1	1	0	1	1	0	1	0	0	0	1
1	1	1	0	1	1	0	1	0	0	0
0	1	1	1	0	1	1	0	1	0	0
0	0	1	1	1	0	1	1	0	1	0
0	0	0	1	1	1	0	1	1	0	1
1	0	0	0	1	1	1	0	1	1	0
0	1	0	0	0	1	1	1	0	1	1
0	0	0	0	0	0	0	0	0	0	0

21.68 Remark The Plackett–Burman designs are standard fractional factorial designs if the number of runs is a power of two. Otherwise, they are obtained from one initial row that is cyclically shifted to obtain all but one of the runs. The final run is $(00\ldots0)$.

21.69 Remark The alias structure of the Plackett–Burman designs can be very messy and the designs should be used with caution. See [1623, 1452], but [1022] takes a more positive approach.

21.70 Table Some small Plackett–Burman designs.

$k = 11$	11011100010
$k = 19$	1100111101010000110
$k = 23$	11111010110011001010000
$k = 35$	01011100011111011100100001010110010

21.71 A *deletion design* is obtained by deleting one or more levels from one or more factors in the original design. *Collapsing levels* is a many-to-one correspondence that maps the s levels of a factor onto $u < s$ levels.

21.72 Example Consider a 3^2 design. The treatment combinations are

$$\{(00), (01), (02), (10), (11), (12), (20), (21), (22)\}.$$

Obtain a 2×3 design by deleting the last level of the first factor, for example. This gives treatment combinations $\{(00), (01), (02), (10), (11), (12)\}$. One can also obtain a 2×3 design by collapsing the last two levels of the first factor. This gives treatment combinations $\{(00), (01), (02), (10), (11), (12), (10), (11), (12)\}$. The second approach means that the levels are no longer equally replicated but they are in proportional frequency. See §VI.39.

21.73 In a *search design* the parameters in the model are divided into two sets. One is a set of unknown parameters, all of which are to be estimated. The second is a set of parameters that is known to have at most v nonzero entries. The aim of a search design is to identify and estimate these v parameters. Any design can be used as a search design, but some layouts have better properties than others. See [461, 897].

21.74 In a *model-robust factorial design* (MRFD) the experimenter is asked for an upper bound on the number of likely interactions. An MRFD is then selected that guarantees (if possible) that any combination of up to g interactions is estimable, thus eliminating the explicit need to choose a confounding scheme. See [1446] for a discussion and several small examples.

21.75 Remark Designs may need to have more than one blocking factor; for instance, the rows and columns in a latin square may represent two directions in the field. It is then necessary to consider more elaborate confounding schemes. See [1203, 1443].

21.6 Small Factorial Designs with 2 and 3 Level Factors

21.76 Remark In this section, tables of small 2^{k-m}, 3^{k-m} and asymmetrical designs with all factors having two or three levels are given.

21.77 Table Small 2^{k-m} factorial designs. To save space the table is arranged as follows. For a given number of factors (k) and degree of fractionation (m), the treatment combinations and the defining contrast (in full, in which case the generators are the first m effects, or by giving the generators) are listed, and the aliasing for the small order interactions is indicated. The resolution and the wordlength pattern are also given. Theorem 21.55 was used to generate the designs. Also indicated are a subdivision of the treatment combinations for the fractional design into blocks and (at least the generators of) the corresponding confounded effects. The treatments in the smallest block size, usually 4, are separated by semicolons; larger blocks are obtained by grouping together an appropriate number of the blocks of size 4, starting from the left-hand side of the first line. The tables can also be used to construct incomplete blocks for a complete factorial. In this context the defining contrast is the set of confounded effects, and a set of coset representatives is given to obtain the other blocks of the design (see Remark 21.30). To save space ab denotes $(1, 1, 0, \ldots, 0)$ and AB denotes $\mathrm{P}(1, 1, 0, \ldots, 0)$. No designs requiring more than 64 treatment combinations have been given. Larger designs can be found in [1581].

$k = 3$
$m = 1$, $R = 3$, wordlength pattern = (0, 0, 1)
Defining contrast: $I \equiv ABC$
Aliasing: $A \equiv BC$, $B \equiv AC$, $C \equiv AB$
Treatment combinations: $(1), ab, ac, bc$
Coset representatives: a

$k = 4$
$m = 1$, $R = 4$, wordlength pattern = (0, 0, 0, 1)
Defining contrast: $I \equiv ABCD$
Aliasing: $A \equiv BCD$, $B \equiv ACD$, $C \equiv ABD$, $D \equiv ABC$, $AB \equiv CD$, $AC \equiv BD$, $AD \equiv BC$
Treatment combinations: $(1), ab, cd, abcd$; ac, ad, bd, bc
Coset representatives: a
Blocks of size 4: $AB \equiv CD$

$k = 4$
$m = 2$, $R = 2$, wordlength pattern = (0, 1, 2, 0)
Defining contrast: $I \equiv AC \equiv ABD \equiv BCD$
Aliasing: $A \equiv C \equiv BD \equiv ABCD$, $B \equiv ABC \equiv AD \equiv CD$, $D \equiv ACD \equiv AB \equiv BC$
Treatment combinations: $(1), abc, bd, acd$
Coset representatives: a, b, c

$k = 5$
$m = 1$, $R = 5$, wordlength pattern = (0, 0, 0, 0, 1)
Defining contrast: $I \equiv ABCDE$

Aliasing: main effects with 4 factor interactions, 2 factor interactions with 3 factor interactions
Treatment combinations: $(1), abcd, abce, de;\ ab, cd, abde, ce;\ ac, bd, be, acde;$
$ad, bc, ae, bcde$
Coset representatives: a
Blocks of size 8: $AB \equiv CDE$
Blocks of size 4: $AB \equiv CDE$, $AC \equiv BDE$, $BC \equiv ADE$

$k = 5$
$m = 2$, $R = 3$, wordlength pattern = (0, 0, 2, 1, 0)
Defining contrast: $I \equiv ABD \equiv BCE \equiv ACDE$
Aliasing: $A \equiv BD \equiv ABCE \equiv CDE$, $B \equiv AD \equiv CE \equiv ABCDE$,
$C \equiv ABCD \equiv BE \equiv ADE$, $D \equiv AB \equiv BCDE \equiv ACE$,
$E \equiv ABDE \equiv BC \equiv ACD$, $AC \equiv BCD \equiv ABE \equiv DE$, $AE \equiv BDE \equiv ABC \equiv CD$
Treatment combinations: $(1), bcd, acde, abe;\ ce, bde, ad, abc$
Coset representatives: a, b, c
Blocks of size 4: $AE \equiv BDE \equiv ABC \equiv CD$

$k = 5$
$m = 3$, $R = 2$, wordlength pattern = (0, 2, 4, 1, 0)
Defining contrast: $I \equiv CD \equiv BDE \equiv ADE \equiv BCE \equiv AB \equiv ACE \equiv ABCD$
Aliasing: $A \equiv ACD \equiv ABDE \equiv DE \equiv ABCE \equiv B \equiv CE \equiv BCD$,
$C \equiv D \equiv BCDE \equiv ACDE \equiv BE \equiv ABC \equiv AE \equiv ABD$,
$E \equiv CDE \equiv BD \equiv AD \equiv BC \equiv ABE \equiv AC \equiv ABCDE$,
Treatment combinations: $(1), cde, abe, abcd$
Coset representatives: a, b, c, d, e, ac, ad

$k = 6$
$m = 1$, $R = 6$, wordlength pattern = (0, 0, 0, 0, 0, 1)
Defining contrast: $I \equiv ABCDEF$
Aliasing: main effects with 5 factor interactions, 2 factor interactions with 4 factor interactions, 3 factor interactions with 3 factor interactions
Treatment combinations: $(1), bcde, acdf, abef;\ ab, ef, acde, bcdf;\ bc, de, abdf, acef;$
$ac, df, abde, bcef;\ bd, adef, ce, abcf;\ ad, abce, cf, bdef;\ cd, af, be, abcdef;$
$abcd, ae, bf, cdef$
Coset representatives: a
Blocks of size 16: $ABC \equiv DEF$
Blocks of size 8: $ABC \equiv DEF$, $ABD \equiv CEF$, $CD \equiv ABEF$
Blocks of size 4: As for 8 and $ACE \equiv BDF$, $ADE \equiv BCF$, $AF \equiv BCDE$,
$BE \equiv ACDF$

$k = 6$
$m = 2$, $R = 4$, wordlength pattern = (0, 0, 0, 3, 0, 0)
Defining contrast: $I \equiv ABCE \equiv BCDF \equiv ADEF$
Aliasing: $A \equiv BCE \equiv ABCDF \equiv DEF$, $B \equiv ACE \equiv CDF \equiv ABDEF$, other main effects similarly. $AB \equiv CE \equiv ACDF \equiv BDEF$, other interactions by multiplication.
Treatment combinations: $(1), bcdf, adef, abce;\ cef, bde, acd, abf;\ abcdef, df, bc, ae;$
cde, bef, acf, abd
Coset representatives: a, b, d
Blocks of size 8: $ABD \equiv CDE \equiv ACF \equiv BEF$
Blocks of size 4: As for 8 and $ABF \equiv CEF \equiv ACD \equiv BDE$,
$DF \equiv ABCDEF \equiv BC \equiv AE$

$k = 6$
$m = 3$, $R = 3$, wordlength pattern = (0, 0, 4, 3, 0, 0)
Defining contrast: $I \equiv CDF \equiv BDE \equiv ADEF \equiv BCEF \equiv ABF \equiv ACE \equiv ABCD$
Aliasing: $A \equiv ACDF \equiv ABDE \equiv DEF \equiv ABCEF \equiv BF \equiv CE \equiv BCD$, others by multiplication
Treatment combinations: $(1), bcef, adef, abcd;\ cde, bdf, acf, abe$
Coset representatives: a, b, c, d, e, f, ad
Blocks of size 4: $AD \equiv ACF \equiv ABE \equiv EF \equiv ABCDEF \equiv BDF \equiv CDE \equiv BC$

$k = 6$
$m = 4$, $R = 2$, wordlength pattern = (0, 3, 8, 3, 0, 1)
Defining contrast: $I \equiv AF \equiv BE \equiv CEF \equiv DEF \equiv ABEF \equiv BCF \equiv ACE \equiv ABC \equiv CD \equiv BDF \equiv ADE \equiv ABD \equiv BCDE \equiv ACDF \equiv ABCDEF$
Aliasing: Main effects A and F, B and E and C and D are aliased
Treatment combinations: $(1), bcde, acdf, abef$
Coset representatives: $a, b, c, d, e, f, ab, ac, ad, ae, af, bc, bd, abc, abd$

$k = 7$
$m = 1$, $R = 7$, wordlength pattern = (0, 0, 0, 0, 0, 0, 1)
Defining contrast: $I \equiv ABCDEFG$
Aliasing: Main effects with 6 factor interactions, 2 factor interactions with 5 factor interactions and 3 factor interactions with 4 factor interactions
Treatment combinations: $(1), aceg, bcde, acdf, abdg, defg, bcfg, abef;\ acef, bc, de, abeg, abdf, acdg, fg, bcdefg;\ ac, abde, bcdg, eg, acdefg, bcef, abfg, df;\ acfg, acde, bcdf, dg, bceg, abdefg, ef, ab;\ abcd, ae, adfg, cg, bf, bdeg, abcefg, cdef;\ ad, abce, cf, bg, aefg, cdeg, abcdfg, bdef;\ bd, ce, abcf, ag, befg, abcdeg, cdfg, adef;\ cd, be, adeg, abcg, cefg, af, bdfg, abcdef$
Coset representatives: a
Blocks of size 32: $ABC \equiv DEFG$
Blocks of size 16: As for 32 and $ADE \equiv BCFG$, $AFG \equiv BCDE$
Blocks of size 8: As for 16 and $BDF \equiv ACEG$, $BEG \equiv ACDF$, $CDG \equiv ABEF$, $CEF \equiv ABDG$
Blocks of size 4: Best aliasing from, giving generators only, $ABC \equiv DEFG$, $ADE \equiv BCFG$, $ABE \equiv CDFG$, $ABG \equiv CDEF$. Two factor interactions CE, BD, CG, BF, EG, DF not estimable. Blocks are not given but can be calculated from the aliasing relationship.

$k = 7$
$m = 2$, $R = 4$, wordlength pattern = (0, 0, 0, 1, 2, 0, 0)
Defining contrast: $I \equiv ABCF \equiv BCDEG \equiv ADEFG$
Aliasing: Main effects with 3 and 4 factor interactions; some 2 factor interactions are aliased (eg AB and CF)
Treatment combinations: $(1), abcf, bdefg, acdeg;\ cef, abe, bcdg, adfg;\ eg, abcefg, bdf, acd; cfg, abg, bcde, adef;\ de, abcdef, bfg, acg;\ cdf, abd, bceg, aefg;\ dg, abcdfg, bef, ace;\ cdefg, abdeg, bc, af$
Coset representatives: a, b, d
Blocks of size 16: $ABD \equiv CDF \equiv ACEG \equiv BEFG$
Blocks of size 8: As for 16 and $CFG \equiv ABG \equiv BDEF \equiv ACDE$, $ABCDFG \equiv DG \equiv AEF \equiv BCE$
Blocks of size 4: As for 8 and $AC \equiv BF \equiv ABDEG \equiv CDEFG$ and generalized interactions.

$k = 7$
$m = 3$, $R = 4$, wordlength pattern = (0, 0, 0, 7, 0, 0, 0)
Defining contrast: $I \equiv CDFG \equiv BDEG \equiv ADEF$ (generators only)
Aliasing: Main effects with 3 factor interactions, 2 factor interactions with each other.
Treatment combinations: $(1), efg, abcd, abcdefg$; $cdfg, cde, abfg, abe$; $bdf, bdeg, acf, aceg$; $bcg, bcef, adg, adef$
Coset representatives: a, b, c, d, e, f, g
Blocks of size 8: $CD \equiv FG \equiv BCEG \equiv ACEF$
Blocks of size 4: As for 8 and $BD \equiv BCFG \equiv EG \equiv ABEF$, $BC \equiv BDFG \equiv CDEG \equiv ABCDEF$

$k = 7$
$m = 4$, $R = 3$, wordlength pattern = (0, 0, 7, 7, 0, 0, 1)
Defining contrast: $I \equiv AFG \equiv BEG \equiv CEF \equiv DEFG$ (generators only)
Aliasing: Main effects with 2 factor interactions
Treatment combinations: $(1), defg, bcfg, bcde, aceg, acdf, abef, abdg$
Coset representatives: $a, b, c, d, e, f, g, ab, ac, ad, ae, af, ag, bc, abc$

$k = 8$
$m = 2$, $R = 5$, wordlength pattern= (0, 0, 0, 0, 2, 1, 0, 0)
Defining contrast: $I \equiv ABCDG \equiv CDEFH \equiv ABEFGH$
Aliasing: Main effects with 4 and 5 factor interactions, 2 factor interactions with 3 and 4 factor interactions
Treatment combinations: $(1), bcdegh, adefh, abcfg$; $dfg, bcefh, aegh, abcd$; $ceg, bdh, acdfgh, abef$; $abdeg, cdef, bfgh, ach$; $dgh, bce, aefg, abcdfh$; $fh, bcdefg, ade, abcgh$; $cdeh, bg, acf, abdefgh$; $cefgh, bdf, acdg, abeh$; $eh, bcdg, adf, abcefgh$; $abcdeh, defgh, bcf, ag$; $cgh, bde, acdefg, abfh$; $abdgh, cdfh, befg, ace$; $deg, bch, afgh, abcdef$; $ef, bcdfgh, adh, abceg$; $cd, begh, acefh, abdfg$; $acdegh, cfg, bdefh, ab$
Coset representatives: a, c, e
Blocks of size 32: $ACE \equiv BDEG \equiv ADFH \equiv BCFGH$
Blocks of size 16: As for 32 and $BDF \equiv ACFG \equiv BCEH \equiv ADEGH$, $ABCDEF \equiv EFG \equiv ABH \equiv CDGH$
Blocks of size 8: As for 16 and $BC \equiv ADG \equiv BDEFH \equiv ACEFGH$ (and generalized interactions)
Blocks of size 4: As for 8 and $AF \equiv BCDFG \equiv ACDEH \equiv BEGH$ (and generalized interactions)

$k = 8$
$m = 3$, $R = 4$, wordlength pattern = (0, 0, 0, 3, 4, 0, 0, 0)
Defining contrast: $I \equiv CDFG \equiv BDEG \equiv ADEFH$ (generators only)
Aliasing: Main effects with interactions with at least 3 factors, 2 factor interactions with interactions with at least 2 factors
Treatment combinations: $(1), bcef, acdfgh, abdegh$; $abcd, cegh, bfgh, adef$; $abcdefg, cfh, beh, adg$; $acdeh, abdfh, efg, bcg$; $dgh, bcdefgh, acf, abe$; $abcgh, cde, bdf, aefgh$; $abcefh, cdfg, bdeg, ah$; $aceg, abfg, defh, bcdh$
Coset representatives: a, b, c, d, e, f, g
Blocks of size 16: $BCH \equiv BDFGH \equiv CDEGH \equiv ABCDEF$
Blocks of size 8: As for 16 and $ABF \equiv ABCDG \equiv ADEFG \equiv BDEH$ (and generalized interactions)
Blocks of size 4: As for 8 and $DG \equiv CF \equiv BE \equiv AEFGH$ (and generalized interactions)

$k = 8$
$m = 4$, $R = 4$, wordlength pattern = (0, 0, 0, 14, 0, 0, 0, 1)
Defining contrast: $I \equiv AFGH \equiv BEGH \equiv CEFH \equiv DEFG$ (generators only)
Aliasing: Main effects with interactions with at least 3 factors, 2 factor interactions with each other
Treatment combinations: $(1), bcde, afgh, abcdefgh$; $cdgh, begh, acdf, abef$; $cefh$, $bdfh, aceg, abdg$; $abch, defg, bcfg, adeh$
Coset representatives: $a, b, c, d, e, f, g, h, ab, ac, ad, ae, af, ag, ah$
Blocks of size 8: $AF \equiv GH \equiv ABEFGH \equiv ACEH \equiv ADEG$ (and generalized interactions)
Blocks of size 4: As for 8 and $AG \equiv FH \equiv ABEH \equiv ACEFGH \equiv ADEF$ (and generalized interactions)

$k = 9$
$m = 3$, $R = 4$, wordlength pattern = (0, 0, 0, 1, 4, 2, 0, 0, 0)
Defining contrast: $I \equiv CDFG \equiv BDEGJ \equiv ADEFH$ (generators only)
Aliasing: Main effects with interactions with at least 3 factors, 2 factor interactions with interactions with at least 2 factors
Treatment combinations: $(1), cdfg, befgj, bcdej, adeghj, acefhj, abdfh, abcgh$; $abcfj$, $fghj, cdhj, beh, bcdefgh, adef, aceg, abdgj$; $dfj, cgj, bdeg, bcef, aefgh, acdeh, abhj$, $abcdfghj$; $dgh, cfh, bdefhj, bceghj, aej, acdefgj, abfg, abcd$; $efg, cde, bj, bcdfgj, adfhj$, $acghj, abdegh, abcefh$; $ehj, cdefghj, bfgh, bcdh, adg, acf, abdefj, abcegj$; $degj, cefj$, $bdf, bcg, ah, acdfgh, abefghj, abcdehj$;
$abcdefg, defh, cegh, bdghj, bcfhj, afgj, acdj, abe$
Coset representatives: a, b, c, d, e, f, g
Blocks of size 32: $ABE \equiv ABCDEFG \equiv ADGJ \equiv BDFH$ (and generalized interactions)
Blocks of size 16: As for 32 and $ACD \equiv AFG \equiv ABCEGJ \equiv CEFH$ (and generalized interactions)
Blocks of size 8: As for 16 and $AH \equiv ACDFGH \equiv ABDEGHJ \equiv DEF$ (and generalized interactions)

$k = 9$
$m = 4$, $R = 4$, wordlength pattern = (0, 0, 0, 6, 8, 0, 0, 1, 0)
Defining contrast: $I \equiv AFGHJ \equiv BEGHJ \equiv CEFH \equiv DEFG$ (generators only)
Aliasing: Main effects with interactions with at least 3 factors, 2 factor interactions with interactions with at least 2 factors
Treatment combinations: $(1), efj, abcdghj, abcdefgh$; $dgj, defg, abch, abcefhj$; chj, $cefh, abdg, abdefgj$; $cdgh, cdefghj, abj, abef$; $bfghj, begh, acdf, acdej$; $bdfh, bdehj$, $acfgj, aceg$; $bcfg, bcegj, adfhj, adeh$; $bcdfj, bcde, afgh, aeghj$
Coset representatives: $a, b, c, d, e, f, g, h, j, ac, ad, ae, af, ag, ah$
Blocks of size 16: $AB \equiv BFGHJ \equiv AEGHJ \equiv ABCEFH \equiv ABDEFG$ (and generalized interactions)
Blocks of size 8: As for 16 and
$AC \equiv ACBEGHJ \equiv AEFH \equiv ACDEFG \equiv CFGHJ$ (and generalized interactions)
Blocks of size 4: As for 8 and
$AD \equiv ADBEGHJ \equiv ADCEFH \equiv AEFG \equiv DFGHJ$ (and generalized interactions)

$k = 10$
$m = 4$, $R = 4$, wordlength pattern = (0, 0, 0, 2, 8, 5, 0, 0, 0, 0)
Defining contrast: $I \equiv AFGHJ \equiv BEGHJ \equiv CEFHK \equiv DEFGK$
Aliasing: Main effects with interactions with at least 3 factors, 2 factor interactions with interactions with at least 2 factors
Treatment combinations: $(1), defg, bfghj, bdehj, acfhjk, acdeghjk, abcgk, abcdefk$; $cefh, cdgh, bcegj, bcdfj, aejk, adfgjk, abefghk, abdhk$; $cefgk, cdk, bcehjk, bcdfghjk$, $aeghj, adfhj, abef, abdg$; $ghk, defhk, bfjk, bdegjk, acfgj, acdej, abch, abcdefgh$; $efghjk, dhjk, bek, bdfgk, aceg, acdf, abcefhj, abcdghj$; $cgjk, cdefjk, bcfhk, bcdeghk$, $afgh, adeh, abj, abdefgj$; $chj, cdefghj, bcfg, bcde, afk, adegk, abghjk, abdefhjk$; efj, $dgj, begh, bdfh, acehk, acdfghk, abcefgjk, abcdjk$
Coset representatives: $a, b, c, d, e, f, g, h, j, k, ac, ad, ae, ag, ah$
Blocks of size 32: $ABJ \equiv BFGH \equiv AEGH \equiv ABCEFHJK \equiv ABDEFGJK$ (and generalized interactions)
Blocks of size 16: $DFH \equiv ADGJ \equiv BDEFGJ \equiv CDEK \equiv EGHK$ (and generalized interactions)
Blocks of size 8: $BEG \equiv ABEFHJ \equiv HJ \equiv BCFGHK \equiv BDFK$ (and generalized interactions)

21.78 Table Small 3^{k-m} factorial designs. The treatment combinations are written as k-tuples with entries of 0, 1, or 2. The values of k (the number of factors) and m (the degree of fractionation) are given. Blocks are indicated by semicolons, as in Table 21.77. Designs with 27 and 81 treatment combinations have been given. For the smaller values of k, coset representatives, to generate the other blocks of a completely randomized design, have been given. (No designs with only nine treatment combinations have been given since these designs can estimate at most four main effects.)

Designs for 27 units

$k = 4$, $m = 1$
Defining contrast: $I \equiv ABCD$
Aliasing: $A \equiv AB^2C^2D^2 \equiv BCD$ and similarly, $AB \equiv ABC^2D^2 \equiv CD$, and so on.
Treatment combinations: 0000, 0012, 0021, 1200, 2100, 1212, 2121, 1221, 2112; 0102, 0111, 0120, 1002, 2202, 1011, 2220, 1020, 2211; 0201, 0210, 2001, 2010, 0222, 2022, 1101, 1110, 1122.
Coset representatives: 1000, 2000
Blocks of size 9: $AB \equiv ABC^2D^2 \equiv CD$

$k = 5$, $m = 2$
Defining contrast: $I \equiv ABC \equiv CDE$
Aliasing: $A \equiv AB^2C^2 \equiv ACDE$, and so on.
Treatment combinations: 00000, 11111, 22222; 01222, 12000, 20111; 02111, 10222, 21000; 00012, 11120, 22201; 01201, 12012, 20120; 02120, 10201, 21012; 00021, 11102, 22210; 01210, 12021, 20102; 02102, 10210, 21021
Coset representatives: 10000, 20000, 00100, 00200, 00010, 00020, 10100, 00110
Blocks of size 9: ABD
Blocks of size 3: ABD, ADE

$k = 6$, $m = 3$
Defining contrast: $I \equiv ABC \equiv ADE \equiv BDF$
Aliasing: $A \equiv AB^2C^2 \equiv AD^2E^2 \equiv ABDF$, and so on.

Treatment combinations: 000000, 111111, 222222; 012121, 120202, 201010; 021212, 102020, 210101; 000122, 111200, 222011; 012210, 120021, 201102; 021001, 102112, 210220; 000211, 111022 , 222100; 012002, 120110, 201221; 021120, 102201, 210012
Coset representatives: 100000, 200000, 010000, 020000, 001000, 002000, 000100, 000200, 000010, 000020, 000001, 000002, 110000, 101000, 100100, 100010, 100001, 011000, 010100, 010001, 000110, 000101, 220000, 200200, 200002, 200001
Blocks of size 9: ACD
Blocks of size 3: ACD, AF^2

$k = 7$, $m = 4$
Defining contrast: $I \equiv ABC \equiv ADE \equiv BDF \equiv CEG$
Aliasing: $A \equiv AB^2C^2 \equiv AD^2E^2 \equiv ABDF \equiv ACEG$, and so on.
Treatment combinations: 0000000, 1111111, 2222222; 0121212, 1202020, 2010101; 0212121, 1020202, 2101010; 0001221, 1112002, 2220110; 0122100, 1200211, 2011022; 0210012, 1021120, 2102201; 0002112, 1110220, 2221001; 0120021, 1201102, 2012210; 0211200, 1022011, 2100122
Blocks of size 9: ABG
Blocks of size 3: ABG, A^2F

$k = 8$, $m = 5$
Defining contrast: $I \equiv ABC \equiv ADE \equiv BDF \equiv CEG \equiv CDFH$
Aliasing: $A \equiv AB^2C^2 \equiv AD^2E^2 \equiv ABDF \equiv ACEG \equiv ACDFH$, and so on.
Treatment combinations: 00000000, 01212122, 02121211, 10202021, 11111110, 12020202, 20101012, 21010101, 22222220; 00012210, 01221002, 02100121, 10211201, 11120020, 12002112, 20110222, 21022011, 22201100; 00021120, 01200212, 02112001, 10220111, 11102200, 12011022, 20122102, 21001221, 22210010
Blocks of size 9: A^2FH

$k = 9$, $m = 6$
Defining contrast: $I \equiv ABC \equiv ADE \equiv BDF \equiv CEG \equiv CDFH \equiv ABEJ$
Aliasing: $A \equiv AB^2C^2 \equiv AD^2E^2 \equiv ABDF \equiv ACEG \equiv ACDFH \equiv AF^2G^2J^2$, and so on.
Treatment combinations: 000000000, 000122101, 000211202, 012002122, 012121220, 012210021, 021001211, 021120012, 021212110, 102020210, 102112011, 102201112, 111022002, 111111100, 111200201, 120021121, 120110222, 120202020, 201010120, 201102221, 201221022, 210012212, 210101010, 210220111, 222011001, 222100102, 222222200

Designs for 81 units

$k = 5$, $m = 1$
Defining contrast: $I \equiv ABCDE$
Aliasing: $A \equiv AB^2C^2D^2E^2$, and so on.
Treatment combinations: 00000, 10122, 20211; 01110, 11202, 21021; 02220, 12012, 22101; 00012, 10101, 20220; 01122, 11211, 21000; 02202, 12021, 22110; 00021, 10110, 20202; 01101, 11220, 21012; 02211, 12000, 22122; 00102, 10221, 20010; 01212, 11001, 21120; 02022, 12111, 22200; 00111, 10200, 20022; 01221, 11010, 21102; 02001, 12120, 22212; 00120, 10212, 20001; 01200, 11022, 21111; 02010, 12102, 22221; 00201, 10020, 20112; 01011, 11100, 21222; 02121, 12210, 22002; 00210, 10002, 20121; 01020, 11112, 21201; 02100, 12222, 22011; 00222, 10011, 20100; 01002, 11121, 21210; 02112, 12201, 22020
Coset representatives: 10000, 20000
Blocks of size 27:ABC^2

Blocks of size 9: ABC^2, ACD^2
Blocks of size 3: ABC^2, ACD^2, ABD

$k = 6$, $m = 2$
Defining contrast: $I \equiv ABCD \equiv AB^2EF$
Aliasing: $A \equiv AB^2C^2D^2 \equiv ABE^2F^2$, and so on.
Treatment combinations: 000000, 112212, 221121; 010201, 122110, 201022; 020102, 102011, 211220; 001212, 110121, 222000; 011110, 120022, 202201; 021011, 100220, 212102; 002121, 111000, 220212; 012022, 121201, 200110; 022220, 101102, 210011; 000012, 112221, 221100; 010210, 122122, 201001; 020111, 102020, 211202; 001221, 110100, 222012; 011122, 120001, 202210; 021020, 100202, 212111; 002100, 111012, 220221; 012001, 121210, 200122; 022202, 101111, 210020; 000021, 112200, 221112; 010222, 122101, 201010; 020120, 102002, 211211; 001212, 110112, 222021; 011101, 120010, 202222; 021002, 100211, 212120; 002100, 111021, 220200; 012010, 121222, 200101; 022211, 101120, 210002
Coset representatives: 100000, 200000, 010000, 020000, 001000, 002000, 000010, 000020
Blocks of size 27: AC^2E
Blocks of size 9: AC^2E, AC
Blocks of size 3: AC^2E, AC, EF

$k = 7$, $m = 3$
Defining contrast: $I \equiv ABCDE \equiv ACDE^2FG^2 \equiv AC^2DE^2G$
Aliasing: $A \equiv AB^2C^2D^2E^2 \equiv AC^2D^2EF^2G \equiv ABC^2DE^2G$, and so on.
Treatment combinations: 0000000, 1111212, 2222121; 0122100, 1200012, 2011221; 0211200, 1022112, 2100021; 0010210, 1121122, 2202001; 0102010, 1210222, 2021101; 0221110, 1002022, 2110201; 0020120, 1101002, 2212211; 0112220, 1220102, 2001011; 0201020, 1012202, 2120111; 0001202, 1112111, 2220020; 0120002, 1201211, 2012120; 0212102, 1020011, 2101220; 0011112, 1122021, 2200200; 0100212, 1211121, 2022000; 0222012, 1000221, 2111100; 0021022, 1102201, 2210110; 0110122, 1221001, 2002210; 0202222, 1010101, 2121010; 0002101, 1110010, 2221222; 0121201, 1202110, 2010022; 0210001, 1021210, 2102122; 0012011, 1120220, 2201102; 0101111, 1212020, 2020202; 0220211, 1001120, 2112002; 0022221, 1100100, 2211012; 0111021, 1222200, 2000112; 0200121, 1011000, 2122212
Blocks of size 27: AG
Blocks of size 9: AG, FG
Blocks of size 3: AG, FG, CG

$k = 8$, $m = 4$
Defining contrast: $I \equiv ABCDEFGH \equiv AB^2CE^2G \equiv BCEF^2G \equiv ACD^2E^2FG^2$
Aliasing: $A \equiv AB^2C^2D^2E^2F^2G^2H^2 \equiv ABC^2EG^2 \equiv ABCEF^2G \equiv AC^2DEF^2G$, and so on.
Treatment combinations: 00000000, 12212112, 21121221; 00001212, 12210021, 21122100; 00002121, 12211200, 21120012; 01100202, 10012011, 22221120; 01101111, 10010220, 22222002; 01102020, 10011102, 22220211; 02200101, 11112210, 20021022; 02201010, 11110122, 20022201; 02202222, 11111001, 20020110; 00120021, 12002100, 21211212; 00121200, 12000012, 21212121; 00122112, 12001221, 21210000; 01220220, 10102002, 22011111; 01221102, 10100211, 22012020; 01222011, 10101120, 22010202; 02020122, 11202201, 20111010; 02021001, 11200110, 20112222; 02022210, 11201022, 20110101; 00210012, 12122121, 21001200; 00211221, 12120000, 21002112; 00212100, 12121212, 21000021; 01010211, 10222020, 22101102; 01011120, 10220202, 22102011; 01012002, 10221111, 22100220; 02110110, 11022222, 20201001; 02111022, 11020101,

20202210; 02112201, 11021010, 20200122
Blocks of size 27: AB^2CD^2
Blocks of size 9: AB^2CD^2, AB
Blocks of size 3: AB^2CD^2, AB, BH^2

$k = 9$, $m = 5$
Defining contrast:
$I \equiv ABCDEF \equiv ABD^2E^2G^2 \equiv AB^2C^2EG^2 \equiv AC^2DE^2GJ \equiv BC^2D^2EGH$
Aliasing:
$A \equiv AB^2C^2D^2E^2F^2 \equiv AB^2DEG \equiv ABCE^2G \equiv ACD^2EG^2J^2 \equiv ABC^2D^2EGH$, and so on.
Treatment combinations: 000000000, 110121221, 220212112; 001212020, 111000211, 221121102; 002121010, 112212201, 222000122; 010122100, 120210021, 200001212; 011001120, 121122011, 201210202; 012210110, 122001001, 202122222; 020211200, 100002121, 210120012; 021120220, 101211111, 211002002; 022002210, 102120101, 212211022; 000111122, 110202010, 220020201; 001020112, 111111000, 221202221; 002202102, 112020020, 222111211; 010200222, 120021110, 200112001; 011112212, 121200100, 201021021; 012021202, 122112120, 202200011; 020022022, 100110210, 210201101; 021201012, 101022200, 211110121; 022110002, 102201220, 212022111; 000222211, 110010102, 220101020; 001101201, 111222122, 221010010; 002010221, 112101112, 222222000; 010011011, 120102202, 200220120; 011220001, 121011222, 201102110; 012102021, 122220212, 202011100; 020100111, 100221002, 210012220; 021012101, 101100022, 211221210; 022221121, 102012012, 212100200
Blocks of size 27: ABG^2
Blocks of size 9: ABG^2, BG
Blocks of size 3: ABG^2, BG, HJ

21.79 Table Small $2^{k_1} \times 3^{k_2}$ designs.

$k = 2$
2×3
Possible block sizes are 3 (which would confound A) or 2 (which would confound B).

$k = 3$
$2^2 \times 3$
Possible block sizes are 6, so AB is confounded (and hence $A \equiv B$ in a fractional plan); 4, where C is confounded; 3, where all information about the two-level factors is lost.
Blocks of size 6: generator: (111); coset representatives: (100)
2×3^2
Possible block sizes are 9, where A is confounded; 6, so 2 degrees of freedom of the two-factor interaction BC is lost and in a fractional design $B \equiv C$; 3, 3, where A and AB or AC are confounded.
Blocks of size 6: generator: (111); coset representatives: (010), (020).

$k = 4$
$2^3 \times 3$
Possible block sizes are: 12, 8, 6, 4 and 3. For 8 and 4, D is confounded with blocks. For 3, the main effects of A, B, C are all confounded with blocks.
Blocks of size 12: confound $I \equiv ABC$; aliasing: $A \equiv BC$, $D \equiv ABCD$; generators: (1100), (1011); coset representative: (1000).

Blocks of size 6: confound: $I \equiv AB \equiv AC$; aliasing: $A \equiv B \equiv C$ (so a fraction should not be used); generator: (1111); coset representatives: (1000), (1100), (0100).
$2^2 \times 3^2$
Possible block sizes are: 18, 12, 9, 6, 4 and 3. For 9, 4 and 3 some main effects must be confounded with blocks.
Blocks of size 18: confound: $I \equiv AB$; aliasing: $A \equiv B$ (so a fraction should not be used); generators: (1110), (0001); coset representative: (1000).
Blocks of size 12: confound: $I \equiv CD$; aliasing: $C \equiv D$ (so a fraction should not be used); generators: (1012), (0100); coset representatives: (0010), (0020).
Blocks of size 6: confound: $I \equiv AB \equiv CD$; aliasing: $A \equiv B$ (so a fraction should not be used); generator: (1112); coset representatives: (1000), (0010), (0020), (1010), (1020).
2×3^3
Possible block sizes are: 27, 18, 9, 6. For 27 and 9 information on some main effects is confounded.
Blocks of size 18: confound $I \equiv BCD$; aliasing: $A \equiv ABCD$, $B \equiv BC^2D^2$; generators: (1111), (0120); coset representatives: (0100), (0200).
Blocks of size 6: confound: $I \equiv BC \equiv CD$; aliasing: $B \equiv C \equiv D$ (so a fraction should not be used); generator: (1120); coset representatives: (0100, (0200), (0001), (0002), (0101), (0202), (0201), (0102).

$k = 5$
$2^4 \times 3$
Possible blocks sizes are: 24, 16, 12, 8, 6. For 16 and 8 the main effect of E is confounded with blocks.
Blocks of size 24: confound: $I \equiv ABCD$; aliasing: $A \equiv BCD$, $E \equiv ABCDE$; generators: (11001), (00110), (10100); coset representative: (10000) .
Blocks of size 12: confound: $I \equiv AB \equiv CD \equiv ABCD$; aliasing: $A \equiv B \equiv ACD \equiv BCD$ (so a fraction should not be used); generators: (11001), (00110) ; coset representatives: (10000), (00100), (10100).
Blocks of size 6: confound: $I \equiv AB \equiv AC \equiv AD$ (generators only); aliasing: $A \equiv B \equiv C \equiv D$ (so a fraction should not be used); generator: (11111); coset representatives: (10000), (11000), (01000), (10100), (00100), (10010), (00010).
$2^3 \times 3^2$
Possible blocks sizes are: 36, 24, 18, 12, 9, 8. For 9 and 8 main effects are confounded with blocks.
Blocks of size 36: confound: $I \equiv ABC$; aliasing: $A \equiv BC$, $D \equiv ABCD$; generators: (11010), (10101); coset representative: (10000).
Blocks of size 24: confound: $I \equiv DE$; aliasing: $D \equiv E$ (so a fraction should not be used); generators: (10012), (01000), (00100); coset representatives: (00010), (00020).
Blocks of size 18: confound: $I \equiv AB \equiv AC \equiv BC$; aliasing: $A \equiv B \equiv C \equiv ABC$ (so a fraction should not be used); generators: (11110), (00001); coset representatives: (10000), (01000), (11000).
Blocks of size 12: confound: $I \equiv ABC \equiv DE$; aliasing: $A \equiv BC \equiv ADE$, $D \equiv ABCD \equiv E$ (so a fraction should not be used); generators: (11000), (10112); coset representatives: (00010), (00020), (10000), (10010), (10020).
$2^2 \times 3^3$
Possible blocks sizes are: 54, 36, 27, 18, 12. Only 36 does not alias main effects in a fraction.
Blocks of size 36: confound: $I \equiv CDE$; aliasing: $A \equiv ACDE \equiv AC^2D^2E^2$, $C \equiv CD^2E^2$; generators: (10111), (01120).

2×3^4
Possible blocks sizes are: 81, 54, 27, 18. For all but 54, main effects are confounded or aliased.
Blocks of size 54: confound: $I \equiv BCDE$; aliasing: $A \equiv ABCDE \equiv AB^2C^2D^2E^2$, $B \equiv BC^2D^2E^2 \equiv CDE$; generators: (11200), (00012), (01110).

See Also

§III.6	Orthogonal arrays of higher index.
§III.7	Orthogonal arrays of higher strength.
§VI.39	Orthogonal main effect plans.
§VII.2	Finite geometry.
[136, 594, 1316]	More on factorial designs and groups.
[177]	Confounding through blocking rather than through rings.
[1516]	More details on deletion designs.
[1724]	An example where Taguchi's methods fail.

References Cited: [91, 126, 136, 177, 276, 314, 461, 472, 473, 485, 490, 491, 511, 594, 805, 829, 830, 833, 897, 1021, 1022, 1203, 1240, 1310, 1316, 1317, 1363, 1365, 1443, 1446, 1452, 1477, 1490, 1516, 1581, 1623, 1641, 1642, 1661, 1724, 1767, 1981, 1984, 2078, 2175]

22 Frequency Squares and Hypercubes

Charles F. Laywine
Gary L. Mullen

22.1 Definitions and Enumeration

22.1 Let $S = \{s_1, s_2, \ldots, s_m\}$ be a set of distinct symbols. A *frequency square* (F-square) $F(n; \lambda_1, \lambda_2, \ldots, \lambda_m)$ of *order* n on S with *frequency vector* $(\lambda_1, \lambda_2, \ldots, \lambda_m)$ is an $n \times n$ array in which symbol $s_i, i = 1, 2, \ldots, m$ occurs exactly λ_i times in each row and column. The order $n = \lambda_1 + \cdots + \lambda_m$.

22.2 An F-square $F(n; \lambda_1, \ldots, \lambda_m)$ is in *standard form* if, in the first row and column, all occurrences of s_i precede those of s_j whenever $i < j$.

22.3 **Remark** Let L be a latin square on n symbols and let $S_1, S_2, \ldots, S_m$ be a partition of the symbol set with $|S_i| = \lambda_i$. If every symbol in S_i is replaced by a new symbol s_i, then the resulting square is an F-square $F(n; \lambda_1, \ldots, \lambda_m)$.

22.4 **Remark** If $\lambda_1 = \lambda_2 = \cdots = \lambda_m = \lambda$, then $F(n; \lambda_1, \ldots, \lambda_m)$ is denoted by $F(n; \lambda)$.

22.5 **Theorem** [685] Let $F(n; \lambda_1, \ldots, \lambda_m)$ and $f(n; \lambda_1, \ldots, \lambda_m)$ be respectively the number of F-squares and the number of standard form F-squares of order n with frequency vector $(\lambda_1, \ldots, \lambda_m)$. Then $F(n; \lambda_1, \ldots, \lambda_m) = \dfrac{n!(n-1)!f(n; \lambda_1, \ldots, \lambda_m)}{\lambda_1!(\lambda_1 - 1)!(\lambda_2!)^2 \ldots (\lambda_m!)^2}$.

22.2 Orthogonality

22.6 Two F-squares $F_1(n; \lambda_1, \ldots, \lambda_m)$ and $F_2(n; \mu_1, \ldots, \mu_k)$ based respectively on symbol sets $S = \{s_1, \ldots, s_m\}$ and $T = \{t_1, \ldots, t_k\}$ are *orthogonal* if each ordered pair (s_i, t_j) occurs exactly $\lambda_i \mu_j$ times when F_1 is superimposed on F_2.

22.7 In an *orthogonal set* of F-squares (MOFS) every pair of F-squares is orthogonal.

22.8 Remark If $F_1(n; 1)$ is orthogonal to $F_2(n; 1)$, then F_1 and F_2 are orthogonal latin squares.

22.9 Remark If two F-squares F_1 and F_2 are constructed from a pair of orthogonal latin squares by the method given in Remark 22.3, then F_1 and F_2 are orthogonal F-squares.

22.10 Theorem [685] Let $F_1, F_2, \ldots, F_t$ be a set of MOFS of order n based respectively on $m_1, m_2, \ldots, m_t$ symbols. Then t satisfies the relation $\sum_{i=1}^{t} m_i - t \leq (n-1)^2$.

22.11 If equality holds in Theorem 22.10, then the set of MOFS is *complete*.

22.12 Remark If $F_1, F_2, \ldots, F_t$ are all of type $F(n; \lambda)$ and form a complete set, then $t = (n-1)^2/((n/\lambda) - 1)$.

22.13 Theorem For m a prime power and $h \geq 1$, there exists a complete set of MOFS of type $F(m^h; m^{h-1})$. These may be constructed

1. from symmetric factorial designs [1073];
2. from linear permutation polynomials in $2h$ indeterminates over the field $\mathbb{F}_m$ [1645];
3. from a complete set of MOLS of order m^h and an AD(m^{h-1}, m) (an affine resolvable design of order m and block size m^{h-1}) [1412];
4. from an AD(m^{2h-1}, m) with at least $2h-2$ independent prime classes; [1409];
5. from a complete set of MOLS of order m and an AD(m^{h-1}, m) [1408].

22.14 Remark The existence of a complete set of MOFS of type $F(m^h; m^{h-1})$ for m not a prime power is an open question; however, there is one known example of complete sets whose order is not a prime power. These are sets of type $F(4t; 2t)$, which can be constructed from a Hadamard matrix of order $4t$.

22.15 Theorem [1074] Suppose that there exists an $(s, \ell; \mu)$-difference matrix D and an orthogonal array A with parameters OA$(\lambda s^2, k, s, 2)$, such that $\lambda \mu s^3$ is a perfect square (written n^2), and such that one of the following conditions holds: (1) $\mu = \lambda s$; (2) $\lambda s^2 = \delta n$ for an integer $\delta \geq 2$ and A is (n/s)-resolvable; or (3) $\mu s = \delta n$ for an integer $\delta \geq 2$ and D is (n/s)-resolvable. Then there exists $k(\ell - 1)$ mutually orthogonal MOFS of the form $F(n; n/s)$.

22.16 Theorem [1074] The existence of k_1 mutually orthogonal $F(n; n/s)$ squares implies the existence of an orthogonal array $OA(n^2, k_1 + 2, s, 2)$. If in addition an $OA(n, k_2, s, 2)$ exists then an orthogonal array $OA(n^2, k_1 + 2k_2, s, 2)$ can be constructed.

22.17 Remark See [1414] for a table of lower bounds for the number of MOFS for orders $n \leq 100$.

22.3 Designs and Complete Sets of MOFS

22.18 Theorem If there exists a complete set of MOFS of type $F(m^h; m^{h-1})$ and an affine design AD(m^{h-1}, m), then there is an AD(m^{2h-1}, m).

22.19 Theorem [1412] Consider some bijection from the symbols of a complete set of desarguesian MOLS of order m^h to the points of the geometry $\mathrm{AG}(h, m)$. Suppose that for some parallel class in the geometry the members of each subset of m^{h-1} symbols (identified with the points in a hyperplane) are replaced by a common unique symbol in each of the $m^h - 1$ MOLS. When done for each of the $(m^h - 1)/(m - 1)$ classes, a complete set of $F(m^h; m^{h-1})$ MOFS is obtained, equivalent to the geometry $\mathrm{AG}(2h, m)$.

22.20 [247] In an $AD(m^3, m)$ affine design, a set of $\mu = m^2$ points contained in $m+1$ blocks is a *special μ-tuple*. A collection of m^2 special m^2-tuples is a *tuple class* [1410] if, collectively, they contain all m^4 points of the $AD(m^3, m)$ design. Two tuple classes are *orthogonal* if the intersection of any two special m^2-tuples, one from each class, contains exactly one point.

22.21 Theorem [1410] For m a prime power the existence of an $AD(m^3, m)$ affine design with two orthogonal m^2-tuple classes is equivalent to the existence of a complete set of MOFS of type $F(m^2; m)$.

22.22 Remark To obtain a more general relation between complete sets of $F(m^h; m^{h-1})$ MOFS and $AD(m^{2h-1}, m)$ affine designs for all $h > 2$, the concept of special μ-tuple is generalized to that of hyperspecial m^h-tuple leading to Theorem 22.23.

22.23 Theorem [1410] The existence of a complete set of MOFS of type $F(m^h; m^{h-1})$ and an $AD(m^{h-1}, m)$ affine design is equivalent to the existence of an $AD(m^{2h-1}, m)$ affine design with two orthogonal classes of hyperspecial m^h-tuples.

22.24 [1232] Let D be a design with n^2 points and μn points in each block. A *frame* of D consists of two partitions $X = \{X_1, \ldots, X_n\}$ and $Y = \{Y_1, \ldots, Y_n\}$ of the points of D into subsets of order n, such that for all $1 \le i, j \le n$:
(a) $|X_i \cap Y_j| = 1$;
(b) $|X_i \cap B| = |Y_j \cap B| = \mu$ for all blocks B.

22.25 Theorem [1232] There exists a set of r MOFS of the form $F(n; \lambda)$ if and only if there exists a framed $(m, r; \lambda^2)$-net, where $n = \lambda m$. (A net is *framed* if the corresponding design has a frame.)

22.4 Nonisomorphic Sets

22.26 Two sets of MOFS are *isomorphic* if the sets have the same number of F-squares and the squares of one set can be transformed into the squares of the second set by a series of row and column permutations on all F-squares of the first set.

22.27 Theorem [1993] There are exactly three nonisomorphic sets of MOFS of type $F(4; 2)$.

22.28 Table The three nonisomorphic complete sets of $F(4; 2)$ MOFS.

H_1 :

0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0	0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0	0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1	0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0	0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1	0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0	0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1	0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1	0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0

H_2 :

0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0	0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0	0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1	0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0	0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1	0 1 0 1 1 0 1 0 0 1 1 0 1 0 0 1	0 1 0 1 1 0 1 0 1 0 0 1 0 1 1 0	0 1 1 0 1 0 0 1 0 1 0 1 1 0 1 0	0 1 1 0 1 0 0 1 1 0 1 0 0 1 0 1

H_3 :

0 0 1 1	0 1 0 1	0 1 1 0	0 0 1 1	0 0 1 1	0 1 0 1	0 1 0 1	0 1 1 0	0 1 1 0
0 0 1 1	0 1 0 1	0 1 1 0	1 1 0 0	1 1 0 0	1 0 1 0	1 0 1 0	1 0 0 1	1 0 0 1
1 1 0 0	1 0 1 0	1 0 0 1	0 1 0 1	1 0 1 0	0 1 1 0	1 0 0 1	0 0 1 1	1 1 0 0
1 1 0 0	1 0 1 0	1 0 0 1	1 0 1 0	0 1 0 1	1 0 0 1	0 1 1 0	1 1 0 0	0 0 1 1

22.29 Table The number N of nonisomorphic complete sets of MOFS of type $F(q^h; q^{h-1})$ for q a prime power [1993].

Type	(4,2)	(8,4)	(9,3)	(16,4)	(16,8)	(25,5)
N	3	≥ 17	≥ 22	≥ 401	≥ 362	≥ 11125

22.5 Hypercubes

22.30 Let $d \geq 2$ be a fixed positive integer and let $n = m\lambda$. An $F_d(n; \lambda)$ *frequency hypercube* H is an $n \times \cdots \times n$ array $H_{(j_1,\ldots,j_d)}$ of dimension d, size n, and order m (that is, each index j_i belongs to an n-set N and the entries belong to an m-set S) with the property that when any one of the d coordinates is fixed, each of the m distinct symbols appears exactly n^{d-1}/m times in that subarray. Two such hypercubes are *orthogonal* if when superimposed, each of the m^2 possible ordered pairs occurs exactly n^d/m^2 times. A set of $r \geq 2$, $F_d(n; \lambda)$ frequency hypercubes is *orthogonal* if any two distinct hypercubes are orthogonal. More generally, a frequency hypercube $F_d(n; \lambda)$ has the *type* j, with $1 \leq j \leq d-1$, if, when any j of the d coordinates is fixed, each of the m distinct symbols appears exactly n^{d-j}/m times in that subarray.

22.31 Example [113] Three mutually orthogonal $F_3(6, 1)$s of type 2.

012345	201534	120453	534012	453201	345120
130452	013245	301524	245130	524013	452301
341520	134052	413205	052341	205134	520413
453201	345120	534012	120453	012345	201534
524013	452301	245130	301524	130452	013245
205134	520413	052341	413205	341520	134052

012345	450123	531204	345012	123450	204531
425013	134250	302541	013425	250134	541302
153420	201534	045312	420153	534201	312045
230154	542301	413025	154230	301542	025413
504231	315042	120453	231504	042315	453120
341502	023415	254130	502341	415023	130254

012345	201534	120453	453120	345012	534201
324501	432150	243015	015243	501324	150432
540132	054213	405321	321405	132540	213054
103254	310425	031542	542031	254103	425310
235410	523041	352104	104352	410235	041523
451023	145302	514230	230514	023451	302145

22.32 Remark If $j \geq 1$, a hypercube of type j is also of type $j-1$.

22.33 Remark For $d \geq 2$, an $F_d(n; 1)$ frequency hypercube of type $j \geq 1$ is a d-dimensional latin hypercube of order n. As type $j \geq 1$ increases, the latin property penetrates deeper into the hypercube. More specifically, as j increases the dimension of the smallest subarray guaranteed to be latin decreases, and thus the entire hypercube

and its subarrays obtain a more uniform structure. In the maximal case, $F_d(n;1)$ hypercubes of type $d-1$ are sometimes referred to as *permutation cubes*; see [685]. In [1308, 1763] are considered *second order* cubes, cubes with the property that each of n^2 symbols occurs exactly once in each layer of the cube.

22.34 Example Adjoining the three squares defined by $L_4(i,j,k) = i+j \pmod 6$, $L_5(i,j,k) = i+k \pmod 6$, and $L_6(i,j,k) = j+k \pmod 6$ to the set in Example 22.31 gives a set of six mutually orthogonal $F_3(6,1)$s of type 1; further adjoining the three squares defined by $L_7(i,j,k) = i$, $L_8(i,j,k) = j$, and $L_9(i,j,k) = k$ gives a set of nine mutually orthogonal $F_3(6,1)$s of type 0.

22.35 Remark An $F_2(n;1)$ hypercube is a latin square of order n; an $F_2(n;\lambda)$ hypercube is an $F(n;\lambda)$ frequency square of size n based upon m distinct symbols. Both latin squares and frequency squares, when interpreted to be frequency hypercubes, are of type 1. This follows because in any row or column each symbol occurs exactly once in a latin square and exactly $\lambda \geq 1$ times in a frequency square.

22.36 Theorem [685] When $\lambda = 1$ and $j = 1$, the existence of a set of $t-d$ mutually orthogonal hypercubes of order n, dimension, d and type 1 implies the existence of an $OA(n^d, t, n, 2)$.

22.37 Remark Theorem 22.36 can be extended to the setting of sets of mutually orthogonal frequency hypercubes.

22.38 Remark An algorithm is given in [1416] for constructing sets of orthogonal cubes from sets of orthogonal latin squares and, more generally, hypercubes of dimension $d \geq 2$ from lower dimensional objects.

22.39 Theorem [1416] Let $\lambda = 1$. If h mutually orthogonal hypercubes of order n and dimension d and ℓ MOLS of order n exist, then $h(\ell+1) + \ell d$ mutually orthogonal hypercubes of order n and dimension $d+1$ exist. In particular, if both sets are complete, the resulting set is also complete.

22.40 Theorem [1416] Let $\lambda = 1$. For $d > j > 0$, a set of k mutually orthogonal hypercubes of order n, dimension d, and type j gives $k + \binom{d}{j}$ mutually orthogonal hypercubes of order n, dimension d, and type $j-1$.

22.41 Remark [1416] When $d = 2$ and $\lambda = 1$, the converse of Theorem 22.40 also holds.

22.42 Theorem [1558] The maximum number r of mutually orthogonal frequency hypercubes of type j and of the form $F_d(n;\lambda)$ with $n = m\lambda$ is bounded above by

$$r \leq \frac{1}{m-1} \sum_{k=j+1}^{d} \binom{d}{k} (n-1)^k.$$

22.43 Remark When $n = q^e$ where q is a prime power and $e \geq 1$, a complete set of mutually orthogonal $F_d(q^e; q^{e-1})$ hypercubes of dimension d and type j can be constructed by using linear polynomials over $\mathbb{F}_q$; see [1645] for the $d = 2$ case. The following generalizes the prime power conjecture for MOLS, namely, that there exist $n-1$ MOLS of order n if and only if n is a prime power.

22.44 Conjecture There exists a complete set of mutually orthogonal $F_d(n^e; n^{e-1})$ hypercubes of dimension d and type j if and only if n is a prime power.

22.45 Remark It is natural to extend the idea of a frame from dimension $d = 2$ to an arbitrary dimension $d \geq 2$.

22.46 Theorem [1558] Let $j \geq 1$. There exists a set of r mutually orthogonal frequency hypercubes of the form $F_d(n;\lambda)$ and type j if and only if there exists a d-framed $(m, r; n^d/m^2)$-net of type j.

22.47 Remark When $\lambda = 1$, let $N_d(n)$ denote the maximum number of mutually orthogonal hypercubes of order n and dimension d, so that as noted earlier, $N_d(n) \leq (n^d-1)/(n-1)-d$. Let $n = q_1 \cdots q_r$ denote the prime power factorization of n, with $q_1 < \cdots < q_r$. For $d \geq 2$, a d-dimensional MacNeish conjecture could be stated as postulating that $N_d(n) \leq (q_1^d - 1)/(q_1 - 1) - d$.

22.48 Conjecture [1416] For $d \geq 2$ and $n \neq 6$ or a prime power, the d-dimensional MacNeish conjecture is false.

22.49 Remark The algorithm in [1416] shows that if the MacNeish conjecture is false for any dimension d and order n, it is false for hypercubes of dimension greater than d and order n. In particular, $N_3(6) \geq 6$ (see [1413] p. 59), and hence, the d-dimensional MacNeish conjecture is false for order $n = 6$ and all dimensions $d \geq 3$.

22.50 Theorem [1415] The class of $AD(m^{2h-1}, m)$ affine designs equivalent to complete sets of MOFS of type $F(m^h; m^{h-1})$ (see Theorem 22.13(4)) is a proper subset of the class of $AD(m^{2h-1}, m)$ designs equivalent to complete sets of latin hypercubes of dimension $2h$ and order m.

22.51 Theorem [1411] The class of $AD(n^{d-1}, n)$ affine designs equivalent to complete sets of latin hypercubes of dimension d and order n is a proper subset of the class of $AD(n^{d-1}, n)$ affine designs equivalent to complete sets of type 0 hypercubes of dimension d and order n.

22.52 Remark The existence of $n + 1$ mutually orthogonal squares of order n is known to be equivalent to the existence of a complete set of $n - 1$ mutually orthogonal latin squares of order n and two canonical row and column squares. By Theorem 22.51, this result cannot be extended for all dimensions $d > 2$.

22.53 Remark Theorem 22.51 is demonstrated by the $AD(16, 2)$ whose first block consists of the 15 quadratic residues mod 31 together with a special point labeled ∞ [1411]. The $i+1$-st block, $i = 1, \ldots, 30$, is constructed by adding 1 modulo 31 to the points other than ∞ in block i. The $AD(64, 2)$ constructed in a similar manner from quadratic residues modulo 127 also demonstrates this theorem. Both of these designs have characteristic zero and hence no special tuples, leading to the following conjectures.

22.54 Conjecture For all Mersenne primes $2^d - 1$ with $d > 3$, quadratic residues mod $2^d - 1$ give an $AD(2^{d-1}, 2)$ affine design with characteristic zero.

22.55 Conjecture No $AD(2^{d-1}, 2)$ design with characteristic zero can be represented by a complete set of $2^d - 1 - d$ latin hypercubes of dimension d and order 2 together with d canonical hypercubes.

22.56 Theorem [1415] The class of complete sets of $(n^d - 1)/(n - 1)$ type 0 hypercubes of dimension d and order n is equivalent to the class of $AD(n^{d-1}, n)$ affine designs.

22.57 Remark A different notion of orthogonality for d-dimensional hypercubes, *equiorthogonality*, is considered in [1634, 1635]. This approach makes more use of the internal structure of the hypercubes and leads to several interesting combinatorial results illustrated by the following theorems.

22.58 Theorem [1634] The maximum possible number of mutually equiorthogonal frequency hypercubes (MEFH) of dimension d and order n based on m symbols is at most $(n-1)^d/(m-1)$.

22.59 Theorem [1635] If m is a prime power and n is a power of m, or if $m = 2$ and there exists a Hadamard matrix of order $n = 4t$, then there exists a complete set of $(n-1)^d/(m-1)$ MEFH of dimension d and order n based on m symbols.

22.60 Theorem [1634] If a complete set of MEFH of dimension $d \geq 3$ and order n based on m symbols exists, then m is a prime power.

22.61 Remark Another definition of orthogonality is given in [1122] for $d \geq 2$-dimensional hypercubes of order n in the $\lambda = 1$ case. An upper bound of $(n-1)^{d-1}$ is found for the maximum number of such orthogonal hypercubes. Moveover, it was shown that for $d \geq 3$, this upper bound was achieved if and only if n was a prime power.

22.62 Remark The following table gives some enumeration results for latin hypercubes. The notions of reduced hypercubes, and isotopy and main classes are generalizations of the corresponding notions from latin squares. In the table, the first column refers to a hypercube of order n and dimension d, which thus contains n^d points. For hypercubes with less than 64 points, all values are 1.

Points	Reduced Hypercubes	Isotopy Classes	Main Classes
4^3	64	12	5
4^4	7,132	328	26
4^5	201,538,000	2,133,586	4,785
5^3	40,246	59	15
5^4	31,503,556	5,466	86
5^5	50,490,811,256	1,501,786	3,102
6^3	95,909,896,152	5,678,334	264,248

22.63 Remark Results on the enumeration and isotopic classification of frequency squares of small orders are found in [319]; Frequency cubes of small orders are studied in [320].

See Also

§III.1	Frequency squares are analogs of latin squares for higher index.
§III.3	MOFS are generalizations of MOLS.
[685]	Contains a chapter on frequency squares with proofs of several of the results given here along with the original references.
[809]	Examines relationships between frequency squares and codes, and frequency squares and orthogonal arrays.
[183]	Connections between sets of orthogonal hypercubes and many-placed operations in quasigroups.
[1094]	Connections to frequency magic squares.
[1993]	Has constructions of sets of orthogonal frequency hyperrectangles based upon a prime power number of symbols.
[1413]	Theorem 13.17 constructs error-correcting codes with large minimum distances from sets of MOFS; Theorem 13.19 constructs similar codes from hypercubes. Section 13.5 gives connections between the number of latin squares and hypercubes, and MDS codes.
[1416]	Connections between sets of orthogonal hypercubes and (t, m, s)-nets in base b. (See §VI.59.)

References Cited: [113, 183, 247, 319, 320, 685, 809, 1073, 1074, 1094, 1122, 1232, 1308, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1558, 1634, 1635, 1645, 1763, 1993]

23 Generalized Quadrangles

Stanley E. Payne

23.1 Definitions and Examples

23.1 A *finite generalized quadrangle* (GQ) is an incidence structure $\mathcal{S} = (P, B, I)$ with pointset P and lineset B satisfying:

1. each point is incident with $1 + t$ lines ($t \geq 1$) and two distinct points are incident with at most one line;
2. each line is incident with $1+s$ points ($s \geq 1$) and two distinct lines are incident with at most one point; and
3. if x is a point and L is a line not incident with x, then there is a unique pair $(y, M) \in P \times B$ for which $xIMIyIL$.

23.2 The integers s and t are the *parameters* of the GQ and $\mathcal{S}$ has *order* (s, t); if $s = t$, $\mathcal{S}$ has *order* s.

23.3 **Remark** There is a point-line duality for GQs of order (s, t) for which in any definition or theorem the words *point* and *line* are interchanged and the parameters s and t are interchanged. Without further notice, the dual of a given theorem or definition is assumed to have also been given. In particular, when listing parameters of known GQs one may assume that $s \leq t$.

23.4 **Remark** A generalized quadrangle is a partial geometry with $\alpha = 1$. See §VI.41.

23.5 **Proposition** If $|P| = v$ and $|B| = b$, then $v = (1 + s)(1 + st)$ and $b = (1 + t)(1 + st)$. Further, $s+t$ divides $st(s+1)(t+1)$, and for $s \neq 1 \neq t$ it holds that $s \leq t^2$ and $t \leq s^2$.

23.6 **Remark** For q any prime power, GQs with parameters (s, t), $s \leq t$ are known for $(s, t) \in \{(q-1, q+1), (q, q), (q, q^2), (q^2, q^3)\}$. With $s = 2$, there are unique examples with $t = 2$ and $t = 4$ (Examples 23.7 and 23.8) and none with $t = 3$. With $s = 3$, there is an example with $t = 3$ (not self-dual, but unique up to point-line duality), unique examples with $t = 5$ and $t = 9$, and no GQ with $t = 4, 6, 7, 8$. With $s = 4$, existence would imply that $t \in \{4, 6, 8, 11, 12, 16\}$. There is a unique example with $t = 4$. Nothing is known about $t = 11$ or $t = 12$. In the other cases unique examples are known, but the uniqueness question is settled only in the case $t = 4$.

23.7 **Example** The GQ with $s = t = 2$. Start with the set $I_6 = \{1, 2, 3, 4, 5, 6\}$. A *duad* is an unordered pair $ab = ba$ of elements of I_6. A *syntheme* is a triple of disjoint duads. Incidence is ordinary containment. There are fifteen duads and fifteen synthemes; the syntheme-duad geometry is a model of the unique GQ of order 2 often denoted $W(2)$. See Example VI.4.20 for the point-block incidence graph of $W(2)$.

23.8 **Example** To the syntheme-duad model, adjoin the 12 symbols $1, 2, \ldots, 6, 1', \ldots, 6'$ as points. Through each duad ab, adjoin the lines $\{a, ab, b'\}$ and $\{a', ab, b\}$. The resulting incidence structure is a model of the unique GQ with parameters $(2, 4)$.

23.2 Classical Constructions

23.9 Construction Let $P = \{x_{ij} : i, j = 0, 1, \ldots s\}$, $B = \{L_0, L_1, \ldots, M_0, M_1, \ldots, M_s\}$, $x_{ij} I L_k$ if and only if $i = k$, $x_{ij} I M_k$ if and only if $j = k$. Then $\mathcal{S} = (P, B, I)$ is a GQ of order $(s, 1)$. Such a (trivial) GQ is a *grid*. A dual grid has order $(1, t)$.

23.10 Construction $Q(d, q)$. Consider a nonsingular quadric Q of projective index 1 (Witt index 2) of the projective space $\mathrm{PG}(d, q)$, with $d = 3, 4,$ or 5. Then the points of Q together with the lines of Q form a GQ denoted $Q(d, q)$ of order (q, q^{d-3}). The quadric Q has the following canonical equation: $x_0 x_1 + x_2 x_3 = 0$, when $d = 3$, in which case $Q(3, q)$ is a grid. When $d = 4$, the equation is ${x_0}^2 + x_1 x_2 + x_3 x_4 = 0$, and when $d = 5$, it is $f(x_0, x_1) + x_2 x_3 + x_4 x_5 = 0$, where f is an irreducible binary quadratic form.

23.11 Construction $H(d, q^2)$. Let H be a nonsingular hermitian variety of the projective space $\mathrm{PG}(d, q^2)$, $d = 3$, or $d = 4$. Then the points of H together with the lines on H form a GQ denoted $H(d, q^2)$ of order (q^2, q) or (q^2, q^3) depending upon whether $d = 3$ or $d = 4$, and H has the canonical equation ${x_0}^{q+1} + {x_1}^{q+1} + \cdots + {x_d}^{q+1} = 0$.

23.12 Construction $W(q)$. The points of $\mathrm{PG}(3, q)$, together with the totally isotropic lines with respect to a symplectic polarity, form a GQ denoted $W(q)$ of order (q, q). Specifically, for points $\mathbf{x} = (x_0, x_1, x_2, x_3)$ and $\mathbf{y} = (y_0, y_1, y_2, y_3)$, define $\mathbf{x}$ and $\mathbf{y}$ to be collinear if and only if $x_0 y_1 - x_1 y_0 + x_2 y_3 - x_3 y_2 = 0$.

23.13 Remark The *classical* GQs from Construction 23.12 were all discovered by J. Tits and are the only ones embedded as full subgeometries of finite projective space. The point-line dual of $Q(4, q)$ is isomorphic to $W(q)$; $Q(4, q)$ (and hence also $W(q)$) is self-dual if and only if q is even. The point-line dual of $Q(5, q)$ is isomorphic to $H(3, q^2)$.

23.3 GQs from Ovals and Ovoids

23.14 Remark In the constructions of this section, let $\pi = \mathrm{PG}(2, q)$ be embedded as a plane of $\Sigma = \mathrm{PG}(3, q)$, q any prime power. Let $\Omega = \{X_0, \ldots, X_q\}$ be an oval of π, so Ω consists of $q + 1$ points of π, no three on a line. Let t_i be the line of π tangent to Ω at X_i, $0 \le i \le q$. Let P_1 be the pointset of $\Sigma \setminus \pi$.

23.15 Construction $T_2(\Omega)$. There is a GQ $\mathcal{S} = \mathcal{S}(\Omega) = (P, B, I)$ of order q defined as follows. The pointset $P = P_1 \cup P_2$, with P_1 as given, and with P_2 the set of planes of Σ containing at least one t_i. B is the set of lines of Σ meeting Ω in exactly one point. Incidence I is inherited from Σ. For example, the "point" π of $\mathcal{S}$ is incident with the $1 + q$ lines $t_0, \ldots, t_q$. The resulting GQ, denoted $T_2(\Omega)$, has order q.

23.16 Construction $\mathcal{S}(\Omega^-)$. Let $\Omega^- = \{X_1, \ldots, X_q\} = \Omega \setminus \{X_0\}$. Each point $X_j \in \Omega^-$ is on two tangents to Ω^-: the line $l_j = X_0 X_j$ and the tangent t_j, $1 \le j \le q$. Put $P_1^- = P_1 = \Sigma \setminus \pi$. Let $P_2^- = \{p : p \ne \pi$ is a plane of Σ with $p \cap \pi = t_j$, $j = 1, \ldots, q\}$; $P_3^- = \{p : p \ne \pi$ is a plane of Σ with $p \cap \pi = l_j$, $j = 1, \ldots, q\}$. Put $P^- = P_1^- \cup P_2^- \cup P_3^-$ and let B^- be the set of lines of Σ not in π and meeting π in a point of Ω^-. With the incidence I^- induced by that of Σ, the structure $\mathcal{S}^- = \mathcal{S}(\Omega^-) = (P^-, B^-, I^-)$ is a GQ of order $(q + 1, q - 1)$.

23.17 Construction $\mathcal{S}(\Omega^+)$. When q is even ($q = 2^e$), there is a unique hyperoval $\Omega^+ = \Omega \cup \{X_\infty\}$ containing Ω. There is a GQ $\mathcal{S}^+ = \mathcal{S}(\Omega^+) = (P^+, B^+, I^+)$ of order $(q - 1, q + 1)$ defined as follows. Let $P^+ = P_1$ and let B^+ be the set of all lines of Σ meeting π at a point of Ω^+. The incidence I^+ is that induced by incidence in Σ.

23.18 Construction $T_3(\mathcal{O})$. Let $\mathcal{O}$ be an *ovoid* of $\Sigma = \mathrm{PG}(3,q)$; that is, $\mathcal{O}$ is a set of $1+q^2$ points of Σ with no three on a line of Σ. Further, let Σ be embedded as an hyperplane in $\mathrm{PG}(4,q) = \mathcal{P}$. Define points as (i) the points of $\mathcal{P} \setminus \Sigma$, (ii) the hyperplanes Z of $\mathcal{P}$ for which $|Z \bigcap \mathcal{O}| = 1$, and (iii) one new symbol (∞). Lines are defined as (a) the lines of $\mathcal{P}$ that are not contained in Σ and meet $\mathcal{O}$ in a (necessarily unique) point, and (b) the points of $\mathcal{O}$. Incidence is defined as follows: A point of type (i) is incident only with lines of type (a); here the incidence is that of $\mathcal{P}$. A point of type (ii) is incident with all lines of type (a) contained in it and with the unique element of $\mathcal{O}$ in it. The point (∞) is incident with no line of type (a) and all lines of type (b). There are no other incidences.

The incidence structure just defined is a GQ with order $(s,t) = (q,q^2)$. It is usually denoted $T_3(\mathcal{O})$. When $\mathcal{O}$ is an elliptic quadric, $T_3(\mathcal{O})$ is isomorphic to $Q(5,q)$. The only nonclassical example known is for $q = 2^e$ with $e = 2h+1 \geq 3$ and $\mathcal{O}$ the Suzuki–Tits ovoid. Both $T_2(\Omega)$ and $T_3(\mathcal{O})$ were first given by J. Tits.

23.4 Flock GQ: GQ from q-Clans or BLT-sets

23.19 A *flock* of a quadratic cone in the finite 3-dimensional projective space $PG(3,q)$ is a partition of the cone minus its vertex into q disjoint conics.

23.20 A *q-clan* is a set $\mathcal{C} = \{A_t : t \in F\}$ containing q 2×2 matrices over $\mathbb{F}_q$ whose pairwise differences are each *anisotropic*; that is, the quadratic forms they determine represent zero only trivially. Let $K_t = A_t + A_t^T$.

23.21 Remark Such flocks are equivalent to the q-clans used in [1254, 1721] to construct GQ [2022]. Moreover, given one flock of a quadratic cone, it determines a set of q additional flocks (and, hence, q-clans). Each of these $q+1$ flocks gives rise to the same GQ, but when q is odd, they correspond to a set of $q+1$ points of the parabolic quadric $Q(4,q)$ with the property that no three are collinear in $Q(4,q)$ with a same point of $Q(4,q)$.

23.22 A set of $q+1$ points as described in Remark 23.21 is a *BLT-set*.

23.23 Remark Some of the GQ discovered in the recent past were discovered by means of computer searches for BLT-sets.

23.24 Remark In addition to the constructions of GQs in §23.2 and §23.3, many examples of GQs with order $(s,t) = (q^2,q)$, q a prime power, have been constructed as a kind of group coset geometry starting with a flock (a q-clan or, when q is odd, a BLT-set). When q is even, these GQs have subquadrangles of order q associated with ovals in $\mathrm{PG}(2,q)$. Moreover, these families of ovals, known as *herds* of ovals, coexist with the q-clans and hence with certain GQs with parameters (q^2,q). It is noteworthy that nearly all of the GQ discovered since 1990 have been found by T. Penttila either alone or with coauthors. See [1722] for references.

23.25 Construction Let $G = \{(\alpha,c,\beta) | \alpha,\beta \in F^2, c \in F\}$ be the group of order q^5 with binary operation $(\alpha,c,\beta) \circ (\alpha',c',\beta') = (\alpha+\alpha', c+c'+\beta\circ\alpha', \beta+\beta')$, where $\alpha \circ \beta = \alpha\beta^T$. Define subgroups of G having order q^2: $A(\infty) = \{(\vec{0},0,\beta) \in G | \beta \in F^2\}$, $A(t) = \{(\alpha, \alpha A_t \alpha^T, \alpha K_t) | \alpha \in F^2\}$. The center of G is $Z = \{(\vec{0},c,\vec{0}) | c \in F\}$. For $A \in \mathcal{J} = \{A(t) : t \in F \cup \{\infty\}\}$, put $A^* = AZ$. $\mathcal{J}$ is a 4-gonal family for G (see [1722]) and so provides the following construction of a GQ. Points are (1) the symbol (∞); (2) right cosets A^*g, $g \in G$, $A \in \mathcal{J}$; and (3) elements g of G. Lines are (a) symbols $[A]$, $A \in \mathcal{J}$; and (b) right cosets Ag, $g \in g$, $A \in \mathcal{J}$. Then (∞) is incident with each line of type (a) and none of type (b). The point A^*g is incident with $[A]$ and with

each line Ah contained in A^*g. The point g is incident with each line Ag containing it.

23.26 Remark When q is odd, in addition to the few infinite families of q-clans or BLT-sets that are known, many sporadic examples are known. See [1722] for a list of those that were known in 2000. The following setup is convenient for giving some of the known BLT-sets. Let $K = \mathbb{F}_q \subset GF(q^2) = E$, $q \geq 5$ and odd. Let ζ be a primitive element for E and put $\eta = z^{q-1}$. Let $T(x) = x + \overline{x}$, where $\overline{x} = x^q$. Let $V = \{(x, y, a) : x, y \in E, a \in K\}$ considered as a 5-dimensional vector space over K in the standard way. Define a map $Q : V \to K$ by: $Q(x, y, a) = x^{q+1} + y^{q+1} - a^2$. So Q is a nondegenerate quadratic form on V with polar form f given by $f((x, y, a), (z, w, b)) = T(x\overline{z}) + T(y\overline{w}) - 2ab$.

23.27 Construction When $q = 2^e$, there is now available a uniform construction for four of the known infinite families of q-clans given explicitly in item 10 of Table 23.28. Let $K = \mathbb{F}_q \subset \mathbb{F}_{q^2} = E$. Let $1 \neq \beta \in E$ satisfy $\beta^{q+1} = 1$, let $T(x) = x + x^q$ for $x \in E$, and let m be a fixed positive integer. Define $a \in K$ and $f, g : K \to K$ by

$$a = \frac{T(\beta^m)}{T(\beta)} + \frac{1}{T(\beta^m)} + 1;$$

$$f(t) = \frac{T(\beta^m)(t+1)}{T(\beta)} + \frac{T((\beta t + \beta^q)^m)}{T(\beta)(t + T(\beta)t^{\frac{1}{2}} + 1)^{m-1}} + t^{\frac{1}{2}};$$

$$ag(t) = \frac{T(\beta^m)}{T(\beta)}t + \frac{T((\beta^2 t + 1)^m)}{T(\beta)T(\beta^m)(t + T(\beta)t^{\frac{1}{2}} + 1)^{m-1}} + \frac{1}{T(\beta^m)}t^{\frac{1}{2}}.$$

$$\mathcal{C} = \{A_t = \begin{pmatrix} f(t) & t^{\frac{1}{2}} \\ 0 & ag(t) \end{pmatrix} : t \in \mathbb{F}_q\}.$$

23.28 Table The known families of q-clans (and/or BLT-sets when q is odd). The parameter t is to vary over all elements of F. See [1209, 1722, 2023] for more details and many references to the literature.

1. Classical: $A_t = \begin{pmatrix} t & bt \\ 0 & ct \end{pmatrix}$, $x^2 + bx + c$ irreducible over F.
2. FTW: $A_t = \begin{pmatrix} t & 3t^2 \\ 0 & 3t^3 \end{pmatrix}$; $q \equiv 2 \pmod 3$.
3. K_1: $A_t = \begin{pmatrix} t & 0 \\ 0 & -mt^\sigma \end{pmatrix}$, q odd, $\sigma \in Aut(F)$, m a nonsquare in F.
4. K_1/JP: $A_t = \begin{pmatrix} t & 5t^3 \\ 0 & 5t^5 \end{pmatrix}$, $q \equiv \pm 2 \pmod 5$.
5. The Thas–Fisher example for q odd. The BLT-set $\mathcal{P}$ (form due to T. Penttila) is given by $\mathcal{P} = \{\eta^{2j}, 0, 1) : 1 \leq j \leq \frac{q+1}{2}\} \cup \{(0, \eta^{2j}, 1)\} : 1 \leq j \leq \frac{q+1}{2}$.
6. K_3/BLT: $A_t = \begin{pmatrix} t & 3t^2 \\ 3t^2 & k^{-1}t(1 + kt^2)^2 \end{pmatrix}$, $q = 5^e$, k a nonsquare in F.
7. G/PTJLW: $A_t = \begin{pmatrix} t & -t^3 \\ -t^3 & -t(t^8 + m^2)/m \end{pmatrix}$, $q = 3^e$, m a nonsquare in F.
8. Penttila: For $q \equiv \pm 1 \pmod{10}$, the BLT-set $\mathcal{P}$ is given by $\mathcal{P} = \{(2\eta^{2j}, \eta^{3j}, \sqrt{5}) : 0 \leq j \leq q\}$.
9. Law–Penttila: For all $q = 3^e$, $A_t = \begin{pmatrix} t & t^4 + nt^2 \\ t^4 + nt^2 & -n^{-1}t^9 + t^7 + n^2t^3 - n^3t \end{pmatrix}$, where n is a fixed nonsquare of K.
10. Now let $q = 2^e$ and use the notation with $\beta^{q+1} = 1$, and so on. If $m \equiv \pm 1 \pmod{q+1}$, then $\mathcal{C}$ is the classical q-clan for all $q = 2^e$ and for all β. If e is odd and $m \equiv \pm\frac{q}{2} \pmod{q+1}$, then $\mathcal{C}$ is the example labeled FTW.

(a) If $m = \pm 5$, then $\mathcal{C}$ is the Subiaco q-clan for all β such that if ℓ is a primitive element of K and $\beta = \ell^{k(q-1)}$, then $q+1$ does not divide km.
(b) If $q = 4^e > 4$ and $m \equiv \pm\frac{q-1}{3} \pmod{q+1}$, then for all β, $\mathcal{C}$ is a q-clan, the *Adelaide q-clan*.

23.29 Remarks Most of what was known about generalized quadrangles up through 1983 is presented in Payne and Thas [1723]. The appearance of Kantor [1254] in 1980 was seminal for the work that followed, leading to the notion of q-clan. Thas [2023] gives an excellent survey of the results published between 1984 and 1992. The Subiaco q-clan of Table 23.28 (10) (originally given in a slightly different form) was found in 1993 by Cherowitzo et al. [493]. For $q = 2^e \geq 16$, it provides a unique nonclassical GQ of order (q^2, q). For $e \not\equiv 2 \pmod 4$, it gives a unique oval in $\mathrm{PG}(2, q)$, and for $e \equiv 2 \pmod 4$, it gives two inequivalent ovals in $\mathrm{PG}(2, q)$. For $q = 4^e$, the Adelaide q-clan provides a unique nonclassical GQ of order (q^2, q). For $q \geq 32$, the GQs constructed from the different q-clans given are all distinct.

23.30 Remark Every flock GQ has a special Property (G) at its point (∞). Thas [2025] found a remarkable geometric construction of flock GQ that works for all q. Moreover, the converse is also true: any GQ with parameters (q^2, q) and having Property (G) at a point must be a flock GQ.

23.31 Let $\mathcal{S}$ be a GQ with parameters (s, t), $s > 1, t > 1$. An *elation* of $\mathcal{S}$ about a point P is a collineation of $\mathcal{S}$ that fixes P linewise and acts semiregularly on the set of points of $\mathcal{S}$ not collinear with P. $\mathcal{S}$ is an *elation GQ* with *base point* P provided there is a group G of elations about P that acts regularly about P, in which case $(\mathcal{S}^P, G)$ is an *EGQ*.

23.32 Remark If G is abelian, it can be shown that G is the complete set of elations about P and $\mathcal{S}$ is a *translation GQ*. A great deal of work has been done on the problem of characterizing the translation GQ since [1723] first appeared. See [2027].

23.5 Other Designs Derived From GQs

23.33 Remark The classical GQs can be used to construct projective planes, inversive planes, Laguerre planes of odd order, and Minkowski planes of even order. The q-clans used to construct GQs of order (q^2, q) can also be used to construct several other types of geometries including translation planes of dimension at most two over their kernel.

23.34 Construction A GQ of order q yields (potentially two) symmetric 2-$(q^3 + q^2 + q + 1, q^2 + q + 1, q + 1)$ designs whose incidence matrix contains the identity matrix, one from the point-collinearity graph and the other from the line-concurrency graph of the GQ.

23.35 Construction A GQ with parameters $(q-1, q+1)$ yields a symmetric 2-$(q^2(q+2), q(q+1), q)$ design whose incidence matrix has a zero diagonal, from the line-concurrency graph. Here distinct concurrent lines represent an incident point-block pair of the design.

23.36 Construction A GQ with parameters (q, q^2) yields an orthogonal array $OA_q(3, q, 1 + q^2)$. Here the $1+q^2$ lines through a fixed point (∞) can have their q other points labeled with q symbols of a set F. Each of the q^4 points not collinear with (∞) determines a "row" of length $1 + q^2$ of symbols from F, since it is collinear with exactly one point on each line through (∞). The fact that each triple of pairwise noncollinear points all collinear with (∞) are collinear with exactly q points not collinear with (∞) provides an orthogonal array of strength 3.

See Also

§II.6	Symmetric designs come from GQs via Constructions 23.34 and 23.35.
§III.7	Certain GQs yield orthogonal arrays via Construction 23.36.
§VI.41	A GQ is a partial geometry with $\alpha = 1$.
§VII.2	The classical GQs are embedded in finite projective space.
[1723]	A book that surveys GQs up through 1983.
[2023]	A survey of results on GQs from 1983 through 1992.
[1209]	An extensive survey of the (finite and infinite) flock GQs and other geometries related to them.
[435]	A fairly complete treatment of the q-clan geometries when $q = 2^e$, available at the home page of the author.
[2028]	A monograph giving an in-depth treatment of finite GQs under a variety of assumptions about their collineation groups.

References Cited: [435, 493, 1209, 1254, 1721, 1722, 1723, 2022, 2023, 2025, 2027, 2028]

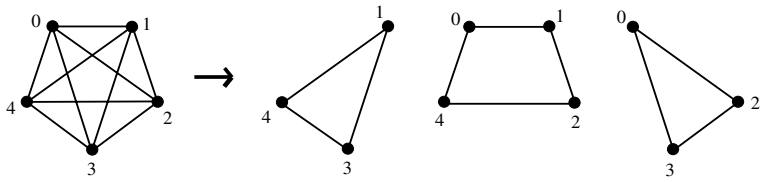
24 Graph Decompositions

Darryn Bryant
Saad El-Zanati

24.1 Definitions

24.1 Let G and K be graphs. The vertex and edge sets of G are denoted by $V(G)$ and $E(G)$ respectively. A *decomposition* of K is a set of subgraphs of K whose edge sets partition the edge set of K. A subgraph in a decomposition is a *G-block* if it is isomorphic to G. A decomposition of K into G-blocks is a *G-decomposition* of K.

24.2 **Example** A decomposition of the complete graph on five vertices into a 4-cycle and two 3-cycles.

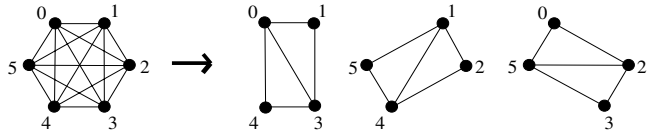


24.3 A *G-factor* of a graph K is a set of G-blocks whose vertex sets partition the vertex set of K. An *almost G-factor* of K is a G-factor of $K - v$ for some vertex v of K. A *G-factorization* is a G-decomposition where the G-blocks are partitioned into G-factors. An *almost G-factorization* is a G-decomposition where the G-blocks are partitioned into almost G-factors. A G-factorization is also a *resolvable* G-decomposition and an almost G-factorization is also an *almost resolvable* G-decomposition.

24.4 Let K be a graph and let $n = |V(K)|$. A G-decomposition of K is *cyclic* if there exists a labeling of $V(K)$ with the elements of $\mathbb{Z}_n$ such that the label permutation $x \mapsto x + 1$ preserves the G-blocks of the decomposition.

24.5 λK_n is the undirected multigraph on n vertices in which each pair of vertices is joined by exactly λ edges. A G-decomposition of λK_n is a *G-design* of *order* n and *index* λ or a *$(\lambda K_n, G)$-design*. A $(\lambda K_n, G)$-design is *balanced* if each vertex of λK_n occurs in the same number of G-blocks.

24.6 Example A (K_6, G)-design where $G = K_4 - e$. The design is balanced and cyclic.



24.7 Remarks A $(\lambda BIBDK_v, K_k)$-design is a (v, k, λ) (see §II.1.1). A decomposition of λK_v into complete subgraphs is a PBD (see §IV.1), and a decomposition of a complete multipartite graph into complete subgraphs is a GDD (see §IV.1). Decompositions into cycles are *cycle systems* (see §VI.12).

24.2 General Results

24.8 Theorem If there exists a $(\lambda K_n, G)$-design, then

1. $|V(G)| \leq n$ for $n > 1$,
2. $\frac{\lambda n(n-1)}{2|E(G)|}$ is an integer (the number of G-blocks), and
3. if d is the gcd of the degrees of the vertices in G, then $\frac{\lambda(n-1)}{d}$ is an integer (since the edges incident with each vertex are partitioned by the G-blocks).

If the design is balanced, then

4. $\frac{\lambda(n-1)|V(G)|}{2|E(G)|}$ is an integer (the number of G-blocks in which each vertex of λK_n occurs), and
5. there exist nonnegative integers $x_1, x_2, \ldots, x_k$ such that $x_1 + x_2 + \cdots + x_k = \frac{\lambda(n-1)|V(G)|}{2|E(G)|}$ and $x_1 d_1 + x_2 d_2 + \cdots + x_k d_k = \lambda(n-1)$ where $k = |V(G)|$ and $(d_1, d_2, \ldots, d_k)$ is the degree sequence of G (x_i is the number of times a vertex of λK_n occurs in a G-block as a vertex of degree d_i).

If the design is a G-factorization of λK_n, then it is balanced and

6. $\frac{n}{|V(G)|}$ is an integer (the number of G-blocks in each G-factor).

If the design is an almost G-factorization of λK_n, then

7. $\frac{n-1}{|V(G)|}$ is an integer (the number of G-blocks in each almost G-factor), and
8. $\frac{\lambda n|V(G)|}{2|E(G)|}$ is an integer (the number of almost G-factors).

24.9 Remark Fisher's Inequality and the Bruck–Ryser–Chowla Theorem (Theorems II.1.9 and II.6.2) give additional necessary conditions for the existence of $(\lambda K_n, G)$-designs when G is a complete graph.

24.10 Theorem [2152] For a given graph G and integer λ, there exists an integer $N(G, \lambda)$ such that if $n > N(G, \lambda)$, then Conditions 2 and 3 of Theorem 24.8 are sufficient for the existence of a $(\lambda K_n, G)$-design.

24.11 Theorem (see [743]) For an arbitrary given graph K, deciding whether there exists a G-decomposition of K is NP-complete if and only if G contains a connected component with three or more edges.

24.3 Decompositions into Trees

24.12 A *tree* is a connected graph with no cycles. Let G be a connected graph. The *distance* $d(x, y)$ between two vertices x and y in G is the number of edges in a shortest walk from x to y, and the *diameter* of G is $\max\{d(x, y) : x, y \in V(G)\}$.

24.13 Remark Many results on decompositions into trees have been inspired by *Ringel's Conjecture* (Conjecture 24.14), and many are obtained under the guise of graph labelings, see §24.6.

24.14 Conjecture There exists a (K_{2n+1}, T)-design for every tree T with n edges (see [854]).

24.15 Remarks It is not true that there is a (K_{2n+1}, G)-design for every graph G with n edges. For example, there is no (K_{43}, K_7)-design. It is unknown whether there is a noncomplete graph G with n edges such that there is no (K_{2n+1}, G)-design.

24.16 Conjecture The complete graph K_n can be decomposed into any collection of trees $T_1, T_2, \ldots, T_n$, where each T_i is a tree with i vertices [1000].

24.17 Remark Conjecture 24.16 is due to Gyárfás and Lehel [1000] and is known as the *Tree Packing Conjecture*. In addition to the results given in Theorem 24.18, further results on the conjecture can be found in [735, 2178].

24.18 Theorem Conjecture 24.16 holds in each of the cases:

1. All the trees except at most three are stars [1000, 1813].
2. Each T_i is a path or a star [1000].
3. At most one of the trees has diameter more than three [1115].
4. For $i = 1, 2, \ldots, n$, there exists an $x_i \in V(T_i)$ such that $T_i - x_i$ has at least $i - \sqrt{6(i-1)}/4$ isolated vertices [735].

▷ Decompositions into Paths

24.19 P_k is the path on k vertices.

24.20 Theorem There exists a $(\lambda K_n, P_k)$-design if and only if $n \geq k$ and $\lambda n(n-1) \equiv 0 \pmod{2k-2}$ (see [1080]).

24.21 Theorem There exists a balanced $(\lambda K_n, P_k)$-design if and only if $n \geq k$, $\lambda(n-1) \equiv 0 \pmod{2k-2}$ for k odd and $\lambda(n-1) \equiv 0 \pmod{k-1}$ for k even (see [1080]).

24.22 Theorem There exists a P_k-factorization of λK_n if and only if $n \equiv 0 \pmod{k}$ and $\lambda k(n-1) \equiv 0 \pmod{2k-2}$ (see [1080]).

24.23 Theorem [2196] There exists an almost P_k-factorization of λK_n if and only if $n \equiv 1 \pmod{k}$ and $\lambda kn \equiv 0 \pmod{2k-2}$.

▷ Decompositions into Stars

24.24 S_k is the star on k vertices, that is, the complete bipartite graph with one part having a single vertex and the other part having $k-1$ vertices.

24.25 Theorem [2005] There exists a $(\lambda K_n, S_k)$-design if and only if $\lambda n(n-1) \equiv 0 \pmod{2k-2}$ and

1. $n \geq 2k-2$ for $\lambda = 1$,
2. $n \geq k$ for even λ, and
3. $n \geq k + \frac{k-1}{\lambda}$ for odd $\lambda \geq 3$.

24.26 Theorem [1451] Let $m_1 \geq m_2 \geq \cdots \geq m_t$ be positive integers. Then K_n can be decomposed into stars $S_{m_1}, S_{m_2}, \ldots, S_{m_t}$ if and only if (1) $\sum_{i=1}^{k}(m_i - 1) \leq \sum_{i=1}^{k}(n-i)$ for $k = 1, 2, \ldots, n-1$ and (2) $\sum_{i=1}^{t}(m_i - 1) = \frac{n(n-1)}{2}$.

24.27 Theorem [2082] For $k \geq 3$ the following three statements are equivalent.

1. There exists a balanced $(\lambda K_n, S_k)$-design.
2. There exists a cyclic $(\lambda K_n, S_k)$-design.
3. $\lambda(n-1) \equiv 0 \pmod{2k-2}$ and $n \geq k$.

24.28 Remark An S_2-factorization is a 1-factorization. An S_2-factorization of λK_n exists if and only if n is even (see §VII.5).

24.29 Theorem [1142] Let $k \geq 4$ be even. An S_k-factorization of λK_n exists if and only if there is a divisor x of $k-1$ such that $n \equiv k \pmod{\frac{k(k-1)}{x}}$ and $\lambda \equiv 0 \pmod{2x}$.

24.30 Theorem [2197] Let k be odd. An S_k-factorization of K_n exists if and only if $n \equiv 1 \pmod{2k-2}$ and $n \equiv 0 \pmod{k}$.

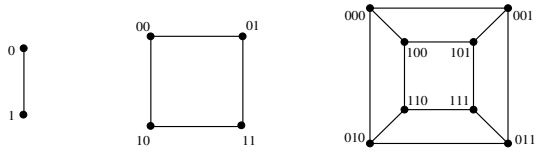
24.31 Theorem [1142] Let k be odd and let q be a positive integer. An S_k-factorization of λK_n exists if either

1. $n = k^{2q}$, or
2. λ is even and $n = k^q$, or
3. there is a divisor x of $k-1$ such that x is even, $n \equiv k \pmod{\frac{2k(k-1)}{x}}$, and $\lambda \equiv 0 \pmod{x}$.

24.4 Decompositions into Cubes

24.32 The *k-dimensional cube* or *k-cube* is the graph with vertex set consisting of all binary vectors of length k and with edges joining pairs of vertices that differ in precisely one coordinate. The k-cube is denoted by Q_k.

24.33 Example The cubes of dimension 1, 2 and 3.



24.34 Remark The k-cube has 2^k vertices and $k2^{k-1}$ edges, is k-regular, and is bipartite. Q_1-decompositions are trivial, Q_1-factorizations are 1-factorizations (see §VII.5), and Q_2-decompositions are 4-cycle systems (see §VI.12).

24.35 Theorem If there exists a (K_n, Q_k)-design, then either

1. $n \equiv 1 \pmod{k2^k}$ or
2. k is odd, $n \equiv 0 \pmod{2^k}$, and $n \equiv 1 \pmod{k}$.

24.36 Theorem [1326] There exists a cyclic (K_n, Q_k)-design if $n \equiv 1 \pmod{k2^k}$.

24.37 Theorem [1510] There exists a (K_n, Q_3)-design if and only if $n \equiv 1$ or $16 \pmod{24}$.

24.38 Theorem [360] There exists a (K_n, Q_5)-design if and only if $n \equiv 1$ or $96 \pmod{160}$.

24.39 Remark Theorems 24.36, 24.37, and 24.38 establish that the necessary conditions of Theorem 24.35 are sufficient for the existence of a (K_n, Q_k)-design except possibly when $k \geq 7$ is odd and n is even.

24.40 Theorem [777] Let $k \geq 1$ be odd, let $e \geq k$ be such that $2^e \equiv 1 \pmod{k}$ and let s be the order of 2 (mod k). If t is a nonnegative integer and $n = 2^e(t(2^s - 1) + 1)$, then there exists a (K_n, Q_k)-design.

24.41 Theorem [375] Let $k \geq 1$ be odd and let $e \geq k$ be such that $2^e \equiv 1 \pmod{k}$. If t is a nonnegative integer and $n = 2^e(k2^k t + 1)$, then there exists a (K_n, Q_k)-design.

24.42 Theorem [61] There exists a $(\lambda K_n, Q_3)$-design if and only if $n \geq 8$, $\lambda(n-1) \equiv 0 \pmod{3}$ and $\lambda n(n-1) \equiv 0 \pmod{24}$.

24.43 Theorem [63] There exists a Q_3-factorization of K_n if and only if $n \equiv 16 \pmod{24}$.

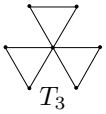
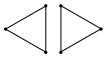
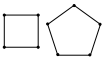
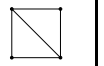
24.44 Theorem [776] Let m and $k_1, k_2, \ldots, k_t$ be positive integers. Then K_{2^m} can be decomposed into a Q_{k_1}-factor, a Q_{k_2}-factor, ..., and a Q_{k_t}-factor if and only if $k_i \leq m$ for all i and $k_1 + k_2 + \cdots + k_t = 2^m - 1$.

24.5 Decompositions into Small Graphs

24.45 Theorem (see [58]) The necessary conditions of Theorem 24.8 are sufficient for the existence of a (K_n, G)-design in each of the following cases, except for the indicated exceptions and unresolved cases. The small graphs T_3, C_3C_3, C_4C_5, $K_4 - e$, G_7, G_8, G_9, G_{13}, G_{14}, G_{16}, G_{18}, G_{19}, G_{20}, G_{21}, G_{22}, $\theta(1,3,3)$, $\theta(2,2,3)$, $\theta(1,4,4)$, $\theta(2,2,5)$, $\theta(3,3,3)$ are shown in Table 24.46.

1. G consists of three internally disjoint paths with common end points and G has 9 or fewer edges.
   Exceptions: $(n,G) \in \{(5, K_4 - e),\ (9, G_{14}),\ (12, G_{14}),\ (7, \theta(1,3,3)),\ (7, \theta(2,2,3)),\ (9, \theta(1,4,4)), (9, \theta(2,2,5)), (9, \theta(3,3,3))\}$.
2. G has 10 or fewer edges, each vertex has even degree, and G is connected or 2-regular.
   Exceptions: $(n,G) \in \{(9, T_3), (9, C_3C_3), (9, C_4C_5)\}$.
3. $G \in \{K_{3,3}, P, O, D, I, C, H\}$ where $K_{3,3}$ is the complete bipartite graph with parts of size 3, P is the Petersen graph, O is the Octahedron, D is the Dodecahedron, I is the Icosahedron, C is the Cuboctahedron, and H is the Heawood graph.
   Exceptions: $(n,G) \in \{(10, K_{3,3}), (10, P), (9, O)\}$
   Unresolved Cases:
   - n satisfying both $n \geq 85$ and $n \equiv 16, 25, 40 \pmod{60}$ for $G = D$.
   - n satisfying both $n \geq 21$ and $n \equiv 16, 21, 36 \pmod{60}$ for $G = I$.
4. G has five or fewer vertices.
   Exceptions: $(n,G) \in \{(4,S_3),(5,K_4-e),(5,G_7),(5,G_8),(5,G_9),(6,G_9),(9,G_{14}),(12,G_{14}),(7,G_{16}),(8,G_{16}),(8,G_{18}),(14,G_{18}),(8,G_{19}),(16,G_{21}),(9,G_{22}),(10,G_{22}),\ (18,G_{22})\}$.
   Unresolved Cases: $(n,G) \in \{(24, G_{13}), (42, G_{18}), (56, G_{18}), (92, G_{18}), (98, G_{18}), (120, G_{18}), (32, G_{20}), (48, G_{20}), (48, G_{21}), (27, G_{22}), (36, G_{22}), (54, G_{22}),\ (64, G_{22}),\ (72, G_{22}),\ (81, G_{22}),\ (90, G_{22}), (135, G_{22}),\ (144, G_{22}), (162, G_{22}),\ (216, G_{22}),\ (234, G_{22})\}$.
5. G is the graph obtained from K_{m+2} by removing a complete subgraph on m vertices, $m \geq 1$.
   Exceptions: $m \geq 2$ is even and $n = 2m + 1$.
   Unresolved Cases: $n \not\equiv 0, 1 \pmod{2m+1}$.

24.46 Table Small graphs referenced in Theorem 24.45.

 T_3	 C_3C_3	 C_4C_5	 K_4-e	 G_7	 G_8	 G_9
 G_{13}	 G_{14}	 G_{16}	 G_{18}	 G_{19}	 G_{20}	 G_{21}
 G_{22}	 $\theta(1,3,3)$	 $\theta(2,2,3)$	 $\theta(1,4,4)$	 $\theta(2,2,5)$	 $\theta(3,3,3)$	

24.47 Remark In [453, 1081], the stated results for G_{20}-decompositions are not correct. These errors appear to have arisen from an error in the statement of a result in [1811].

24.48 Remarks The nonexistence of a $(K_{10}, K_{3,3})$-design follows from the result of Graham and Pollak (see [2080]) that there is no decomposition of K_n into fewer than $n-1$ complete bipartite graphs. There is also no (K_n, G)-design with $n-1$ blocks when G is a complete bipartite graph with at least two vertices in each part [640]. For any complete bipartite graph G, the existence of a (K_n, G)-design with n blocks follows from the fact that G has an α-labeling (see §24.6).

Many additional existence results for (K_n, G)-designs can be obtained from results on graph labelings (see §24.6).

24.6 Graph Labelings

24.49 The *length* of an edge $\{i, j\}$ in K_n with $V(K_n) = \{0, 1, \ldots, n-1\}$ is $\min\{|i-j|, n-|i-j|\}$.

24.50 Remarks If n is odd, then K_n consists of n edges of length i for $i = 1, 2, \ldots, \frac{n-1}{2}$. If n is even, then K_n consists of n edges of length i for $i = 1, 2, \ldots, \frac{n}{2}-1$, and $\frac{n}{2}$ edges of length $\frac{n}{2}$; moreover, in this case, the edges of length $\frac{n}{2}$ constitute a 1-factor in K_n.

24.51 Let G be a graph with n edges. A *ρ-labeling* of G is a one-to-one function $f : V(G) \mapsto \{0, 1, \ldots, 2n\}$ such that $\{\min\{|f(u)-f(v)|, 2n+1-|f(u)-f(v)|\} : \{u, v\} \in E(G)\} = \{1, 2, \ldots, n\}$.

24.52 Remark A ρ-labeling of G with n edges is an embedding of G in K_{2n+1} with $V(K_{2n+1}) = \{0, 1, \ldots, 2n\}$ so that there is exactly one edge in G of length i for $i = 1, 2, \ldots, n$.

24.53 Theorem [1821] Let G be a graph with n edges. There exists a cyclic (K_{2n+1}, G)-design if and only if G has a ρ-labeling.

24.54 Theorem Let G be a graph with n edges and a vertex v of degree 1 in G. If $G-v$ has a ρ-labeling, then there exists a (K_{2n}, G)-design.

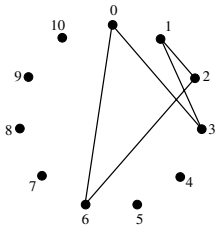
24.55 Conjecture Every tree admits a ρ-labeling.

24.56 Conjecture Every bipartite graph admits a ρ-labeling.

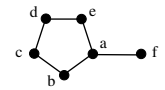
24.57 Conjecture Every 2-regular graph admits a ρ-labeling.

24.58 Remarks Kotzig is usually credited with Conjecture 24.55. Conjectures 24.56 and 24.57 are due to El-Zanati and Vanden Eynden. Some small graphs that do not admit ρ-labelings are given in Theorem 24.81.

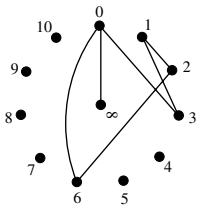
24.59 Example A ρ-labeling of the 5-cycle C_5, the corresponding cyclic (K_{11}, C_5)-design, and a (K_{12}, G)-design obtained from the ρ-labeling of C_5 (G is a 5-cycle with a pendant edge).



$(0, 3, 1, 2, 6)$
$(1, 4, 2, 3, 7)$
$(2, 5, 3, 4, 8)$
$(3, 6, 4, 5, 9)$
$(4, 7, 5, 6, 10$
$(5, 8, 6, 7, 0)$
$(6, 9, 7, 8, 1)$
$(7, 10, 8, 9, 2)$
$(8, 0, 9, 10, 3)$
$(9, 1, 10, 0, 4)$
$(10, 2, 0, 1, 5)$



G = (f:a,b,c,d,e)



$(\infty : 0, 3, 1, 2, 6)$
$(\infty : 1, 4, 2, 3, 7)$
$(\infty : 2, 5, 3, 4, 8)$
$(\infty : 3, 6, 4, 5, 9)$
$(\infty : 4, 7, 5, 6, 10)$
$(\infty : 5, 8, 6, 7, 0)$
$(\infty : 6, 9, 7, 8, 1)$
$(\infty : 7, 10, 8, 9, 2)$
$(\infty : 8, 0, 9, 10, 3)$
$(\infty : 9, 1, 10, 0, 4)$
$(\infty : 10, 2, 0, 1, 5)$

24.60 A ρ-labeling f of a graph G with n edges is a *σ-labeling* if $\{|f(u) - f(v)| : \{u, v\} \in E(G)\} = \{1, 2, \ldots, n\}$.

24.61 Theorem If G has n edges and admits a σ-labeling, then there exists a cyclic G-decomposition of $K_{2n+2} - I$, where I is a 1-factor of K_{2n+2}.

24.62 Let G be a graph with n edges. A one-to-one function $f : V(G) \mapsto \{0, 1, \ldots, n\}$ is a *β-labeling* of G if $\{|f(u) - f(v)| : \{u, v\} \in E(G)\} = \{1, 2, \ldots, n\}$.

24.63 Remark A β-labeling of G is better known as a *graceful* labeling of G. A graph that admits a graceful labeling is *graceful*. A β-labeling is necessarily a σ-labeling, which in turn is a ρ-labeling.

24.64 Conjecture Every tree is graceful.

24.65 Remark Conjecture 24.64 is known as the *Graceful Tree Conjecture* and is often credited to Kotzig and Ringel or to Rosa. Its first appearance in the literature is in [1821].

24.66 Remark A necessary condition for a graph G to be graceful is $|E(G)| \geq |V(G)| - 1$. There are no similar restrictions for σ- and ρ-labelings of G.

24.67 A graph G with n edges satisfies the *parity condition* if $n \equiv 0$ or $3 \pmod 4$ or if G has a component that is not eulerian.

24.68 Theorem [1821] If G admits a σ-labeling, then G satisfies the parity condition.

24.69 Remark There is no known bipartite graph that satisfies the parity condition and has no σ-labeling. However, there are bipartite graphs that satisfy the parity condition as well as the condition in Remark 24.66, yet fail to be graceful. The vertex-disjoint union of a 4-cycle and K_2 is one such example.

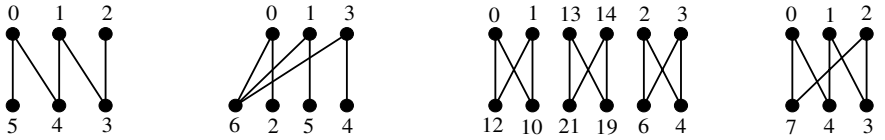
24.70 A β-, σ-, or ρ-labeling f of a bipartite graph G with n edges and bipartition (A, B) is *ordered* if $f(a) < f(b)$ for each edge $\{a, b\}$ with $a \in A$ and $b \in B$. Ordered β-, σ-, and ρ-labelings are β^+-, σ^+-, and *ρ^+-labelings*, respectively.

24.71 Theorem [774] Let G be a bipartite graph with n edges. If G admits a ρ^+-labeling, then there exists a cyclic (K_{2nx+1}, G)-design for all nonnegative integers x.

24.72 A β-labeling f of a bipartite graph G with n edges and bipartition (A, B) is an *α-labeling* if there exists an integer k such that $f(a) \leq k$ and $f(b) > k$ for every $a \in A$ and every $b \in B$.

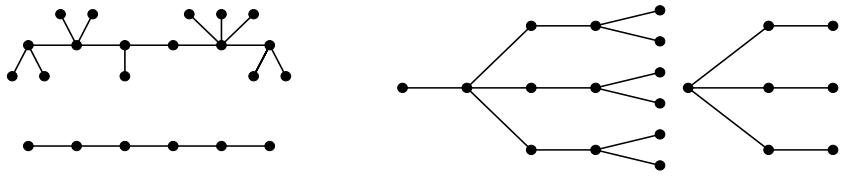
24.73 Remarks An α-labeling is a special type of β^+-labeling. Not all trees admit α-labelings. For example, trees of diameter 4 containing the seven-vertex tree in Example 24.74 do not admit α-labelings [1821]. There is no known example of a tree that does not admit a β^+-labeling, and no known example of a bipartite graph that does not admit a ρ^+-labeling.

24.74 Example An α-labeling of P_6, a β^+-labeling of a tree (which has no α-labeling), a σ^+-labeling of the union of three vertex-disjoint 4-cycles, and a ρ^+-labeling of a 6-cycle.



24.75 The *base* of a graph G is the graph obtained when the vertices of degree 1 are removed from G. A *caterpillar* is a tree whose base is a path. A tree is *symmetric* if it can be rooted such that any two vertices in the same level have the same degree.

24.76 Example A caterpillar and a symmetric tree together with their respective bases.



24.77 Theorem The graphs that admit α-labelings include

1. Caterpillars, complete bipartite graphs, $4k$-cycles for all $k \geq 1$ [1821].
2. Cubes [1326].
3. Bipartite 2-regular graphs that satisfy the parity condition and have at most 3 components, except for the union of three vertex disjoint 4-cycles (see [854]).
4. Numerous other graphs (see [854]).

24.78 Theorem The graphs that are graceful (see [854]) include

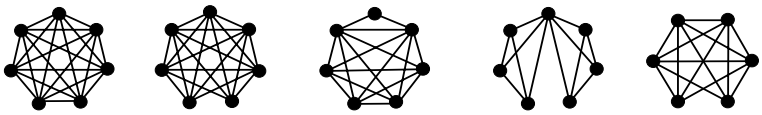
1. Trees with at most 27 vertices.
2. Trees with at most 4 end-vertices.
3. Trees of diameter at most 5.
4. Symmetric trees.
5. K_n if and only if $n \leq 4$.
6. 2-regular graphs satisfing the parity condition that have at most two components.
7. Numerous other graphs.

24.79 Remark Some 2-regular graphs satisfying the parity condition are not graceful. The vertex-disjoint union of two 3-cycles and a 5-cycle is the smallest such graph.

24.80 Theorem The graphs that admit the indicated ordered labelings include

1. Trees with up to 20 edges have β^+-labelings (see [854]).
2. Symmetric trees of diameter 4 have β^+-labelings (see [854]).
3. 2-regular bipartite graphs have σ^+-labelings if the parity condition is satisfied, and ρ^+-labelings, otherwise [282].
4. The union of vertex-disjoint graphs that have α-labelings has a σ^+-labeling (see [854]).

24.81 Theorem [55] Five graphs that do not admit ρ-labelings are



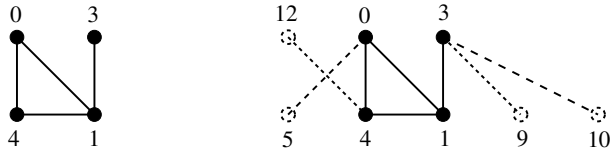
K_7 $K_7 - e$ $K_7 - S_5$ $K_7 - K_{3,3}$ $K_6 - e$

24.82 Theorem Graphs that admit ρ-labelings, and σ-labelings if indicated, include

1. Graphs with at most 7 vertices, except for those listed in Theorem 24.81 [55].
2. Graphs with at most 11 edges [55].
3. Trees with at most 55 vertices admit σ-labelings [318].
4. K_{p^t+1} where p is prime and $t \geq 1$ (see §VI.18).
5. 2-regular graphs with at most 3 components. These admit σ-labelings if the parity condition is satisfied [66, 67].
6. The union of vertex-disjoint triangles admit σ-labelings if the parity condition is satisfied and ρ-labelings otherwise [718].
7. Graphs in which one component has a β-labeling and every other component has an α-labeling admit σ-labelings [1093].
8. Graphs with graceful bases admit σ-labelings.

24.83 Remark A ρ-labeling of K_{n+1} is equivalent to a cyclic $(n^2+n+1, n+1, 1)$ difference set (see §VI.18).

24.84 Example A β-labeling of a graph G and a σ-labeling of a graph with base G.



24.7 Isomorphic Factorizations

24.85 Remark An *isomorphic factorization* problem asks for G-decomposition of a given graph K where the number of G-blocks is specified but G itself is not.

24.86 A graph K is *t-rational* if for some graph G, there exists a G-decomposition of K containing exactly t G-blocks or if t does not divide the number of edges in K. Otherwise K is *t-irrational*. A graph is *rational* if it is t-rational for all $t \geq 1$. Otherwise it is *irrational*.

24.87 Theorems (see [1057, 2116, 2177]) Complete graphs are rational. Regular complete multipartite graphs are rational. Complete bipartite graphs are rational. Complete tripartite graphs are t-rational for all even $t \geq 2$, but there exist t-irrational complete tripartite graphs for all odd $t \geq 3$.

24.88 Theorem [2169] For $k \in \{1, 2\}$, all k-regular graphs are rational. For $t \geq 2$ and $k \geq 2t+1$, almost all k-regular graphs with number of edges divisible by t are t-irrational.

24.89 Remarks It is unknown whether there exist irrational k-regular graphs for $k \in \{3, 4\}$. Theorem 24.88 is proved using enumerative methods. No irrational regular graph has been constructed. No irrational vertex-transitive graphs are known. Some results on isomorphic factorizations of circulant graphs appear in [82].

24.90 Theorem [782] Let G be a graph, let $\Delta(G)$ denote the maximum degree of a vertex in G, and let $t \geq \Delta(G) + 1$. Then G is t-rational.

24.91 Theorems (see [781]) Let G be a k-regular graph with n vertices. G is k-rational if

- $k \in \{3, 4, 25, 27\}$ or $k \geq 29$;
- k is even and G contains either no 3-cycles or no 5-cycles;
- $k \geq 9$ is odd and $n > 32(k+1)/(k-7)$; or
- $k \geq 18$ and $n > 24(k+1)/(k-17)$.

24.92 Remark There are numerous results on isomorphic factorizations of trees, see [1082] and the references therein.

See Also

§II.1.1	A $(\lambda K_v, K_k)$-design is a (v, k, λ) balanced incomplete block design.
§IV.1	A decomposition of λK_v into complete subgraphs is a PBD.
§IV.4	A decomposition of a complete multipartite graph into complete subgraphs is a GDD.
§VI.12	Decompositions into cycles are cycle systems.
§VI.27	An application in optical networking.
[973]	A comprehensive survey on ODCs and their connections to designs. An *orthogonal double cover (ODC)* is a collection of n spanning subgraphs (pages) of the complete graph K_n such that they cover every edge of the complete graph twice and the intersection of any two of them contains exactly one edge.

References Cited: [55, 58, 61, 63, 66, 67, 82, 282, 318, 360, 375, 453, 640, 718, 735, 743, 774, 776, 777, 781, 782, 854, 973, 1000, 1057, 1080, 1081, 1082, 1093, 1115, 1142, 1326, 1451, 1510, 1811, 1813, 1821, 2005, 2080, 2082, 2116, 2152, 2169, 2177, 2178, 2196, 2197]

25 Graph Embeddings and Designs

Jozef Širáň

25.1 Definitions and Examples

25.1 Remark Topological design theory studies representations of designs on surfaces, most commonly by means of surface embeddings of the incidence graphs of designs. In this chapter, graphs are identified with the topological 1-dimensional complexes they form.

25.2 Let G be a graph, regarded as a 1-dimensional complex. An *embedding* of G on a surface S is the image $f(G)$ of a continuous, piecewise linear, one-to-one mapping $f : G \to S$. The embedding is *cellular* if every connected component of $S \setminus f(G)$ (a *region*) is homeomorphic to an open disc.

25.3 Remark Intuitively, an embedding $f : G \to S$ is a "crossing-free drawing" of G on the surface S; the graph G is then usually identified with its embedded image $f(G)$.

25.4 Given a graph G, the *orientable (nonorientable) genus* of G is the smallest genus of a compact, connected, orientable (nonorientable) surface on which G embeds.

25.5 Let $D = (V, \mathcal{B})$ be a balanced incomplete block design (BIBD). The *incidence graph* I_D of D has vertex set $V \cup \mathcal{B}$ and edge set $\{(v, B);\ v \in V,\ B \in \mathcal{B},\ v \in B\}$.

25.6 Construction *Embedding of a design.* Let $D = (V, \mathcal{B})$ be a BIBD(v, b, r, k, λ). Take an embedding of I_D on some surface S. At any vertex $B \in \mathcal{B}$ of I_D perform the following operations:

(1) Choose a local orientation on S at B and form a cyclic list $(v_1, v_2, \ldots, v_k)$ of the k vertices adjacent to B in I_D in the order they appear around B in the chosen orientation.

(2) Add k new edges (piecewise linear curves) e_i on S, $1 \leq i \leq k$, joining v_i with v_{i+1} (mod k) in such a way that each e_i is contained in a sufficiently narrow band on one side of the path $v_i B v_{i+1}$ on S and so that no intersections on S in internal points of any edges arise.

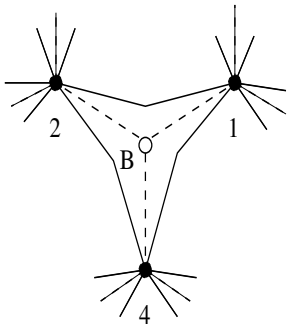
(3) Discard from S the vertices $B \in \mathcal{B}$ together with the open arcs $v_i B$ of I_D.

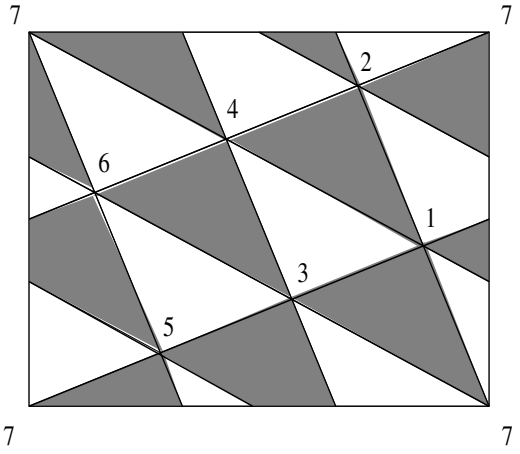
25.7 The embedded graph $H(I_D)$ from Construction 25.6 is an *embedding of the design D on S*. By definition, every embedding of D on S is induced by an embedding of I_D as described. For each $B \in \mathcal{B}$ the open topological disc bounded by the closed walk $e_1 e_2 \ldots e_k$ in $H(I_D)$ and having contained B before discarding is a *block region*; the remaining regions are *nonblock regions*. The embedding of D is *cellular* if each nonblock region (and hence each region) of the embedding is homeomorphic to an open disc.

25.8 Remark Since I_D is a bipartite graph, the embedding of D has a natural proper 2-colorings of regions given by the partition into block and non-block regions.

25.9 Example Remark 25.10 displays an embedding of the $(7, 3, 1)$-design $D = (V, \mathcal{B})$ with $V = \{1, 2, 3, 4, 5, 6, 7\}$ and $\mathcal{B} = \{\{i, i+1, i+3\} \text{ (mod } 7);\ 1 \leq i \leq 7\}$ on a torus, with block regions shaded. The underlying embedded graph $H_I(D)$ is isomorphic to the complete graph of order 7.

25.10 Remark Left: Illustration of Step (2) in Construction 25.6. Right: An embedding of D.





25.11 Proposition (Euler's formula for embedded designs) Suppose that a BIBD(v, b, r, k, λ) is cellularly embedded on an orientable surface S of genus γ, or on a nonorientable surface of genus $\tilde{\gamma}$, with r non-block regions. Then, $v - b(k-1) + r$ is equal to $2 - 2\gamma$ if S is orientable and to $2 - \tilde{\gamma}$ if S is nonorientable.

25.2 The Genus of a Design

25.12 Let D be a BIBD. The *orientable genus* $\gamma(D)$ (*nonorientable genus* $\tilde{\gamma}(D)$) of D is the orientable (nonorientable) genus of its incidence graph I_D.

25.13 Remark The genus of the incidence graph I_D should not be confused with the genus of the graph $H(I_D)$ constructed in Construction 25.6.

25.14 Remark Any embedding of a design D on an orientable surface of genus $\gamma(D)$ is cellular. Counterexamples exist for nonorientable embeddings.

25.15 Proposition [2132] A BIBD(v, b, r, k, λ) is planar (genus 0) if and only if either $k = 1$, or $k = 2$ and $2 \le v \le 4$, or else $k = 3$ and $(v, b, r, k, \lambda) = (3, 1, 1, 3, 1)$, $(3, 2, 2, 3, 2)$ or $(4, 4, 3, 3, 2)$.

25.16 Proposition [2132] For every $n \ge 2$ the orientable genus of the BIBD$(n, n, n-1, n-1, n-2)$ is equal to $\lceil (n-1)(n-4)/4 \rceil$.

25.17 Theorem [2131] Let $D = PG(2, q)$ be the desarguesian finite projective plane over a field of order q (a symmetric $(q^2+q+1, q+1, 1)$-design). Then, $\gamma(D) = (q^3-q^2-q+1)/3$ if $q \equiv 2 \pmod 3$, and $\gamma(D) = (q^3 - q^2 - q + 1)/3 + O(q^2)$ if $q \equiv 1 \pmod 3$. Moreover, if $D' = -PG(2, q)$ is the inverse plane on the same point set, then $D \cup D'$ is a BIBD$(q^2 + q + 1, 2(q^2 + q + 1), 2(q + 1), q + 1, 2)$ and $\gamma(D \cup D') = (q^3 - q^2 - q)/2$ if q is a power of 2.

25.18 Theorem Let D be a Steiner triple system of order n (STS(n)), $n \equiv 1$ or $3 \pmod 6$. Then, $\gamma(D) \ge \lceil (n-3)(n-4)/12 \rceil$ and $\tilde{\gamma}(D) \ge \lceil (n-3)(n-4)/6 \rceil$ for $n > 7$, with $\tilde{\gamma}(D) = 3$ for $D = \text{STS}(7)$.

25.19 Remark If $D = \text{STS}(n)$, then for any embedding of I_D the corresponding graph $H(I_D)$ is the complete graph K_n. Therefore, Proposition 25.18 is a consequence of the Map Color Theorem [1806]. It is believed that equality holds in *all* cases in Theorem 25.18.

25.3 Bi-Embeddings of Steiner Triple Systems

25.20 Remark Suppose that $D = \text{STS}(n)$ has an orientable embedding on a surface of genus $(n-3)(n-4)/12$ for $n \equiv 3$ or $7 \pmod{12}$, or that D has a nonorientable embedding on a surface of genus $(n-3)(n-4)/6$ for $n \equiv 1$ or $3 \pmod 6$. In both cases, all regions of the embeddings are triangular. It follows that the nonblock regions of the embeddings determine another embedded STS(n) D', possibly isomorphic to D, giving thus a pair of STS(n) simultaneously embedded in one surface.

25.21 Two Steiner triple systems D, D' of the same order n are orientably (nonorientably) *bi-embeddable* if there is a triangular embedding of K_n on an orientable (nonorientable) surface, the regions of which can be properly two-colored such that the STS induced by all regions of color 1 (color 2) isomorphic to D (D').

25.22 Proposition [214, 212] All possible pairs of the 80 isomorphism classes of STS(15) are nonorientably bi-embeddable. Referring to the list of all STS(15) in Table II.1.28, the systems #1 and #2 are not orientably bi-embeddable; and neither is #2 with itself. For any k, $3 \le k \le 80$ and $k \ne 79$, the STS(15) #k orientably bi-embeds with itself.

25.23 Theorem [295, 948] For $n \equiv 7$ or $19 \pmod{36}$, $n \equiv 15 \pmod{60}$, $n \equiv 15$ or $43 \pmod{84}$, and $n \equiv 27 \pmod{108}$, the number of nonisomorphic pairs of STS(n) that admit an (orientable as well as nonorientable) bi-embedding is at least $2^{cn^2 - o(n^2)}$ for an absolute constant c.

25.24 Remark The number in Theorem 25.23 is still far from $n^{n^2/3}$, which is the asymptotic number of nonisomorphic pairs of STS(n). Nevertheless, it has been suggested that for n sufficiently large, every pair of STS(n) admits an orientable as well as a nonorientable bi-embedding.

25.25 Remark A pair of bi-embedded STS(n) forms a special case of a twofold triple system. In general, there is a one-to-one correspondence between 2-fold triple systems of order n (BIBD with $v = n$, $k = 3$ and $\lambda = 2$) and triangular embeddings of K_n on generalized pseudosurfaces (obtained from a collection of compact surfaces by a finite number of identifications, of finitely many points each; in the embedding the points arising from identification are assumed to carry a vertex of K_n).

25.4 Bi-Embeddings of Latin Squares

25.26 Remark Let $T(K_{n,n,n})$ be an orientable triangular embedding of the complete tripartite graph $K_{n,n,n}$ with vertex tripartition $V_1 \cup V_2 \cup V_3$ into independent sets, each of order n. Then, regions of $T(K_{n,n,n})$ can be properly two-colored, say, black and white. For every $i \in V_1$ and $j \in V_2$, there exist unique $k = L_b(i,j)$ and $k' = L_w(i,j)$ in V_3 such that $\{i,j,k\}$ and $\{i,j,k'\}$ are vertices of a black and a white triangular region, respectively. The mappings L_b and L_w determine a pair of *latin squares* of order n.

25.27 A pair L_1 and L_2 of latin squares of order n has a *bi-embedding* if there is an orientable triangular embedding $T(K_{n,n,n})$ with a proper 2-coloring of its regions such that $L_b \cong L_1$ and $L_w \cong L_2$.

25.28 Remark In [942], all bi-embeddings of pairs of latin square of order n where $3 \le n \le 6$ are given, and the corresponding results for $n = 7$ are summarized.

See Also

§II.5	Any pair of STS(n) yields a triangular embedding of K_n on some generalized pseudosurface.
§VI.35	Mendelsohn triple systems correspond to triangular embeddings of complete graphs on oriented generalized pseudosurfaces.
§VI.12	Bi-embeddings of latin squares of order n and the corresponding triangular embeddings of complete tripartite graphs $K_{n,n,n}$ yield Hamilton cycle systems for $2K_{n,n}$.
[211]	Cyclic bi-embeddings of (cyclic) STS(n) for $n \equiv 7 \pmod{12}$.
[947]	A proof of the Heawood Map Color Theorem for $n \equiv 3 \pmod{12}$ using bi-embeddings of the classical Bose STS(n) with itself.
[2133]	Embeddings of finite geometries, in particular, affine 2-dimensional geometries, and partial geometries, on generalized pseudosurfaces.
[2134]	A discussion of embeddings of biplanes, that is, symmetric $(v,k,2)$-designs, on generalized pseudosurfaces.

References Cited: [211, 212, 214, 295, 942, 947, 948, 1806, 2131, 2132, 2133, 2134]

26 Graphical Designs

Yeow Meng Chee
Donald L. Kreher

26.1 Definition and Graphical Designs of Type 1^r

26.1 A nontrivial t-(v, K, λ) tBD $(X, \mathcal{B})$ is *graphical of type* $n_1^{r_1} n_2^{r_2} \cdots n_s^{r_s}$ if

1. X is the set of v edges of the complete r-partite graph $\Gamma = K_{n_1^{r_1}, n_2^{r_2}, \ldots, n_s^{r_s}}$, and
2. whenever B is a block and α is an automorphism of Γ, then $\alpha(B)$ is also a block.

26.2 **Remark** t-wise balanced designs (or tBD) are defined in §VI.63.

26.3 **Remarks** The block set $\mathcal{B}$ of a graphical design is a union of orbits under the action of $\mathrm{Aut}(\Gamma)$ on the edges of Γ. The notation of type $n_1^{r_1} n_2^{r_2} \cdots n_s^{r_s}$ is adopted from that used for group divisible designs (see §IV.1), because Γ is a group divisible design of this type with block size 2.

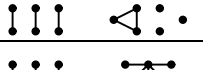
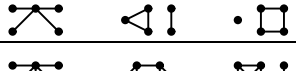
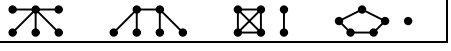
26.4 **Remarks** Graphical tBDs of type 1^r, for $r \geq 2$, are *graphical designs*. In particular, a graphical design $(X, \mathcal{B})$ of type 1^r has parameters t-$(\binom{r}{2}, \mathcal{K}, \lambda)$ and has the symmetric group S_r as the automorphism group. So X is the set of $v = \binom{r}{2}$ labeled edges of the undirected complete graph K_r, and if $B \in \mathcal{B}$, then all subgraphs of K_r isomorphic to B are also in $\mathcal{B}$.

26.5 **Theorem** [1343] The only simple graphical t-$(10, k, \lambda)$ designs (note $10 = \binom{5}{2}$) with $t \geq 2$ have parameters: $(t, k, \lambda) = (2, 3, 4)$, $(2, 4, 2)$, $(2, 4, 4)$, $(2, 4, 8)$, $(2, 4, 10)$, $(2, 4, 12)$, $(2, 5, 16)$, $(2, 5, 20)$, $(3, 4, 1)$, $(3, 5, 6)$.

26.6 **Table** [1343] Parameters of the only simple graphical t-$(15, k, \lambda)$ designs with $t \geq 2$.

(t, k, λ)							
$(2, 3, 1)$	$(2, 4, 6)$	$(2, 4, 24)$	$(2, 4, 30)$	$(2, 4, 36)$	$(2, 7, 3)$	$(2, 7, 24)$	$(2, 7, 27)$
$(2, 7, 30)$	$(2, 7, 33)$	$(2, 7, 36)$	$(2, 7, 39)$	$(3, 5, 30)$	$(3, 6, 100)$	$(3, 7, 60)$	$(3, 7, 75)$
$(3, 7, 90)$	$(3, 7, 135)$	$(3, 7, 150)$	$(3, 7, 165)$	$(3, 7, 180)$	$(3, 7, 225)$	$(3, 7, 240)$	$(4, 7, 60)$
$(2, 5, \lambda) : 16 \leq \lambda \leq 142,\ \lambda \equiv 0, 2, 4, 6 \pmod{10},\ \lambda \neq 20, 50$							
$(2, 6, \lambda) : 10 \leq \lambda \leq 355,\ \lambda \equiv 0, 10 \pmod{15}$							
$(2, 7, \lambda) : 48 \leq \lambda \leq 642,\ \lambda \equiv 0 \pmod{3}$							

26.7 **Table** [500] All graphical t-$(v, K, 1)$ designs.

Parameters	Representation
1-$(6, 2, 1)$	
2-$(15, 3, 1)$	
2-$(15, \{3, 5\}, 1)$	
3-$(10, 4, 1)$	
4-$(15, \{5, 7\}, 1)$	

26.8 Theorem [500] The only simple graphical t-$(v, K, 2)$ designs with $t > 1$ have the parameters: 2-$(6, \{3, 4\}, 2)$, 2-$(10, \{3, 4\}, 2)$, 2-$(10, 4, 2)$, 2-$(15, \{3, 6\}, 2)$, 2-$(15, \{5, 6\}, 2)$, and 3-$(10, \{4, 5, 6\}, 2)$.

26.9 Table [500] Parameters of the only simple graphical t-$(v, K, 3)$ designs with $v \leq 15$ (excluding those presented in Theorem 26.5 and Table 26.6).

(t, v, K)					
$(1, 6, \{2, 3\})$	$(1, 6, \{2, 4\})$	$(1, 10, 2)$	$(1, 10, 3)$	$(1, 15, 3)$	$(2, 10, \{4, 6\})$
$(2, 15, \{3, 4\})$	$(2, 15, \{3, 5, 6\})$	$(2, 15, \{3, 10\})$	$(3, 10, \{4, 6\})$	$(3, 15, \{4, 5, 7\})$	$(3, 15, \{7, 8\})$

26.10 Theorem [463, 464, 237] A simple graphical 2-$(v, 3, \lambda)$ design exists if and only if $(v, \lambda) \in \{(10, 4), (15,1), (28,6), (28,10), (55, 25)\}$. The only simple graphical 3-$(v, 4, \lambda)$ design is the 3-$(10, 4, 1)$ design. There exist no simple graphical 4-$(v, 5, \lambda)$ or 5-$(v, 6, \lambda)$ designs.

26.11 Table [463] Parameters of all simple graphical 2-$(v, 4, \lambda)$ designs.

(v, λ)						
$(10, 2)$	$(10, 4)$	$(10, 8)$	$(10, 10)$	$(10, 12)$	$(15, 6)$	$(15, 24)$
$(15, 30)$	$(15, 36)$	$(21, 6)$	$(21, 12)$	$(21, 18)$	$(21, 36)$	$(21, 42)$
$(21, 45)$	$(21, 48)$	$(21, 51)$	$(21, 54)$	$(21, 57)$	$(21, 60)$	$(21, 63)$
$(21, 66)$	$(21, 69)$	$(21, 72)$	$(21, 75)$	$(21, 78)$	$(21, 81)$	$(21, 84)$
$(28, 5)$	$(28, 55)$	$(28, 80)$	$(28, 85)$	$(28, 95)$	$(28, 110)$	$(28, 120)$
$(28, 125)$	$(28, 135)$	$(28, 150)$	$(36, 15)$	$(36, 90)$	$(36, 111)$	$(36, 120)$
$(36, 135)$	$(36, 165)$	$(36, 210)$	$(36, 231)$	$(36, 240)$	$(36, 255)$	$(36, 276)$
$(45, 63)$	$(45, 105)$	$(45, 252)$	$(45, 357)$	$(45, 378)$	$(45, 420)$	$(55, 168)$
$(55, 336)$	$(55, 504)$	$(78, 630)$	$(78, 1080)$	$(78, 1350)$	$(91, 836)$	$(91, 1430)$
$(91, 1496)$	$(105, 1320)$	$(105, 1326)$	$(105, 1650)$	$(105, 1656)$	$(105, 1782)$	$(105, 1788)$
$(105, 1980)$	$(105, 1986)$	$(105, 2112)$	$(105, 2118)$	$(105, 2442)$	$(105, 2448)$	$(153, 4935)$
$(153, 5025)$	$(253, 14535)$					

26.12 Table [237, 465, 1336, 1351] Simple graphical t-(v, k, λ) designs are known in the following sporadic cases.

(t, k, v)	λ
(2,5,21)	7, 12, 19, 22, 34, 35, 47, 50, 52, 55, 57, 60, 62, 64, 67, 69, 70, 72, 77, 79, 82, 84, 89, 94, 95, 100, 120
(2,6,21)	13, 30, 38, 45, 48, 50, 51, 55, 58, 60, 61, 63, 68, 70.
(2,7,21)	42, 63, 78, 84, 105
(2,8,21)	84, 168, 336, 672
(2,9,21)	12, 54, 72, 108, 216, 432, 864
(2,10,21)	99, 162, 180, 189
(2,5,28)	60, 100, 140, 160, 200, 240, 260, 300, 340, 360
(2,6,28)	25, 40, 50, 65, 70, 80, 90, 100
(2,7,28)	16, 140, 156, 182, 198
(2,8,28)	70, 210
(2,9,28)	40, 160, 320, 480, 640, 960, 1920, 3840
(2,5,36)	60, 80, 140, 164, 180, 224, 240, 244, 480, 720
(2,6,36)	20, 45, 120, 240, 540, 720, 1080, 2160, 4320
(2,7,36)	210, 246, 336, 372, 420, 456, 462, 546
(2,5,55)	4512, 4540, 4652, 5212, 5352, 5576, 5912, 7312, 7256, 7900, 7942, 8572, 8712, 8600
(2,5,171)	131040
(2,5,741)	29216880
(3,5,21)	3, 30, 33, 39, 48, 69, 75
(3,6,21)	68, 100, 108, 128, 136, 140, 148, 156, 160, 168, 176, 180, 188, 196, 200

(t,k,v)	λ
(3,7,21)	105, 120, 210, 225, 315
(3,8,21)	168, 252, 336, 420
(3,5,28)	30, 150
(3,6,28)	80, 120, 180, 220, 240, 260
(3,7,28)	210, 225, 240, 245, 275
(3,8,28)	168, 378, 672

(t,k,v)	λ
(3,9,28)	280
(3,5,36)	180, 270
(4,6,28)	132
(5,7,28)	93
(5,8,28)	756, 791, 840, 875
(5,7,36)	165

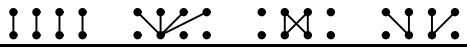
26.13 Theorem [499] For any pair (t,λ) with $t>1$ or λ odd, there cannot exist a graphical t-$(\binom{n}{2},K,\lambda)$ design with $n \geq 2t+\lambda+4$. Thus, in particular, for each such pair (t,λ), there are only a finite number of nontrivial graphical t-(ν,K,λ) designs. If $t>1$ or $\lambda \neq 2$, there do not exist *simple* nontrivial graphical t-$(\binom{n}{2},K,\lambda)$ designs with $n \geq 2t+\lambda+4$.

26.14 Theorem [237, 466] There exists only finite many nontrivial graphical t-(v,k,λ) designs for any fixed pair (t,k) whenever $t=2$ or $2 \leq t < k \leq 6$ or $k \leq 4t/3$.

26.2 Bigraphical Designs

26.15 Remarks Graphical tBDs of type m^1n^1 $(m \leq n)$ are *bigraphical*. A bigraphical design has parameters t-$(m \cdot n, \mathcal{K}, \lambda)$ and has $S_m \times S_n$ as the automorphism group when $m \neq n$ and the wreath product $S_n \, wr \, S_2$ otherwise. Here X is the set of all labeled edges of the complete bipartite graph $K_{m,n}$.

26.16 Example [1117] All bigraphical t-$(v,K,1)$ designs.

Parameters	Representation
1-$(n,n^2,1)$	$K_{1,n}$
1-(4, 2, 1)	
2-(9, 3, 1)	
3-(16, 4, 1)	
3-(16, {4, 6}, 1)	
5-(16, {6, 8}, 1)	

26.17 Table [2127] Parameters of the only bigraphical simple t-$(v,K,2)$ designs.

(t,v,K)					
$(1,mn,m) : 2 \leq m \leq n$			$(1,mn,n) : 2 \leq m \leq n$		
$(1,3n,2n) : n \geq 3$			$(1,3n,2) : n \geq 3$		
$(1,3m,2m) : m \in \{2,3\}$			$(1,3m,2) : m \in \{2,3\}$		
$(1,mn,\{m,n\}) : 2 \leq m \leq n$			$(1,4,2)$	$(1,6,2)$	$(1,9,3)$
$(2,9,3)$	$(2,9,\{3,4\})$	$(2,9,\{3,6\})$	$(2,12,3)$	$(2,12,\{3,4\})$	$(2,12,\{3,5\})$
$(2,16,\{3,4\})$	$(2,16,4)$	$(2,16,6)$	$(3,8,4)$	$(3,8,\{4,6\})$	$(3,10,4)$
$(3,10,\{4,5\})$	$(3,16,4)$	$(3,16,\{4,6\})$	$(3,20,4)$	$(3,20,\{4,5\})$	$(3,25,\{4,5\})$
$(5,12,6)$	$(5,16,\{6,8\})$				

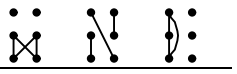
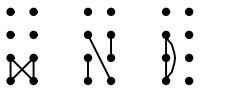
26.18 Remark [422] A bigraphical 3-(77, 20, 3135283200) is known.

26.3 Graphical Designs of Type $\mathbf{n^r}$

26.19 Remarks Graphical tBDs of type n^r with $\lambda = 1$ are studied in [1698]. A graphical tBD of type n^r has parameters $t\text{-}(n^2\binom{r}{2}, \mathcal{K}, \lambda)$ and has the wreath product $S_n \, wr \, S_r$ as the automorphism group. Here, X is the set of all labeled edges of the complete multi-partite graph $K_{\underbrace{n, n, \ldots n}_{r}}$.

26.20 Table [1698] All graphical t-$(v, K, 1)$ designs of type n^r with $n \geq 2$ and $r \geq 3$.

Parameters	Representation
1-$(6n^2, 2n^2, 1)$	$K_{n,n} \dot{\cup} K_{n,n}$
1-$(6\binom{r}{2}, n^2, 1)$	$K_{n,n}$
1-$(4\binom{r}{2}, 2, 1)$, $r \geq 3$	

Parameters	Representation
2-$(12, \{3, 4\}, 1)$	
2-$(24, \{3, 4\}, 1)$	

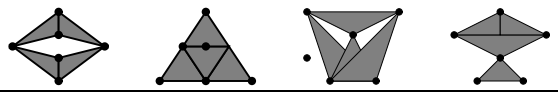
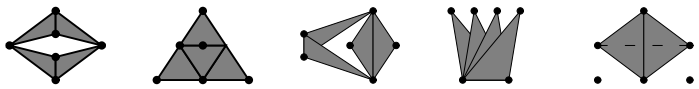
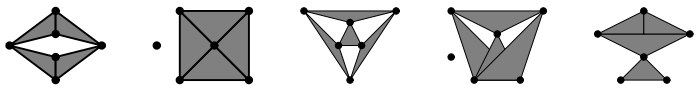
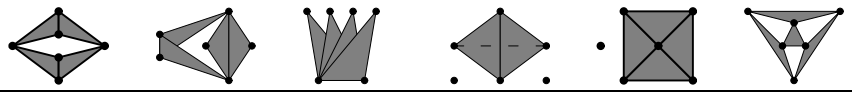
26.4 Generalization to Hypergraphs

26.21 A nontrivial t-(v, K, λ) tBD $(X, \mathcal{A})$ is *r-hypergraphical* if

1. X is the set of $v = \binom{n}{r}$ edges of the complete r-hypergraph $K_n^{(r)}$, and
2. $\mathcal{A}$ is closed under isomorphism of hypergraphs: that is, whenever $A \in \mathcal{A}$ and σ is automorphism of $K_n^{(r)}$, then $\sigma(A) \in \mathcal{A}$.

26.22 Remarks An r-hypergraphical t-$(\binom{n}{r}, K, \lambda)$ design has S_n as an automorphism group. Also note that a 2-hypergraphical t-(v, K, λ) design is a graphical t-(v, K, λ) design.

26.23 Example [641] The four hypergraphical 3-$(20, 4, 1)$ designs.

	Representation
1	
2	
3	
4	

See Also

§II.1	Some graphical designs are block designs with symmetric groups as automorphism groups.
§VI.63	Graphical designs are t-wise balanced designs with symmetric groups as automorphism groups.
[2046]	Sections 3.4 and 3.5 present another interpretation of graphical designs, obtained from strongly regular graphs.

References Cited: [237, 422, 463, 464, 465, 466, 499, 500, 641, 1117, 1336, 1343, 1351, 1698, 2046, 2127]

27 Grooming

Jean-Claude Bermond
David Coudert

27.1 Definitions and Examples

27.1 **Remark** Traffic grooming in networks refers to grouping low rate traffic into higher speed streams (containers) so as to minimize the equipment cost [762, 823, 925, 1620, 2111, 2209]. There are many variants according the type of network considered, the constraints used, and the parameters one wants to optimize, each giving rise to interesting design theory problems (particularly related to graph decompositions; see §VI.24).

To fix ideas, suppose that an optical network is represented by a directed graph (in many cases a symmetric one) on n vertices, for example, an unidirectional ring $\vec{C}_n$ or a bidirectional ring C_n^*. Also provided is a traffic matrix, that is, a family of connection requests represented by a multidigraph I (the number of arcs from i to j corresponding to the number of requests from i to j). An interesting case is when there is exactly one request from i to j; then $I = K_n^*$. Satisfying a request from i to j consists of finding a route (directed path) in G and assigning it a wavelength. The grooming factor, g, means that a request uses only $1/g$ of the bandwith available on a wavelength along its route. Said otherwise, for each arc e of G and for each wavelength w, there are at most g paths of wavelengths w containing arc e.

During the 90s, research concentrated on minimizing the number of wavelengths used. Meanwhile the bandwidth of each wavelength (> 10 Gbit/s), the number of wavelengths per fiber (> 100), and the number of fibers per cable (> 100) have exploded, thus moving the operational cost of a wavelength into the terminal equipment cost: filters, optical cross-connect, add/drop multiplexer (ADM), and so on. For example, in a node of an optical network, place an ADM only for those wavelengths carrying a request to be added or dropped in this node. So now the objective is to minimize the total number of ADMs in the network, which is a challenging issue.

27.2 [221] *Grooming problem*: Given a digraph G (network), a digraph I (set of requests), and a grooming factor g, find for each arc $r \in I$ a path $P(r)$ in G and a partition of the arcs of I into subgraphs I_w, $1 \le w \le W$, such that $\forall e \in E(G)$ $\text{load}(I_w, e) = |\{P(r); r \in E(I_w); e \in P(r)\}| \le g$. The objective is to minimize $\sum_{w=1}^{W} |V(I_w)|$, and this minimum is denoted by $A(G, I, g)$.

27.3 A *transitive tournament* on n vertices, TT_n, is the digraph with arcs $\{(i, j) \mid 1 \le i < j \le n\}$. The notation $\{a, b, c\}$ is for the TT_3 with arcs (a, b), (a, c), and (b, c).

27.4 **Remark** When $G = P_n^*$, the shortest path from i to j is unique, and we can split the requests into two classes, those with $i < j$ and those with $i > j$. Therefore, the grooming problem for P_n^* can be reduced to two distinct problems on $\vec{P}_n$. In particular, $A(P_n^*, K_n^*, g) = 2A(\vec{P}_n, TT_n, g)$.

27.5 **Example** $A(\vec{P}_7, TT_7, 2) = 20$, and the partition consists of the 6 subgraphs

{1,2,3}+{3,5,7} {2,4,5} {3,4,6} {1,5,6} {2,6,7} {1,4,7}

27.6 Theorem [217] When n is odd, $A(\vec{P}_n, TT_n, 2) = \lceil (11n^2 - 8n - 3)/24 \rceil$. When n is even, $A(\vec{P}_n, K_n, 2) = (11n^2 - 4n)/24 + \varepsilon(n)$, where $\varepsilon(n) = 1/2$ when $n \equiv 2, 6 \pmod{12}$, $\varepsilon(n) = 1/3$ when $n \equiv 4 \pmod{12}$, $\varepsilon(n) = 5/6$ when $n \equiv 10 \pmod{12}$, and $\varepsilon(n) = 0$ when $n \equiv 0, 8 \pmod{12}$.

27.7 Remark In a unidirectional cycle $\vec{C}_n$, the path from i to j is unique. Without loss of generality one can assign the same wavelength to the two requests (i, j) and (j, i); then the two associated paths contain each arc of $\vec{C}_n$. Therefore, the load condition becomes $|E(I_w)| \le g$ and the grooming problem is given in the next definition.

27.8 [221] *Grooming problem for $G = \vec{C}_n$:* Given n and g, partition K_n into subgraphs B_w, $1 \le i \le W$, such that $|E(B_w)| \le g$, which minimizes $\sum_{w=1}^{W} |V(B_w)|$. The minimum value is $A(\vec{C}_n, K_n^*, g)$.

27.9 Remark The partition in the grooming problem for $G = \vec{C}_n$ is obtained by associating to each B_w of the partition its symmetric digraph B_w^* and letting $I_w = B_w^*$.

27.10 Example $A(\vec{C}_4, K_4^*, 3) = 7$, using a partition of K_4 consisting of the K_3 $\{1, 2, 3\}$ and the $K_{1,3}$ with edges $\{1, 4\}$, $\{2, 4\}$, and $\{3, 4\}$. $A(\vec{C}_7, K_7^*, 3) = 21$ using a (7,3,1) design (Steiner triple system) and $A(\vec{C}_{13}, K_{13}^*, 6) = 52$ using a (13,4,1) design.

27.11 Theorem [218] $A(\vec{C}_n, K_n^*, 3) = n(n-1)/2 + \varepsilon_3(n)$, where $\varepsilon_3(n) = 0$ when $n \equiv 1, 3 \pmod 6$, $\varepsilon_3(n) = 2$ when $n \equiv 5 \pmod 6$, $\varepsilon_3(n) = \lceil N/4 \rceil + 1$ when $n \equiv 8 \pmod{12}$, and $\varepsilon_3(n) = \lceil N/4 \rceil$ otherwise.

27.12 Theorem [1141] $A(\vec{C}_n, K_n^*, 4) = n(n-1)/2$.

27.13 Theorem [220] $A(\vec{C}_n, K_n^*, 5) = 4\lfloor n(n-1)/10 \rfloor + \varepsilon_5(n)$, where $\varepsilon_5(n) = 0$ when $n \equiv 0, 1 \pmod 5$, $n \ne 5$, $\varepsilon_5(5) = 1$, $\varepsilon_5(n) = 2$ when $n \equiv 2, 4 \pmod 5$, $n \ne 7$, $\varepsilon_5(7) = 3$, $\varepsilon_5(n) = 3$ when $n \equiv 3 \pmod 5$, $n \ne 8$, and $\varepsilon_5(8) = 4$.

27.14 Theorem [219] When $n \equiv 0 \pmod 3$, then $A(\vec{C}_n, K_n^*, 6) = \lceil n(3n-1)/9 \rceil + \varepsilon_6(n)$, where $\varepsilon_6(n) = 1$ when $n \equiv 18, 27 \pmod{36}$, and $\varepsilon_6(n) = 0$ otherwise, except for $n \in \{9, 12\}$ and some possible exceptions when $n \le 2580$.

When $n \equiv 1 \pmod 3$, $A(\vec{C}_n, K_n^*, 6) = \lceil n(n-1)/3 \rceil + \varepsilon_6(n)$, where $\varepsilon_6(n) = 2$ when $n \equiv 7, 10 \pmod{12}$, and 0 otherwise, except for $A(\vec{C}_7, K_7^*, 6) = 17$, $A(\vec{C}_{10}, K_{10}^*, 6) = 34$, and $A(\vec{C}_{19}, K_{19}^*, 6) = 119$.

When $n \equiv 2 \pmod 3$, then $A(\vec{C}_n, K_n^*, 6) = (n^2 + 2)/3$, except possibly for $n = 17$.

27.15 Remark In another grooming problem [222], the requests are routed via different pipes. Each pipe contains at most g requests, and the objective is to minimize the total number of pipes (as equipment is placed only at the terminal nodes of the pipe). Thus, given a digraph I (requests) and a grooming factor g, the problem is to find a virtual multidigraph H and, for each arc $r \in I$, a path $P(r)$ in H such that $\forall e \in E(H)$, $\text{load}(I, e) \le g$. The objective is to minimize $|E(H)|$; $T(I, g)$ denotes this minimum.

27.16 Example When $I = K_4^*$ and $C = 2$, then $H = C_4^*$. Requests $(i, i+1)$ ($(i, i-1)$, resp.) are routed via arc $(i, i+1)$ ($(i, i-1)$, resp.), requests $(1, 3)$ and $(3, 1)$ are routed clockwise, and $(2, 4)$ and $(4, 2)$ counterclockwise.

27.17 Remark For $C = 2$, the problem can be reduced to a partition of K_n^* or $(K_n - e)^*$ in TT_3; see VI.20 and VI.35. For $C = 3$, the result follows from the existence of a $PBD(n, \{3, 4, 5\})$ for $n \ne 6, 8$; see IV.3.

27.18 Theorem [222] $T(K_n^*, 2) = \lceil 2n(n-1)/3 \rceil$ and $T(K_n^*, 3) = n(n-1)/2$.

See Also

§VI.20	Directed designs.
§VI.24	Graph decompositions
§VI.35	Mendelsohn designs
[563]	A variant with bidirectional traffic.

References Cited: [217, 218, 219, 220, 221, 222, 563, 762, 823, 925, 1141, 1620, 2111, 2209]

28 Hall Triple Systems

Lucien Bénéteau

28.1 Definition and Examples

28.1 A *Hall triple system* (HTS) is a pair $(S, \mathcal{L})$ where S is a set of elements (*points*) and $\mathcal{L}$ a set of *lines* satisfying

1. Every line is a 3-subset of S,
2. Any two distinct points lie in exactly one line, and
3. Any two intersecting lines generate a subsystem isomorphic to the affine plane of nine points AG(2,3).

28.2 **Example** Let S be some $(n+1)$-dimensional vector space over $\mathbb{F}_3$, with $n \geq 3$. Let $\{e_0, e_1, \ldots, e_n\}$ be a basis for S. For any two points $x = \sum \alpha^i e_i$ and $y = \sum \beta^i e_i$ set $z = x \circ y$ as defined by $x + y + z = (\alpha^1 - \beta^1)(\alpha^2\beta^3 - \alpha^3\beta^2)e_0$. This defines a binary operation on S. One has either $x = y = z$, or the three points x, y, z are pairwise distinct. The 3-subsets of the form $\{x, y, z\}$ such that $z = x \circ y$ provide S with a structure of an HTS. This particular HTS is referred to as $H(n)$.

28.3 **Example** Let S be a 7-dimensional vector space over $\mathbb{F}_3$. Let $\{e_0, e_1, \ldots, e_n\}$ be a basis for S. Define the lines as the 3-subsets of the form $\{x, y, z\}$ such that $x = \sum \alpha^i e_i$, $y = \sum \beta^i e_i$ and $x+y+z = ((\alpha^1-\beta^1)(\alpha^2\beta^3-\alpha^3\beta^2+\alpha^4\beta^7-\alpha^7\beta^4)+(\alpha^2-\beta^2)(\alpha^5\beta^7-\alpha^7\beta^5)+(\alpha^3-\beta^3)(\alpha^6\beta^7-\alpha^7\beta^6)+(\alpha^4-\beta^4)(\alpha^5\beta^6-\alpha^6\beta^5))e_0$. The so-defined family of lines provides S with a structure of HTS whose order is 3^8 that admits a minimal generator set of 8 points. It has been established that there are exactly 11 such HTSs.

28.4 **Example** Any affine space $\mathrm{AG}(n, 3)$ over $\mathbb{F}_3$ with the usual lines may be viewed as an HTS. Such an HTS is an *affine* HTS.

28.2 Existence

28.5 **Theorem** The cardinality of any HTS is 3^m for some integer $m \geq 2$. Nonaffine HTS of order 3^m exist for any $m \geq 4$ and do not exist for $m = 2$ or 3.

28.6 **Remark** The existence of a nonaffine HTS of order $3^m > 3^3$ is provided by $H(m-1)$ in Example 28.2. For the orders 3^4 and 3^5, there is a unique nonaffine HTS, namely, $H(3)$ and $H(4)$, respectively.

28.7 **Table** The maximum number of nonisomorphic HTSs of order 3^m.

Order	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	3^m
Affine HTS	1	1	1	1	1	1	1	1	1	1
Nonaffine HTS	0	0	0	1	1	3	12	≥ 45	?	?

28.3 The Rank of a HTS

28.8 The rank r of a HTS is the smallest integer r such that there exists a generator set of r points.

28.9 Theorem In a Hall triple system of order 3^m the rank r is at most $m+1$, with equality only in the affine case. Moreover *any* minimal generator subset consists of exactly r distinct points.

28.10 Table The number of nonisomorphic HTSs of order 3^m of rank r.

Order	3^4	3^5	3^6	3^7	3^8
Rank 3 HTS	1	0	0	0	0
Rank 4 HTS	1	1	1	1	4
Rank 5 HTS	0	1	2	6	≥ 17
Rank 6 HTS	0	0	1	5	≥ 13
Rank 7 HTS	0	0	0	1	11
Rank 8 HTS	0	0	0	0	1

28.4 Equivalent Quasigroups and Groups

28.11 Remark All the classification theorems concerning the HTSs have been derived from their algebraic description in quasigroup theory, either in terms of distributive Steiner quasigroups or in terms of exponent 3 commutative Moufang loops.

The HTSs are a special case of Steiner triple systems. Any Steiner triple system may be provided with a structure of a *Steiner quasigroup* by setting $z = x \circ y$ when $\{x, y, z\}$ is a block of the design or when $x = y = z$.

28.12 A *Steiner quasigroup* is a commutative quasigroup whose binary operation $\circ$ satisfies $x \circ x = x$ and $(x \circ y) \circ y = x$.

28.13 Remark Given a Steiner quasigroup, one recovers a Steiner triple system by letting the blocks be the sets $\{x, y, z\}$ when $z = x \circ y$ and x and y are two distinct points.

28.14 Theorem The correspondence $(S, \mathcal{L}) \longrightarrow (S, \circ)$ between Steiner triple systems and Steiner quasigroups is one-to-one up to isomorphism.

28.15 Theorem A Hall triple system is a Steiner triple system whose related Steiner quasigroup is distributive; that is, the identity $a \circ (x \circ y) = (a \circ x) \circ (a \circ y)$ holds.

28.16 An *exponent 3 commutative Moufang loop* is a commutative quasigroup whose binary operation $x+y$ admits an identity element ω and satisfies the two identities $x+x+x = \omega$ and $(x + y) + (x + z) = (x + x) + (y + z)$.

28.17 Proposition An exponent 3 commutative Moufang loop arises from a Hall triple system S if one defines the sum of two points as $x + y = (x \circ y) \circ \alpha$, where α is an arbitrary fixed point of S. This binary law admits an identity element which is α. Different choices of the point α yield isomorphic loops.

28.18 Remark The kinship between HTSs and exponent 3 commutative Moufang loops recalls the kinship between affine spaces and vector spaces. The correspondence is one-to-one up to isomorphism. For various investigations concerning HTSs, the best setting is loop theory where powerful results due to Bruck can be used.

28.19 A group G is a *Fischer group* (in the restrictive sense) if the set $S = S(G)$ of order 2 elements generates G, contains at least two elements, and satisfies order$(xy) = 3$ for any two distinct elements x and y from S.

28.20 Proposition $S(G)$ may then be provided with a structure of a distributive Steiner quasigroup by $x \circ y = xyx$. So the lines of the related HTS are the sets of three involutions from G of the form (x, y, xyx). Any HTS arises in this way from various (nonisomorphic) Fischer groups. Among the different Fischer groups associated with some fixed HTS, say $(S, \mathcal{L})$, there is one and only one centerless group (up to isomorphism); it can be described as the group of permutations of S spanned by all the reflections of the form $x \longrightarrow \sigma \circ x$ with σ ranging in S.

28.5 Constructing HTSs via Exterior Algebra

28.21 Remark The construction of Example 28.2 may be generalized as follows. Consider some $(n+1)$-dimensional vector space S over $\mathbb{F}_3$, with $n > 2$, and with some chosen basis, say $e_0, e_1, e_2, \ldots e_n$. For any two points $x = \sum \alpha^i e_i$ and $y = \sum \beta^i e_i$, set $z = x \circ y$ when $x + y + z = \sum_{i<j<k} \Lambda_{ijk}(\alpha^i - \beta^i)(\alpha^j \beta^k - \alpha^k \beta^j)e_0$ where (Λ_{ijk}) for $i < j < k$ form a nonvanishing sequence of elements from $\mathbb{F}_3$. This defines a binary operation of a distributive Steiner quasigroup on S. The corresponding Hall triple system has rank $n + 1$.

28.22 Theorem Any rank $n+1$ Hall triple system of order 3^{n+1} arises in the manner described in Remark 28.21.

28.23 Let V be the n-dimensional vector space over $\mathbb{F}_3$ spanned by $e_1, e_2 \ldots, e_n$. Consider again a nonvanishing sequence (Λ_{ijk}) $i < j < k$ of elements from $\mathbb{F}_3$. The equalities

$$\phi(e_i, e_j, e_k) = \Lambda_{ijk} \text{ for } i < j < k$$

define a unique symplectic trilinear form ϕ from V^3 onto $\mathbb{F}_3$. Any two symplectic trilinear forms ϕ and ϕ' are *equivalent* when $\phi'(x, y, z) = \phi(f(x), f(y), f(z))$ for some automorphism f of V.

28.24 Proposition Two sequences $(\Lambda_{ijk}{}')$ and (Λ_{ijk}) give rise to equivalent symplectic trilinear forms if their related HTSs are isomorphic.

28.25 Proposition The so-defined correspondence between rank $n + 1$ HTS of order 3^{n+1} and nonvanishing symplectic trilinear forms of V (n dimensional vector space over $\mathbb{F}_3$) is one-to-one up to isomorphism for Hall triple systems and up to equivalence for symplectic trilinear forms.

28.26 Remark This correspondence may be extended by considering rank $n+1$ HTS or order greater than 3^{n+1} and nonvanishing symplectic trilinear mappings.

28.27 Remark Let V and W be vector spaces over $\mathbb{F}_3$ of dimension n and m respectively. The set $\mathrm{AT}(n, m)$ of symplectic trilinear mappings from V^3 to W whose images have rank m may be provided with a natural notion of equivalence (up to compositions with isomorphisms of V and W). Denote by $\alpha(n, m)$ the number of such equivalence classes. It can be shown that each class is related to an essentially unique HTS (see [2]). As a by-product one derives Theorem 28.28.

28.28 Theorem If $m = 1, 2$ or 3, then $\alpha(n, m)$ coincides with the maximum number $\sigma(n, m)$ of pairwise nonisomorphic rank $n + 1$ HTS of order 3^{n+m}. Particularly $\alpha(7, 1) = \sigma(7, 1) = 11$ and $\alpha(6, 2) = \sigma(6, 2) \geq 13$. If $m \geq 4$, then $\sigma(n, m) \geq 3 + \alpha(n, m)$.

28.29 Remark The main significance of Theorem 28.28 is that the classification of the Hall triple systems whose 3-order is not too large with respect to their rank r can be dealt with by counting orbits in $\mathrm{AT}(n, m)$. But among the rank r HTSs whose 3-order is larger than $3 + r$, there are some systems that are not constructible from symplectic trilinear mappings.

See Also

§II.2	Hall triple systems are a type of STS.
§III.2	Related material on quasigroups.
[186, 470, 1518]	Additional information about quasigroups and groups related to HTS.
[1015]	Cubic hypersurfaces might give rise to some HTS.

References Cited: [186, 470, 1015, 1518]

29 Howell Designs

Jeffrey H. Dinitz

29.1 Definitions, Examples, and Existence

29.1 Let S be a set of $2n$ *symbols*. A *Howell design* $H(s, 2n)$ (on symbol set S) is an $s \times s$ array, H, that satisfies:

1. every cell of H either is empty or contains an unordered pair of symbols from S,
2. each symbol of S occurs once in each row and column of H, and
3. every unordered pair of symbols occurs in at most one cell of H.

29.2 The pairs of symbols in the cells of an $H(s, 2n)$ can be thought of as the edges of a s regular graph on $2n$ symbols, the *underlying graph* of the Howell design.

29.3 An $H^*(s, 2n)$ is an $H(s, 2n)$ whose underlying graph contains a maximal independent set, one of size $2n - s$.

29.4 Examples An $H(4, 6)$, $H(6, 12)$ and an $H^*(4, 8)$ with independent set $\{1, 2, 3, 4\}$.

04		13	25
23	14	05	
	35	24	01
15	02		34

1 7	2 8	3 9	4 *a*	5 *b*	6 *c*	
2 3	*c* 7	4 5	8 9	6 1	*a* *b*	
b *c*	3 4	7 8	5 6	9 *a*	1 2	
5 *a*	6 *b*	1 *c*	2 7	3 8	4 9	
6 9	1 *a*	2 *b*	3 *c*	4 7	5 8	
4 8	5 9	6 *a*	1 *b*	2 *c*	3 7	

15	26	37	48
47	38	25	16
28	17	46	35
36	45	18	27

29.5 Theorem [90, 1963] Let s and n be positive integers, where n is even and $s+1 \leq 2n \leq 2s$. Then there exists an $H(s, 2n)$ if and only if $(s, 2n) \neq (2, 4)$, $(3, 4)$, $(5, 6)$, or $(5, 8)$.

29.6 Remark The proof of nonexistence of an $H(2, 4)$ is trivial. The ordered pairs $(3, 4)$ and $(5, 6)$ correspond to (nonexistent) Room squares of sides 3 and 5. The nonexistence of an $H(5, 8)$ is more difficult to establish; a reasonably short proof is given in [1823].

29.7 Remark The underlying graph of an $H(2n - 1, 2n)$ is the complete graph K_{2n}. The underlying graph of an $H(2m, 2m + 2)$ is the *cocktail party graph* $K_{2m+2} - f$, where

f is a 1-factor. Also, an $H(s, 2s)$ with underlying graph $K_{s,s}$ is equivalent to a pair of mutually orthogonal latin squares of order s. Existence or nonexistence of Howell designs with specified underlying graphs has been determined for all graphs on at most 10 vertices [1823].

29.2 Related Combinatorial Objects

29.8 Theorem The existence of a pair of orthogonal latin squares of side n implies the existence of an $H^*(n, 2n)$ with underlying graph $K_{n,n}$.

29.9 Remarks To construct an $H^*(n, 2n)$ from a pair of orthogonal latin squares of side n (on disjoint symbol sets), superimpose the two latin squares. The symbols from either of the symbol sets forms a maximal independent set in the underlying graph $K_{n,n}$. The $H^*(4, 8)$ in Example 29.4 was constructed in this manner. It is also interesting that there exists an $H(6, 12)$ (Example 29.4), yet there is no pair of orthogonal latin squares of side 6. Given H, an $H(n, 2n)$, one can only construct a pair of orthogonal latin squares of side n from H if the underlying graph of H is $K_{n,n}$.

29.10 Theorem An $H(2n-1, 2n)$ is a Room square of side $2n-1$. See §VI.50.

29.11 Theorem The existence of an $H(s, 2n)$ is equivalent to the existence of a pair of orthogonal 1-factorizations of the underlying graph of the $H(s, 2n)$ (an $s-$regular graph on $2n$ vertices). See §VII.5.

29.12 Remark As with Room squares, Howell designs are often constructed using starters and adders. The starter-adder construction for Howell designs follows.

29.13 Suppose G is an additive abelian group of order s, and $s+1 \le 2n \le 2s$. A *Howell n-starter* in G is a set

$$S = \{\{s_i, t_i\} : 1 \le i \le s-n\} \cup \{\{s_i\} : s-n+1 \le i \le n\}$$

that satisfies the two properties:

1. $\{s_i : 1 \le i \le n\} \cup \{t_i : 1 \le i \le s-n\} = G$;
2. $(s_i - t_i) \ne \pm(s_j - t_j)$ if $i \ne j$.

29.14 If S is a Howell n-starter, then a set $A = \{\{a_i\} : 1 \le i \le n\}$ is an *adder* for S if the elements in A are distinct, and the set

$$S + A = \{\{s_i + a_i, t_i + a_i\} : 1 \le i \le s-n\} \cup \{\{s_i + a_i\} : s-n+1 \le i \le n\}$$

is again a Howell n-starter.

29.15 Example $S = \{\{5, 6\}, \{2, 0\}, \{1\}, \{3\}, \{4\}\}$ is a Howell 5-starter in the group $G = \mathbb{Z}_7$.
$A = \{4, 5, 0, 1, 2\}$ is an adder for S.

29.16 Theorem If A is an adder for S, then an $H^*(s, 2n)$ exists. (In the case where the group G is cyclic, the resulting Howell design is *cyclic*).

29.17 Construction Let S be a Howell n-starter, and let A be an adder for S. An $H^*(s, 2n)$ is constructed on the symbol set $G \cup \{\infty_1, \infty_2, \ldots, \infty_{2n-s}\}$. The first row of the Howell design H has the pairs $\{s_i, t_i\}$ in cell $H(0, -a_i)$ for $1 \le i \le s-n$ and pairs $\{s_i, \infty_{i-s+n}\}$ in cell $H(0, -a_i)$ for $s-n+1 \le i \le n$. The remainder of the Howell design is filled out by developing the square via the group G; that is, place pairs $\{s_i + x, t_i + x\}$ in cell $H(x, -a_i + x)$ and place pairs $\{s_i + x, \infty_{i-s+n}\}$ in cell $H(x, -a_i + x)$ where all arithmetic is in the group G. This construction is illustrated in Example 29.18.

29.18 Example An $H(7,10)$ constructed from the starter and adder in Example 29.15.

$\infty_1 1$		20	56		$4\infty_3$	$3\infty_2$
$\infty_2 4$	$\infty_1 2$		31	60		$\infty_3 5$
$6\infty_3$	$\infty_2 5$	$\infty_1 3$		42	01	
	$0\infty_3$	$\infty_2 6$	$\infty_1 4$		53	12
23		$\infty_3 1$	$0\infty_2$	$\infty_1 5$		64
05	34		$\infty_3 2$	$1\infty_2$	$\infty_1 6$	
	16	45		$3\infty_3$	$2\infty_2$	$\infty_1 0$

29.19 Construction [1155] There exist cyclic Howell designs $H(n,2n)$ and $H(n+1,2n)$ when $n \geq 3$ is odd. For the $H(n,2n)$, let $S = \{\{0\},\{n-1\},\{n-2\},\ldots,\{3\},\{2\},\{1\}\}$ and $A = \{0, n-1, n-2, \ldots, 3, 2, 1\}$ (arithmetic modulo n). For $H(n+1,2n)$, let $S = \{\{0\},\{n\},\ldots,\{4\},\{2,3\},\{1\}\}$ and $A = \{0, n, n-1, \ldots, \frac{n+1}{2}+3, \frac{n+1}{2}+1, \frac{n+1}{2}, \ldots, 3, 2, 1\}$.

29.20 Theorem [1155] There do *not* exist cyclic Howell designs $H(n,2n)$ and $H(n+1,2n)$ when n is even.

29.21 Table Starters and adders for small (cyclic) Howell designs $H(s,2n)$ where $s+1 < 2n < 2s$ and $s \leq 11$.

$H(4,6)$	$S =$ {3,2} 4 1 $A =$ 1 2 0
$H(5,8)$	No Howell design
$H(6,8)$	No starter-adder [1155]
$H(6,10)$	$S =$ {2,3} {0} {5} {4} {1} $A =$ 2 0 4 3 1
$H(7,10)$	$S =$ {5,6} {2,0} {1} {3} {4} $A =$ 4 5 0 1 2
$H(7,12)$	No starter-adder (Thm. 29.20). For a noncyclic H(7,12), see Example 29.30.
$H(8,10)$	No starter-adder [1155]
$H(8,12)$	$S =$ {3,2} {7,4} {5} {6} {0} {1} $A =$ 3 4 5 6 7 0
$H(8,14)$	$S =$ {2,3} {0} {7} {6} {5} {4} {1} $A =$ 2 0 7 5 4 3 1
$H(9,12)$	$S =$ {5,3} {0,6} {2,7} {8} {4} {1} $A =$ 4 5 6 7 8 0
$H(9,14)$	$S =$ {0,7} {3,8} {1} {6} {5} {4} {2} $A =$ 8 4 0 7 6 5 3
$H(9,16)$	No starter-adder (Thm. 29.20).
$H(10,12)$	$S =$ {4,5} {9,1} {3,6} {8,2} {0} {7} $A=$ 0 1 3 5 8 4
$H(10,14)$	$S =$ {4,5} {9,1} {3,6} {0} {2} {7} {8} $A=$ 0 1 3 7 6 4 5
$H(10,16)$	$S =$ {0,8} {3,9} {1} {7} {6} {5} {4} {2} $A =$ 9 3 0 8 7 5 4 2
$H(10,18)$	$S =$ {2,3} {0} {9} {8} {7} {6} {5} {4} {1} $A =$ 2 0 9 8 6 5 4 3 1
$H(11,14)$	$S =$ {5,8} {3,7} {9,10} {4,6} {0} {2} {1} $A =$ 5 8 9 10 6 7 0
$H(11,16)$	$S =$ {2,6} {5,7} {9,8} {3} {10} {11} {4} {1} $A =$ 4 6 7 5 8 9 10 0
$H(11,18)$	$S =$ {0,9} {3,10} {1} {8} {7} {6} {5} {4} {2} $A =$ 10 4 0 9 8 7 6 5 3
$H(11,20)$	No starter-adder (Thm. 29.20).

29.3 Orthogonal 1-Factorizations

29.22 A d-dimensional Howell design $H_d(s, 2n)$ is a d-dimensional array where every cell is either empty or contains an unordered pair of symbols from an s-set and such that each two-dimensional projection is an $H(s, 2n)$. An $H_3(s, 2n)$ is a *Howell cube*.

29.23 Proposition An $H_d(s, 2n)$ is equivalent to d mutually orthogonal 1-factorizations of the underlying graph (an s regular graph on $2n$ vertices).

29.24 $\nu(s, 2n)$ denotes the maximum value of d such that an $H_d(s, 2n)$ exists.

29.25 Proposition $\nu(s, 2n) \leq s - 1$.

29.26 Conjecture [1823] $\nu(s, 2n) \leq n - 1$.

29.27 Theorem Graphs on $2n$ vertices having at least $n - 1$ orthogonal 1-factorizations include

1. K_{2n}, if $2n - 1 \equiv 3 \pmod 4$ is a prime power, or $2n = 10$ (see §VI.50.8).
2. $K_{n,n}$, if n is a prime power (Theorem III.3.28).
3. K_{2n} minus a 1-factor, if $2n = 2^j + 2$, $j \geq 2$ [1394].

29.28 Table Values for $\nu(s, 2n)$, $2n \leq 10$.

$\nu(2, 4) = \nu(3, 4) = \nu(5, 6) = \nu(5, 8) = 1$.
$\nu(3, 6) = \nu(4, 6) = \nu(6, 8) = \nu(6, 10) = \nu(7, 10) = 2$.
$\nu(4, 8) = \nu(7, 8) = 3$.
$\nu(5, 10) = \nu(8, 10) = \nu(9, 10) = 4$.

29.29 Example [325] A Howell cube $H_3(6, 12)$. The underlying graph G is the icosahedron with antipodal points joined. This is the only known case where $\nu(s, 2s)$ exceeds the maximum number of mutually orthogonal latin squares of order s. (The cube is presented as three orthogonal one factorizations of G).

1,2 3,4 5,6 7,8 9,10 11,12	1,2 4,8 3,6 9,11 7,12 5,10	1,2 5,7 4,9 3,11 6,12 8,10
3,8 4,6 5,7 1,10 9,11 2,12	3,4 5,7 2,8 1,6 9,12 10,11	3,4 1,7 2,5 8,12 9,11 6,10
2,8 3,5 4,9 6,10 1,11 7,12	5,6 4,9 2,3 1,10 7,11 8,12	5,6 3,8 2,9 1,4 7,12 10,11
1,6 2,9 4,7 5,10 3,11 8,12	7,8 5,9 1,4 2,12 6,10 3,11	2,3 4,6 7,8 5,10 1,11 9,12
1,7 2,3 5,9 4,8 6,12 10,11	3,8 2,5 4,7 1,11 9,10 6,12	1,6 3,5 4,8 9,10 7,11 2,12
1,4 2,5 3,6 8,10 7,11 9,12	1,7 4,6 3,5 2,9 8,10 11,12	2,8 4,7 5,9 3,6 1,10 11,12

29.30 Example [1862] A Howell cube $H_3(7, 12)$.

1,2 3,4 8,9 6,11 5,10 7,12	1,2 4,9 3,7 6,8 5,11 10,12	1,2 7,9 5,6 3,10 4,11 8,12
1,3 6,7 2,9 5,11 8,12 4,11	1,3 7,9 2,5 6,11 8,10 4,12	1,3 2,8 4,9 6,10 7,11 5,12
1,4 6,8 2,5 7,11 3,10 9,12	1,4 2,8 6,7 3,9 5,10 11,12	1,4 2,7 3,8 5,9 6,11 10,12
1,5 7,9 2,8 4,6 3,11 10,12	1,5 3,8 2,9 4,11 6,10 7,12	1,5 3,4 6,7 8,10 2,11 9,12
1,6 2,7 3,9 5,12 4,11 8,10	1,6 5,9 3,4 2,10 7,11 8,12	1,6 2,5 3,7 8,9 4,10 11,12
1,7 4,9 3,8 5,6 2,10 11,12	1,7 8,9 4,6 3,10 5,12 2,11	1,7 2,9 6,8 5,10 3,11 4,12
1,8 3,7 5,9 6,10 2,11 4,12	1,8 5,6 2,7 4,10 3,11 9,12	1,8 4,6 3,9 2,10 5,11 7,12

29.4 Enumeration of Small Howell Designs

29.31 $\mathrm{IR}_d(G)$ denotes the number of inequivalent sets of d pairwise orthogonal 1-factorizations of a graph G. $\mathrm{NH}_d(s, 2n)$ denotes the number of nonisomorphic d-dimensional Howell designs $H_d(s, 2n)$.

29.32 Remark $\mathrm{NH}_d(s, 2n) = \sum_G \mathrm{IR}_d(G)$, where the sum is taken over all s-regular graphs G on $2n$ vertices.

29.33 Table $\mathrm{NH}_d(s, 2n)$, $2n \le 10$ [1823, 1862]. Since $\mathrm{NH}_d(2n-1, 2n) = \nu(2n-1)$, these values are given in Table VI.50.51. For $d = 1$, the values can be found in Table VII.5.42

s	3	4	4	4	5	6	5	5	5	6	7	8	8	8
$2n$	6	6	8	8	8	8	10	10	10	10	10	10	10	10
d	2	2	2	3	2	2	2	3	4	2	2	2	3	4
$\mathrm{NH}_d(s, 2n)$	1	1	1	1	0	3	6	1	1	18	901	18220	3	1

29.34 Remark [532] Isomorphism of two Howell designs $H(s, 2n)$ can be decided in time $O(n^{O(\log n)})$.

29.5 Howell Designs with Subdesigns

29.35 Let V be a set of $2n$ symbols and let U be a subset of V of cardinality $2m$. An *incomplete Howell design* $H(s, 2n) - H(t, 2m)$ is an $s \times s$ array H that satisfies the following conditions:

1. Every cell in H is either empty or contains an unordered pair of elements of V.
2. Every unordered pair of elements from V is in at most one cell of the array.
3. There is an empty $t \times t$ subarray G of F.
4. Every element of $V - U$ occurs in precisely one cell of each row and each column of H.
5. Every element of U occurs once in each row and column not meeting G, but not in any row or column meeting G.
6. The pairs of elements in $F - G$ plus the pairs of elements occurring in some $H(t, 2m)$ (defined on the elements of U) are the pairs that occur in an $H(s, 2n)$ defined on the elements of V.

29.36 Remark If an $H(s, 2n) - H(t, 2m)$ exists and an $H(t, 2m)$ exists, then there exists a Howell design $H(s, 2n)$ with a $H(t, 2m)$ subdesign

29.37 Theorem [717] Subdesign existence theorems.

1. There exists an $H(n, n+2) - H(3, 4)$ if and only if $n \equiv 0 \pmod 2$, $n \ge 10$.
2. There exists an $H(n, n+2) - H(5, 6)$ if and only if $n \equiv 0 \pmod 2$, $n \ge 16$.
3. There exists an $H(n, n+2) - H(7, 8)$ if and only if $n \equiv 0 \pmod 2$, $n \ge 22$.
4. There exists an $H(n, n+1) - H(2, 4)$ if and only if $n \equiv 1 \pmod 2$, $n \ge 9$.
5. There exists an $H(n, n+2) - H(2, 4)$ if and only if $n \equiv 0 \pmod 2$, $n \ge 8$.
6. There exists an $H(n, n+1) - H^*(3, 6)$ if and only if $n \equiv 1 \pmod 2$, $n \ge 13$.
7. There exists an $H(n, n+2) - H^*(3, 6)$ if and only if $n \equiv 0 \pmod 2$, $n \ge 12$
8. There exists an $H(n, n+1) - H^*(4, 8)$ if and only if $n \equiv 1 \pmod 2$, $n \ge 17$.
9. There exists an $H(n, n+2) - H^*(4, 8)$ if and only if $n \equiv 0 \pmod 2$, $n \ge 16$

29.6 Application to Duplicate Bridge

29.38 Remark Cyclic Howell designs are used as *Howell movements* in duplicate bridge. The rows of the design represent the rounds, the columns represent the boards, and the diagonals represent the tables. See [977] and §VI.51.10.

29.39 A cyclic Howell design (Howell movement) is *compact* if the n filled cells in any row are adjacent.

29.40 Theorem If there exists a compact cyclic Room square of side $2n-1$, then n is odd.

29.41 Theorem (see [725]) Suppose $0 \leq t \leq 3$ and $n \geq 2t+1$, then there exists a compact cyclic $H(n+t, 2n)$.

29.42 Remark Howell designs $H(n, n+2)$ with an additional property, can be used to construct complete coupling round robin schedules. See Theorem VI.51.76.

See Also

§VI.50	Howell designs are generalizations of Room squares.
§VI.55	Starters are used to construct Howell designs.
§VII.5	A connection with 1-factorizations is given by Theorem 29.11.
§VI.51.10	More on scheduling duplicate bridge tournaments
[725]	A broad survey of Room squares with a chapter on Howell designs. This survey contains most of the information in this chapter.
[90, 1963]	Contain the existence proof of Howell designs.
[1155]	The first paper on Howell designs.
[977]	A book on directing duplicate bridge tournaments. Contains a chapter on Howell movements and many schedules of play.

References Cited: [90, 325, 532, 717, 725, 977, 1155, 1394, 1823, 1862, 1963]

30 Infinite Designs

Peter J. Cameron
Bridget S. Webb

30.1 Cardinal Arithmetic

30.1 Remark In order to motivate the "right" generalization of t-designs to infinite sets, one must say a bit about the arithmetic of infinite cardinal numbers. Zermelo–Fraenkel set theory with the Axiom of Choice (ZFC) is adopted, and the definition and basic properties of ordinal numbers are assumed to be known.

30.2 Definition A *cardinal number* is an ordinal number that is not bijective with any smaller ordinal number. The *cardinality* of a set X is the unique cardinal number that is bijective with X.

30.3 Examples The natural numbers $0, 1, 2, \ldots$ are cardinal numbers; the smallest infinite cardinal number is $\aleph_0$, the cardinality of the set of all natural numbers.

30.4 Theorem Let α, β be cardinals with α infinite, then $\alpha + \beta = \alpha \cdot \beta = \max\{\alpha, \beta\}$. If also $2 \leq \beta \leq 2^\alpha$. Then $\beta^\alpha = 2^\alpha > \alpha$.

30.2 The Definition of a t-Design

30.5 Remark The usual definition of a t-design requires some strengthening when extending to infinite sets if one wishes to retain the property that (for example) the complement of a t-design is a t-design. The authors [426] proposed the following definition and gave examples to show that relaxing these conditions admits structures that should probably not be called t-designs.

30.6 Let t be a positive integer, v an infinite cardinal, k and $\overline{k}$ cardinals with $k + \overline{k} = v$, and Λ a $(t+1) \times (t+1)$ matrix with rows and columns indexed by $\{0, \ldots, t\}$ with (i, j) entry a cardinal number if $i+j \leq t$ and blank otherwise. Then a *simple infinite* t-$(v, (k, \overline{k}), \Lambda)$ *design* consists of a set V of points and a set $\mathcal{B}$ of subsets of V, having the properties

- $|B| = k$ and $|V \setminus B| = \overline{k}$ for all $B \in \mathcal{B}$.
- For $0 \leq i + j \leq t$, let $x_1, \ldots, x_i, y_1, \ldots, y_j$ be distinct points of V. Then the number of elements of $\mathcal{B}$ containing all of $x_1, \ldots, x_i$ and none of $y_1, \ldots, y_j$ is precisely Λ_{ij}.
- No block contains another block.

30.7 Remark Sometimes, where there is no confusion, the design is more briefly written as a t-(v, k, λ) design, where $\lambda = \Lambda_{t,0}$, as in the finite case.

30.8 Remark In a nonsimple infinite design, repeated blocks are allowed, but the last condition should be replaced by

- No block strictly contains another block.

30.3 Examples and Results

30.9 Example A 2-$(\aleph_0, \aleph_0, \Lambda)$ design: the points are the vertices of the random graph (Rado's graph), and the blocks are the maximal cliques and co-cliques. Here, $\lambda_{i,j} = 2^{\aleph_0}$ for all $i + j \leq 2$, so $b = r = \lambda > v = k$, where $b = \lambda_{0,0} = |\mathcal{B}|$, and $r = \lambda_{1,0}$.

30.10 For t finite, v an infinite cardinal, and k an arbitrary cardinal, an $S(t, k, v)$ *infinite Steiner system* consists of a set V of v points and a family $\mathcal{B}$ of k-subsets of V (*blocks*), such that any t points lie in exactly one block and (if $v = k$) no block contains every point.

30.11 Theorem An infinite Steiner system is an infinite t-design according to the earlier definition. Moreover, Steiner systems exist for all t, k, v with $t < k < v$ and t finite and v infinite. If k is also finite, then a large set of Steiner systems exists; this is a partition of the set of all k-subsets into Steiner systems.

30.12 Theorem *(Infinite analogue of Fisher's inequality)* Let $\mathcal{D}$ be an infinite t-$(v, (k, \overline{k}), \Lambda)$ design with t finite. Then $b = v$, unless λ is infinite and either

- $\lambda < v$ and $k > r$ (infinite), in which case, $b \leq v$, or
- $\lambda > v$, in which case k is infinite and $b > v$.

30.13 Remark There is no "characterization of equality" as in the finite case. Indeed, Theorem 30.14 holds.

30.14 Theorem Let s, t, λ, μ be positive integers satisfying $t \leq \mu$ if and only if $s \leq \lambda$. Then there exists a countable design with the properties:

(a) every t points lie in exactly λ blocks; and
(b) every s blocks intersect in exactly μ points.

30.15 Example In the case $s = t = 2$, $\lambda = \mu = 1$, one obtains the *free projective planes*.

30.16 Remark Some remarkable highly symmetric projective planes are constructed using stability theory [1369, 2101]. Space does not permit the discussion of these interesting infinite designs, nor their connections with logic, except for the following consequence.

30.17 Remark There is no infinite analogue of Block's lemma (Theorem VI.5.3). In fact, this result does not even hold for infinite Steiner systems.

30.18 Theorem [802] Let v be an infinite cardinal and s a positive integer. Suppose that $t \geq 2$, $s \leq k/t$ and $k > t$, then there exists an infinite $S(t, k, v)$ with a block-transitive automorphism group that acts with s point-orbits.

See Also

[426]	A comprehensive introduction to infinite designs including examples of designs and structures that are not designs; contains much of the information given in this chapter.
[2101]	A survey discussing Hrushovski's amalgamation method and its use in constructing an ω-categorical pseudoplane.

References Cited: [426, 802, 1369, 2101]

31 Linear Spaces: Geometric Aspects

Lynn Margaret Batten

31.1 Finite Linear Spaces

31.1 A PBD on v points is also a *linear space* of order v if all blocks have size at least 2. If all blocks have size at least 3, then such a linear space is *proper*. It is *nontrivial* if it contains more than one block.

31.2 Remark This chapter deals with the geometric aspects of linear spaces. Linear spaces are also pairwise balanced designs; see §IV.6 for this perspective on linear spaces. See also §VII.2.

31.3 Remark It is customary to refer to elements as *points* and to blocks as *lines* when dealing with linear spaces, and theorems are often stated in this geometric language. In geometric terms, a linear space is a pair $(\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is a set of *points* and $\mathcal{B}$ is a collection of subsets of $\mathcal{P}$ (the *lines*) satisfying:

1. every pair of points is contained on exactly one line, and
2. every line contains at least two points.

31.4 Let L be a finite linear space. The *degree of a line* is the number of points on it, and the *degree of a point* is the number of lines that pass through it.

31.5 A finite linear space with $n \geq 3$ points is a *near-pencil* if it contains one line consisting of $n - 1$ points and the remaining lines contain two points.

31.6 Example The lines of a near-pencil on the 5 points {1, 2, 3, 4, 5} are {1, 2, 3, 4}, {1, 5}, {2, 5}, {3, 5}, {4, 5}.

31.7 Theorem (de Bruijn and Erdős, [1597]) Let L be a nontrivial finite linear space. Let v denote the number of points in L, and b denote the number of lines. Then $b \geq v$, with equality if and only if L is a finite projective plane, or L is a near-pencil.

31.8 Remark The inequality of Theorem 31.7 holds for all PBDs with more than one block since adjoining additional blocks of sizes 0 or 1 only strengthens the inequality.

31.9 A finite linear space is *nondegenerate* if it is nontrivial and is not a near-pencil.

31.10 For any integer $v \geq 2$, there is a unique integer n satisfying $n^2-n+2 \leq v \leq n^2+n+1$. Throughout this chapter, the letter n denotes this unique integer.

31.11 Theorem [1597] Let L be a nondegenerate linear space having v points and b lines. Then $b \geq B(v)$ where

$$B(v) = \begin{cases} n^2+n+1 & \text{if} \quad n^2+2 \leq v \leq n^2+n+1 \\ n^2+n & \text{if} \quad n^2-n+3 \leq v \leq n^2+1 \quad \text{or} \quad v = 4 \\ n^2+n-1 & \text{if} \quad v = n^2-n+2 \neq 4. \end{cases}$$

This is best possible in as much as the bounds are attained infinitely often.

31.12 Let L be a finite linear space. Then L is *embeddable* in a projective plane if there exists a projective plane π with the property that L can be obtained by deleting points (and any resulting lines of length 0 and 1) from π.

31.13 Remark If a linear space is embeddable in a projective plane, this yields a method of generating the linear space when n is a prime power and may be an indicator of the difficulty of constructing the linear space otherwise.

31.14 Remark To discuss the embeddability of finite linear spaces whose numbers of points and lines meet the bound in Theorem 31.11, Example 31.15 is required.

31.15 Example A special finite linear space $E_1 : v = 8$, $b = 11$. $\mathcal{P} = \{1,2,3,4,5,6,7,8\}$, $\mathcal{B} = \{\{1,2,3,8\},\{1,4,5\},\{2,4,6\},\{3,4,7\},\{1,6,7\},\{2,5,7\},\{3,5,6\},\{4,8\},\{5,8\},\{6,8\},\{7,8\}\}$.

31.16 Remark The configuration of Example 31.15 is not embeddable in a projective plane of order 3.

31.17 Theorem [1597] Let L be a nondegenerate finite linear space with v points and b lines. If $b = B(v)$, then either L can be embedded in a projective plane of order n or $v = 8$, $b = 11$, and L is the special linear space E_1 given in Example 31.15.

31.18 Remark The case of finite linear spaces L with v points and b lines where $n^2-n+2 \leq v \leq B(v)+1$ is also of interest. Such spaces have been classified [1597], but infinitely many cannot be embedded in a finite projective plane of order n. However if such a linear space contains a point of degree at most n, then, apart from a finite number of exceptions, it can be embedded in a projective plane of order n. For this and other results an expanded set of special linear spaces is required.

31.19 Example More special finite linear spaces. Lines appear as columns.

$E_2 : v = 8, b = 12$	$E_3 : v = 8, b = 13$	$E_4 : v = 8, b = 13$
131122445566	1135122234454	1112342233446
277878787878	2676867866778	2575566768577
38	3788	368878
4	4	4
5	5	
6		
$E_5 : v = 6, b = 8$	$E_6 : v = 7, b = 10$	$E_7 : v = 7, b = 10$
12113344	1311224455	1143122234
25565656	2667676767	2556656757
36	37	3767
4	4	4
	5	

31.20 Theorem Let L be a nondegenerate linear space with at least n^2-n+2 points and at most n^2+n+1 lines for some integer $n \geq 2$. If L has a point of degree at most n, then one of the following cases occurs.

1. L can be embedded into a projective plane of order n.
2. L is one of the linear spaces E_1, E_2, E_3, or E_4; in particular, $n = 3$ and $v = n^2 - n + 2 = 8$.
3. $v = n^2 - n + 2$ and $b = n^2 + n + 1$, L has a point p of degree n that lies on one line l of degree $n+1$ and on $n-1$ lines of degree n. The n points different from p on l do not all have degree $n + 1$.

31.21 Corollary In a nondegenerate linear space with n^2+n+1 lines and at least n^2-n+3 points, every point has degree at least $n + 1$.

31.22 Theorem [1597] If L is a nondegenerate linear space with $v = n^2 - n + 2$ points and $b = B(v) + 1 = n^2 + n$ lines for some integer $n \geq 2$, then either L can be embedded in a projective plane of order n or $v = 8$, $b = 12$, and L is the linear space E_2.

31.23 Remark Totten studied *restricted* linear spaces, those that satisfy $(b - v)^2 \leq v$, where v and b are the number of points and lines of the space, respectively. Such linear spaces bound the difference between the numbers of points and lines. Theorem 31.24 yields useful information about restricted linear spaces.

31.24 Theorem [1597] Let L be a nondegenerate linear space with v points and b lines.

1. If $(b - v)^2 \leq v$, then $b \leq v + n$.
2. If $v < (b - v)^2 \leq b$, then $v = 8$ and $b = 11$, or $v \in \{n^2 + n, n^2 + n + 1\}$ and $b = v + n + 1$.
3. If $(b - v)^2 \leq b$ and if L has maximal line degree $k \geq n + 2$, then L is one of the linear spaces E_5, E_6 or E_7.

31.25 A *punctured* affine plane is an affine plane with one of its points deleted.

31.26 Theorem (Totten, see [1597]) Every nondegenerate restricted, finite linear space is one of the following structures.

1. A projective plane with at most n points deleted but not more than $n - 1$ being deleted from the same line.
2. An affine plane π of order n, or an affine plane π of order n with a new point, say ∞, that has been adjoined to all lines of one of the parallel classes of π.
3. An affine plane π of order n from which a point has been deleted, and to which a new point, say ∞, has been adjoined to all lines that are the remnants of one of the orginal parallel classes of π.
4. The configuration obtained from a projective plane π of order n by deleting s points from a line ℓ, and replacing the remaining $n - s + 1$ points of ℓ by either a projective plane of order $n - s$ or a near-pencil on $n - s + 1$ points.
5. The linear space $E_5(v = 6, b = 8)$.

31.27 Remark Napolitano [1667] extended Totten's classification to the case $b - v = \sqrt{v} + 1$. He shows that, apart from a few cases with small numbers of points and lines, such spaces can be obtained from a projective plane either by replacing one of its lines by a new configuration, or by removing a suitable set of points.

31.28 Remarks

1. Theorems 31.20, 31.22, 31.24, and 31.26 are useful in ruling out the existence of certain linear spaces as well as yielding information about the types of linear spaces obtained by deleting relatively few points from a projective plane.
2. Good general references for properties of finite linear spaces are [164, 962, 1597].

31.2 Semiaffine Linear Spaces

31.29 If (p, l) is a nonincident, point-line pair of a linear space, $\pi(p, l)$ is the number of lines through p that miss l.

31.30 Remark A nondegenerate linear space is a projective plane if and only if $\pi(p, l) = 0$. A nondegenerate linear space is an affine plane if and only if $\pi(p, l) = 1$.

31.31 Let I be a set of nonnegative integers. A linear space is *I-semiaffine* if $\pi(p, l) \in I$ for every nonincident point-line pair (p, l).

31.32 Theorem [164] A finite $\{0, 1\}$-semiaffine linear space is a near-pencil, a projective or affine plane, a projective plane with one point deleted, or an affine plane with one point added to all lines of a parallel class.

31.33 If $n + 1$ is the maximum number of lines on any point in a finite linear space, then n is the *order* of the space.

31.34 Theorem [164] A finite $\{1, 2\}$-semiaffine linear space of order n is an affine plane of order n with no, one, or all points of a line removed or is a linear space on 5 points with a single line on 3 points, K_5, K_6, a linear space on 12 points with 19 lines, constant point size 5, each point on four lines with 3 points and one line with 4 points, or a 2-(46, 6, 1) design.

31.35 Theorem [164] A finite $\{0, 1, 2\}$-semiaffine linear space of order $n \leq 6$ that is neither $\{0, 1\}$- nor $\{1, 2\}$-semiaffine is embeddable in a projective plane of order n as the complement of a set of points.

31.36 Theorem [164] A finite $\{0, 1, s\}$-semiaffine linear space of order n that is not $\{0, 1\}$-, $\{0, s\}$-, or $\{1, s\}$-semiaffine is the complement of a set of points in a projective plane of order n such that each line of the plane meets the set in 0, 1 or s points.

31.37 Theorem [831] For $1 \leq s < t$, an $\{s, t\}$-semiaffine linear space of order n with non-constant point degree is a near-pencil on $t + 3$ points with one line of length $t - s + 2$.

31.38 Remark The constant point degree case of Theorem 31.37 remains open.

31.3 Group Action on Linear Spaces

31.39 The *automorphism group* of a linear space $(\mathcal{P}, \mathcal{B})$ is the set of all permutations of the point set and of the line set that preserve point-line incidence. This group is denoted by $Aut(\mathcal{P}, \mathcal{B})$.

31.40 The *point orbits* of $(\mathcal{P}, \mathcal{B})$ under G, G a subgroup of $Aut(\mathcal{P}, \mathcal{B})$ are the equivalence classes of $\mathcal{P}$ under the relation R defined by $\mathcal{P}R\mathcal{Q}$ if and only if there exists $g \in G$ such that $g(\mathcal{P}) = \mathcal{Q}$. The *line orbits* are similarly defined.

31.41 Let (a, b) be an ordered pair of elements, $a, b \in \mathcal{P} \cup \mathcal{B}$. Let X be any subset of the set of all such ordered pairs. The *orbits* of X are the equivalence classes of X under the relation R defined by $(a, b)R(a', b')$ if and only if there exists $g \in G$ such that $g(a) = a'$ and $g(b) = b'$.

31.42 Remark The ideas here can be extended in a natural way to ordered and unordered R-tuples.

31.43 If $p \in l$, the pair (p, l) is a *flag*; if $p \notin l$, (p, l) is an *antiflag*.

31.44 $G \subseteq Aut(\mathcal{P}, \mathcal{B})$ is point, line, flag, or antiflag transitive if there is a single point, line, flag, or antiflag orbit, respectively, under the relation R. If $G = Aut(\mathcal{P}, \mathcal{B})$, then $(\mathcal{P}, \mathcal{B})$ is *transitive*.

31.45 Let v_G and b_G denote the number of point and block orbits, respectively, of a linear space under a group G.

31.46 Theorem [164] Let $(\mathcal{P}, \mathcal{B})$ be a nontrivial finite linear space and G a subgroup of $Aut(\mathcal{P}, \mathcal{B})$. Then $v_G \leq b_G$.

31.47 Corollary Let $(\mathcal{P}, \mathcal{B})$ be a nontrivial finite linear space in which $v = b$. Let G be a subgroup of $Aut(\mathcal{P}, \mathcal{B})$. Then $v_G = b_G$.

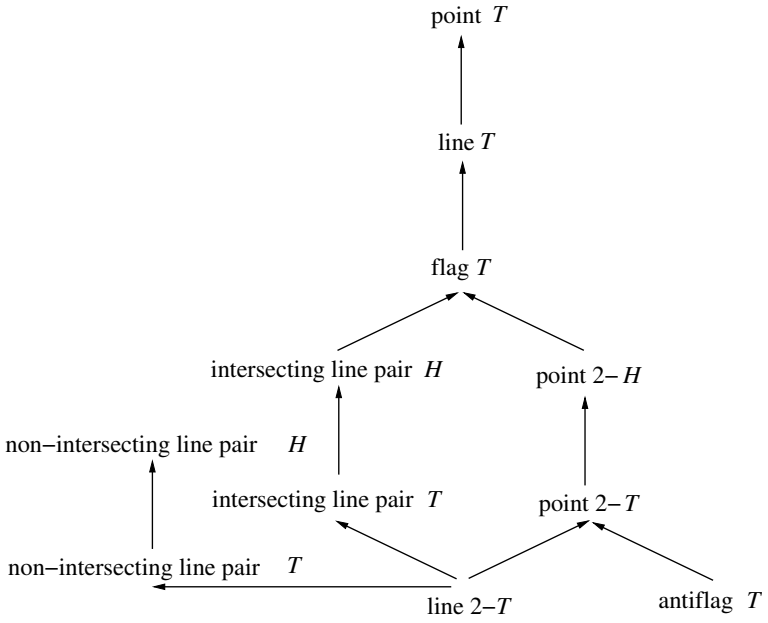
31.48 Theorem [164] For all integer pairs (v_G, b_G) with $v_G \leq b_G$, there is a finite linear space with v_G point orbits and b_G line orbits.

31.49 Remark The proof of Theorem 31.48 is constructive; an example is obtained for each v_G and b_G.

31.50 Remark Because the focus is on the point and line structure of a linear space when considering the automorphism group, the only transitivities of interest are those between points, lines, point pairs, line pairs, and point and line pairs.

31.51 When considering a set X of unordered pairs of points and lines, G is *homogeneous* on X if there is a single orbit on X under G.

31.52 Example [164] The diagram represents the implications between transitivities and homogeneities of points, lines, and pairs. The letters T and H stand for transitive and homogeneous, respectively.



31.53 Remark Much work has been done on the classification of finite linear spaces with certain transitivity properties. Refer to [371] for a nearly complete classification of flag-transitive linear spaces and [671] for a classification of a special category of line-transitive linear spaces. See also §VI.5.

31.4 Dimension and Linear Spaces

31.54 If it is possible to choose a *subset* of the set of subspaces (a set of points that contains the entire line on any two points in it) of a finite linear space, S, including all the points and lines, and such that the intersection of any two elements of the subset is again in the subset, and in addition assign to each element of this subset a unique integer between 0 and d for some fixed integer $d \geq 2$ so that

(i) each point is assigned 0 and each line is assigned 1;
(ii) if V is assigned i, for any point p not in V, there is a unique subspace W on V and p that is assigned $i+1$; and
(iii) S is assigned d,

then S is a *d-dimensional linear space*.

31.55 In what follows, *plane* always denotes a 2-subspace of a linear space S.

31.56 If each plane is isomorphic to a single plane $\prod$, then the space is a $\prod$-space.

31.57 Remark The first result follows immediately from the definitions. Suppose that the set of planes of S is precisely the set of subspaces generated (using linear closure) by three noncollinear points. Then *S is a projective space precisely when each of its planes is projective*; moreover, if S has dimension at least 3, then all of its planes are desarguesian and of the same order.

31.58 Theorems [164]

1. Let S be a nontrivial linear space such that each plane is affine and such that each line has at least four points. Then S is an affine space.
2. If every plane of a linear space S is projective or affine, then all planes are projective or all planes are affine.
3. Let S be a 3-dimensional finite linear space in which every plane is isomorphic to the linear space π_0, and in which the residue at every point is isomorphic to π_0. Then S is a (possibly degenerate) projective space $PG(3,n)$ or a linear space consisting of two disjoint lines of the same size, all other lines are size 2.
4. Let π be a linear space with at least two lines of different sizes. Then there exists only a finite number of finite dimensional linear spaces in which each plane is isomorphic to π.

31.59 Remark d-dimensional linear spaces of dimension $d \geq 3$ that are line-plane flag-transitive have been classified by Delandtsheer [164].

31.60 For each point p of any linear space S, let S_p denote the structure of all subspaces of S that contain p. Any linear space S in which S_p is a projective space at each point p is a *locally projective space*.

31.61 Remark The following is straightforward to prove: Let S be a linear space in which for each point p, the structure S_p is that of a projective space. Then S is a dimensional linear space; moreover, S_p is isomorphic to S_q, for each q, which implies in particular that the orders of the projective spaces at each point are the same.

31.62 Theorem A finite locally projective space of dimension greater than 3 in which all lines have n points is either a projective space or an affine space.

31.63 Theorem A finite locally projective space of dimension 3 in which all lines have n points is a projective space, an affine space or a space in which each plane is I-semiaffine, where $I = \{n^2 - n + s\}$ or $I = \{n^3 + s\}$.

See Also

§IV.1	Linear spaces are pairwise balanced designs.
§VII.2	Further information on finite geometries.
[164, 962, 1597]	Good general references for properties of finite linear spaces.
[668]	Various additional results on dimensional linear spaces.

References Cited: [164,371,668,671,831,962,1597,1667]

32 Lotto Designs

(Ben) P. C. Li
G. H. John van Rees

32.1 Definitions, Examples and Remarks

32.1 An (n,k,p,t)-*lotto design* is an n-set, V, of elements and a set $\mathcal{B}$ of k-element subsets (blocks) of V, so that for any p-subset P of V, there is a block $B \in \mathcal{B}$, for which $|P \cap B| \geq t$. $L(n,k,p,t)$ denotes the smallest number of blocks in any (n,k,p,t)-lotto design.

32.2 **Remark** There are many lotteries in the world run by governments and casinos. Generally, for a small fee, a person chooses k numbers from n numbers or has the numbers chosen randomly. This is the ticket. At a certain point, no more tickets are sold and the government or casino picks p numbers from the n numbers, in some random fashion. These are the *winning numbers*. If any of the sold tickets match t or more of the winning numbers, then a prize is given to the holder of the winning ticket. The larger the value of t (usually $t \geq 3$), the larger the prize. Many gamblers and researchers are interested in knowing what is the minimum number of tickets necessary to ensure a match of at least t numbers. The minimum is $L(n,k,p,t)$. Buying $L(n,k,p,t)$ tickets guarantees a minimum return but does not in any way change the expected return.

32.3 **Remark** Of course, $L(n,k,p,1) = \lceil \frac{n-p+1}{k} \rceil$ and $L(n,k,k,k) = \binom{n}{k}$. A few other lottery numbers are known. The Hungarian Lottery is a (90,5,5,t)-lotto design and $L(90,5,5,2) = 100$. Lotteries with parameters (49,6,6,t) are popular with governments all over the world and it is known that $L(49,6,6,2) = 19$. But many of these numbers are very difficult to obtain. For example, $L(49,6,6,3)$ is not known, although it is known that $87 \leq L(49,6,6,3) \leq 163$. The upper bound is obtained by adjoining the 77 blocks of the Steiner system, S(3,6,22), to the 86 blocks of a (27,6,4,3)-lotto design that was found using simulated annealing. The lower bound is obtained by counting.

32.4 **Example** The following three blocks form a (7,5,4,3)-lotto design with the fewest blocks: {1,2,3,4,7}, {1,2,5,6,7}, {3,4,5,6,7}.

32.5 **Example** The following six blocks form a (20,10,6,4)-lotto design with the fewest blocks: {1,3,5,6,7,10,11,12,13,14}, {2,4,5,6,7,8,9,10,12,15},
{1,2,3,4,8,9,11,13,14,15}, {3,5,6,10,12,16,17,18,19,20},
{1,7,9,11,14,16,17,18,19,20}, {2,4,8,13,15,16,17,18,19,20}.

32.6 **Theorem** If the blocks of a lotto design are complemented, a lotto design results so $L(n,k,p,t) = L(n,n-k,n-p,n-k-p+t)$.

32.2 Connections between Lotto Designs and Other Designs

32.7 A t-(v,k,m,λ) *general cover* is a v-set V of elements and a set $\mathcal{B}$ of k-element subsets of V (blocks), so that for any m-subset M of V, there are at least λ blocks B of $\mathcal{B}$ for which $|M \cap B| \geq t$. $C_\lambda(v,k,m,t)$ is the smallest number of blocks in a t-(v,k,m,λ) general cover. (See §VI.11.)

32.8 Proposition An (n,k,p,t)-lotto design is a t-$(n,k,p,1)$ general cover, so $L(n,k,p,t) = C_1(n,k,p,t)$.

32.9 An (n,k,t) *covering design* or *cover* is an n-set X of elements and a set $\mathcal{B}$ of k-element subsets of X (blocks), so that every t-subset of X occurs in a block of $\mathcal{B}$. $C(n,k,t)$ is the smallest number of blocks in a (n,k,t) covering design.

32.10 Proposition Since an (n,k,t,t)-lotto design is an (n,k,t) covering design, $L(n,k,t,t) = C(n,k,t)$.

32.11 An (n,p,t) *Turán system* is an n-set X of elements and a set $\mathcal{B}$ of t-element subsets of X (blocks), so that every p-subset of X contains a block of $\mathcal{B}$. $T(n,p,t)$ is the smallest number of blocks in an (n,p,t) Turán system. (See §VI. 61.)

32.12 Proposition An (n,t,p,t)-lotto design is an (n,p,t) Turán system, so $L(n,t,p,t) = T(n,p,t)$.

32.13 Remark If the blocks of a covering design are complemented, then one gets a Turán system, so $C(n,k,t) = T(n,n-t,n-k)$. This is a just special case of Theorem 32.6.

32.14 Let $\mathcal{V}$ be a nonempty set of binary vectors (codewords), each of length n and each having weight k (k 1s and $n-k$ 0s). $\mathcal{V}$ is an (n,k,p,d)-*constant weight covering code* if every binary vector of weight p and length n has Hamming distance at most d from at least one codeword. $K(n,k,p,d)$ is the smallest number of codewords in an (n,k,p,d)-constant weight covering code.

32.15 Proposition Assuming $d \equiv k+p \pmod 2$, then $K(n,k,p,d) = L(n,k,p,(k+p-d)/2)$.

32.3 Theorems on Lotto Designs

32.16 Theorem
$$\frac{\binom{n}{t}}{\binom{p-1}{t-1}\binom{k}{t}} \cdot \frac{n-p+1}{n-t+1} \leq L(n,k,p,t) \leq \left\lceil \frac{\min(\binom{n}{p},\binom{n}{t})}{\lfloor \frac{k}{t} \rfloor} \right\rceil.$$

32.17 Lemma (volume bound)
$$L(n,k,p,t) \geq \frac{\binom{n}{p}}{\sum_{i=t}^{\min(k,p)} \binom{k}{i}\binom{n-k}{p-i}}.$$

32.18 Theorem $L(n,k,p,t)$ is a nondecreasing function under any one of the following conditions: if n increases, k decreases, p decreases, or t increases. $L(n,k,p,t)$ is a nondecreasing function under any one of the following conditions: if n and k both decrease, n and p both decrease, k and t both increase, or p and t both increase. $L(n,k,p,t)$ is a nondecreasing function if n,k,p,t all increase.

32.19 Theorem [397] For all $1 \leq t \leq \{k,p\} \leq n$

(a) $L(n,k,p,t) = 1$ if and only if $k+p \geq n+t$.

(b) $L(n,k,p,t) = 2$ if and only if $2t-1+\max\{n-2k,0\} \leq p \leq n+t-k-1$.

(c) $L(n,k,p,t) = 3$ if and only if $p \leq \min\{2t-2+\max\{n-2k,0\}, n-k+t-1\}$ and
$$p \geq \begin{cases} 3t-2+\max\{n-3k,0\}, & \text{if } n \geq 2k, \\ \frac{3}{2}t-1+\max\{n-\frac{3}{2}k,0\}, & \text{if } n < 2k. \end{cases}$$

32.20 Remark For $t = 1$, $L(n,k,p,t)$ has been completely determined. For $t = 2$, the determination of $L(n,k,p,t)$ is closely related to finding the largest independent set in a multigraph. Using this, many families of infinite cardinality have been determined for $t = 2$, and the bounds on $L(n,k,p,2)$ are quite good. For $t \geq 3$, the situation is much more open. Independent sets in graphs are also useful for general t.

32.21 Theorem [1046] $L(n,k,p,2) \geq \frac{n(n-p+1)}{k(k-1)(p-1)}$ with equality if a Steiner system $S(2,k,v)$ exists with $n = v(p-1)$, where v is an integer (see §II.5).

32.22 Theorem [350]
$$\begin{aligned} L(2m+1,3,3,2) &= C(m,3,2) + C(m+1,3,2), \\ L(4m+2,3,3,2) &= C(2m+1,3,2) + C(2m+1,3,2), \text{ and} \\ L(4m,3,3,2) &= C(2m-1,3,2) + C(2m+1,3,2). \end{aligned}$$

32.23 Theorem [846]
$$\min_{\sum_{i=1}^{p-1}\alpha_i = n} \sum_{i=1}^{p-1} \alpha_i \left\lceil \frac{\alpha_i - 1}{k-1} \right\rceil \leq L(n,k,p,2) \leq \min_{\sum_{i=1}^{p-1}\alpha_i = n} \sum_{i=1}^{p-1} C(\alpha_i, k, 2)$$

32.24 Theorem [163] For $6 \leq n \leq 30$, $L(n,6,6,2) = \lceil \frac{n-1}{2} \rceil$.

n	31–33	34	35–36	37	38–39	40	41–42	43	44–45	46	47	48	49–50	51	52	53	54
$L(n,6,6,2)$	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

32.25 Theorem [1445](Generalized Schönheim bound) For $n \geq 2k-t+1$ and $n \geq k-t+p+1$,
$$L(n,k,p,t) \geq \left\lceil \frac{\binom{n}{k-t+1} L(n-k+t-1,k,p,t)}{\binom{n}{k-t+1} - \binom{k}{k-t+1}} \right\rceil.$$
For $L(n,k,t,t)$ this bound is the usual Schönheim Bound for coverings. (See §VI.11.)

32.26 Proposition [1445] $L(n,k,t+1,t) \geq \min\{L(n,k,t-1,t-1), L(n-t+1,k-t+2,2,2)\}$. There are many similar lower bounds.

32.27 Proposition If $k_1 > k_2$, then $L(n,k_1,p,t) \geq \frac{L(n,k_2,p,t)}{L(k_1,k_2,t,t)}$.

32.28 Proposition [1445] If $n - k \geq p - t + 1$ and $\lceil \frac{r}{r+1} n \rceil \leq k$ where $r = \left\lfloor \frac{p}{p-t+1} \right\rfloor$, then $L(n,k,p,t) = r + 1$.

32.29 Proposition [1445] If $k \geq 3$, then $L(2k+1,k,5,3) = 5$. If $k \geq 3$, then $L(3k+2,k,8,3) = 5$. If $k \geq 4$, then $L(2k+2,k,8,4) = 4$.

32.30 Proposition [1445] If there exists an element of frequency 0 in an (n,k,p,t) lotto design with $y > 1$ blocks, then there exists an $(n-1,k,p-1,t)$-lotto design on y blocks where $n \geq k+1$.

32.31 Proposition [1445] If there exists an element of frequency 1 in an (n,k,p,t)-lotto design with $y > 1$ blocks, then there exists an $(n-k+t-2,k,p-1,t)$-lotto design with y-1 blocks where $n > 2k-t+1$ and $t > 1$.

32.4 Constructions, Algorithms and Tables

32.32 Proposition If $n = n_1 + n_2$ and $p = p_1 + p_2 - 1$, then $L(n,k,p,t) \leq L(n_1,k,p_1,t) + L(n_2,k,p_2,t)$.

32.33 Proposition $L(n+1,k+1,p+1,t+1) \leq L(n,k,p,t) + L(n,k+1,p+1,t+1)$.

32.34 Proposition [1445] (Semi-direct Product) Suppose n,k,p,t,n_1,k_1 and r are integers such that $n_1 < n$, $p - r \geq t$, $k_1 \geq t - r - 1$, and $k_1 = k - n + n_1$. Then $L(n,k,p,t) \leq L(n_1,k,p-r,t) + L(n_1,k_1,p-r-1,t-r-1)$.

32.35 Construction [223] Let $n = a+b+c$ where $a \geq 3, c \geq 3, a+b \geq 6, b+c \geq 6$, and $m = 5$ or 6. Then $L(n, 6, m, 4) \leq L(a+b, 6, m-1, 4)+L(b+c, 6, m-1, 4)+L(a, 3, 2, 2)L(c, 3, 2, 2)$.

32.36 Remarks Another way to improve the bounds is to use computational search. The lower bounds can be improved by running backtrack algorithms. Unfortunately, they are very slow and useful only if the number of blocks is very small. The upper bounds can often be improved by heuristic algorithms. The most successful heuristic algorithm used is simulated annealing, although tabu search, integer linear programming, greedy algorithms, and other algorithms have found some upper bounds. See §VII.6 for descriptions of these algorithms.

32.37 Table $L(n, k, p, t)$ for $t = 2, 3, 4$; $p = t+1, \ldots, 11$; $k = t+1, \ldots, 14$, and $n = p+1, \ldots, 20$. If the value is unknown, upper and lower bounds are given. Since Theorem 32.19 determines when the number of blocks is 1, 2, or 3, any row with just these numbers is omitted. Also $L(n, k, t, t)$ entries are omitted as they are recorded in the tables on coverings (see §VI.11). For more tables on lotto designs, see `http://dip.sun.ac.za/~vuuren/repositories/lottery/repository.php`, `http://www.cs.umanitoba.ca/~lipakc/lottotables.html`, or `http://www.xs4all.nl/~rbelic`.

$p = 3$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
7	4	2	2	1	1							
8	5	2	2	2	1	1						
9	7	4	2	2	2	1	1					
10	8	4	2	2	2	2	1	1				
11	10	6	4	2	2	2	2	1	1			
12	11	6	4	2	2	2	2	2	1	1		
13	13	8	5	4	2	2	2	2	2	1	1	
14	14	9	6	4	2	2	2	2	2	2	1	1
15	18	11	7	4	4	2	2	2	2	2	2	1
16	19	12	8	5	4	2	2	2	2	2	2	2
17	23	14	9	6	4	4	2	2	2	2	2	2
18	24	15	10	6	5	4	2	2	2	2	2	2
19	29	16	11	7	6	4	4	2	2	2	2	2
20	31	18	12	8	6	4	4	2	2	2	2	2

$p = 4$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
10	5	3	2	2	2	1	1	1				
11	6	3	2	2	2	2	1	1	1			
12	8	3	3	2	2	2	2	1	1	1		
13	9	5	3	2	2	2	2	2	1	1	1	
14	11	5	3	3	2	2	2	2	2	1	1	1
15	12	7	3	3	2	2	2	2	2	2	1	1
16	14	7	5	3	3	2	2	2	2	2	2	1
17	15	9	5	3	3	2	2	2	2	2	2	2
18	17	9	6	3	3	3	2	2	2	2	2	2
19	18	11	7	5	3	3	2	2	2	2	2	2
20	20	12	8	5	3	3	3	2	2	2	2	2

$p = 5$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
11	4	3	2	2	2	1	1	1	1			
12	4	3	2	2	2	2	1	1	1	1		
13	6	3	3	2	2	2	2	1	1	1	1	
14	7	4	3	2	2	2	2	2	1	1	1	1
15	9	4	3	3	2	2	2	2	2	1	1	1
16	10	4	3	3	2	2	2	2	2	2	1	1
17	12	6	4	3	3	2	2	2	2	2	2	1
18	13	6	4	3	3	2	2	2	2	2	2	2
19	15	8	4	3	3	3	2	2	2	2	2	2
20	16	8	4	4	3	3	2	2	2	2	2	2

$p = 6$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
12	4	3	2	2	2	1	1	1	1	1		
13	4	3	2	2	2	2	1	1	1	1	1	
14	5	3	3	2	2	2	2	1	1	1	1	1
15	5	4	3	2	2	2	2	2	1	1	1	1
16	7	4	3	3	2	2	2	2	2	1	1	1
17	8	4	3	3	2	2	2	2	2	2	1	1
18	10	5	4	3	3	2	2	2	2	2	2	1
19	11	5	4	3	3	2	2	2	2	2	2	2
20	13	5	4	3	3	3	2	2	2	2	2	2

$p = 7$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
13	4	3	2	2	2	1	1	1	1	1	1	
14	4	3	2	2	2	2	1	1	1	1	1	1
15	5	3	3	2	2	2	2	1	1	1	1	1
16	5	4	3	2	2	2	2	2	1	1	1	1
17	6	4	3	3	2	2	2	2	2	1	1	1
18	6	4	3	3	2	2	2	2	2	2	1	1
19	8	5	4	3	3	2	2	2	2	2	2	1
20	9	5	4	3	3	2	2	2	2	2	2	2

$p = 8$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
14	4	3	2	2	2	1	1	1	1	1	1	1
15	4	3	2	2	2	2	1	1	1	1	1	1
16	5	3	3	2	2	2	2	1	1	1	1	1
17	5	4	3	2	2	2	2	2	1	1	1	1
18	6	4	3	3	2	2	2	2	2	1	1	1
19	6	4	3	3	2	2	2	2	2	2	1	1
20	7	5	4	3	3	2	2	2	2	2	2	1

$p = 9$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
15	4	3	2	2	2	1	1	1	1	1	1	1
16	4	3	2	2	2	2	1	1	1	1	1	1
17	5	3	3	2	2	2	2	1	1	1	1	1
18	5	4	3	2	2	2	2	2	1	1	1	1
19	6	4	3	3	2	2	2	2	2	1	1	1
20	6	4	3	3	2	2	2	2	2	2	1	1

$p = 10$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
16	4	3	2	2	2	1	1	1	1	1	1	1
17	4	3	2	2	2	2	1	1	1	1	1	1
18	5	3	3	2	2	2	2	1	1	1	1	1
19	5	4	3	2	2	2	2	2	1	1	1	1
20	6	4	3	3	2	2	2	2	2	1	1	1

$p = 11$, $t = 2$

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
17	4	3	2	2	2	1	1	1	1	1	1	1
18	4	3	2	2	2	2	1	1	1	1	1	1
19	5	3	3	2	2	2	2	1	1	1	1	1
20	5	4	3	2	2	2	2	2	1	1	1	1

$p = 4$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
7	4	3	1	1							
8	6	3	3	1	1						
9	9	5	3	3	1	1					
10	12–14	7	4	3	3	1	1				
11	16–19	9	5	3	3	3	1	1			
12	21–26	11–12	6	4	3	3	3	1	1		
13	28–33	11–16	8–9	6	4	3	3	3	1	1	
14	35–42	14–20	8–11	6	5	3	3	3	3	1	1
15	44–52	18–24	10–14	7–9	6	4	3	3	3	3	1
16	54–64	22–32	11–16	7–11	7	5	4	3	3	3	3
17	66–77	27–40	14–20	9–13	7–9	6	4	3	3	3	3
18	79–93	32–48	16–25	10–15	7–9	6	5	4	3	3	3
19	94–110	38–57	19–30	11–18	9–14	7–9	6	5	4	3	3
20	111–128	45–70	23–35	13–20	9–14	7–10	6–8	5	4	3	3

$p = 5$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
9	5	2	2	1	1	1					
10	7	2	2	2	1	1	1				
11	10	5	2	2	2	1	1	1			
12	10–12	6	2	2	2	2	1	1	1		
13	13	8	5	2	2	2	2	1	1	1	
14	17–20	8–10	5	2	2	2	2	2	1	1	1
15	21–26	9–13	7	5	2	2	2	2	2	1	1
16	26–28	11–14	7–8	5	2	2	2	2	2	2	1
17	32–39	13–18	7–11	6–7	5	2	2	2	2	2	2
18	39–44	16–22	8–12	7–8	5	2	2	2	2	2	2
19	46–55	19–26	10–15	7–10	6	5	2	2	2	2	2
20	54–60	22–32	11–18	7–11	6–7	5	2	2	2	2	2

$p = 6$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
10	4	2	2	1	1	1	1				
11	5	2	2	2	1	1	1	1			
12	7	4	2	2	2	1	1	1	1		
13	10	4	2	2	2	2	1	1	1	1	
14	10–12	6	4	2	2	2	2	1	1	1	1
15	13–15	8	4	2	2	2	2	2	1	1	1
16	16–20	8–10	5	4	2	2	2	2	2	1	1
17	19–23	8–12	6	4	2	2	2	2	2	2	1
18	23–28	10–14	7	4	4	2	2	2	2	2	2
19	28–33	11–17	7–9	5	4	2	2	2	2	2	2
20	33–40	13–20	7–10	6–7	4	4	2	2	2	2	2

$p = 7$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
13	6	3	2	2	2	1	1	1	1	1	
14	8	3	2	2	2	2	1	1	1	1	1
15	9–10	3	3	2	2	2	2	1	1	1	1
16	10–12	6	3	2	2	2	2	2	1	1	1
17	12–14	7	3	3	2	2	2	2	2	1	1
18	14–17	7–9	3	3	2	2	2	2	2	2	1
19	17–19	8–11	6	3	3	2	2	2	2	2	2
20	20–25	8–13	6	3	3	2	2	2	2	2	2

$p = 8$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
14	5	3	2	2	2	1	1	1	1	1	1
15	6	3	2	2	2	2	1	1	1	1	1
16	7–8	3	3	2	2	2	2	1	1	1	1
17	9–11	5	3	2	2	2	2	2	1	1	1
18	9–13	5	3	3	2	2	2	2	2	1	1
19	11–16	7	3	3	2	2	2	2	2	2	1
20	13–17	7–9	5	3	3	2	2	2	2	2	2

$p = 9$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
15	4	3	2	2	2	1	1	1	1	1	1
16	4	3	2	2	2	2	1	1	1	1	1
17	7	3	3	2	2	2	2	1	1	1	1
18	7–9	4	3	2	2	2	2	2	1	1	1
19	8–11	4	3	3	2	2	2	2	2	1	1
20	10–13	4	3	3	2	2	2	2	2	2	1

$p = 10$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
16	4	3	2	2	2	1	1	1	1	1	1
17	4	3	2	2	2	2	1	1	1	1	1
18	6	3	3	2	2	2	2	1	1	1	1
19	7	4	3	2	2	2	2	2	1	1	1
20	8–9	4	3	3	2	2	2	2	2	1	1

$p = 11$, $t = 3$

$n\backslash k$	4	5	6	7	8	9	10	11	12	13	14
17	4	3	2	2	2	1	1	1	1	1	1
18	4	3	2	2	2	2	1	1	1	1	1
19	5	3	3	2	2	2	2	1	1	1	1
20	5	4	3	2	2	2	2	2	1	1	1

$p = 5$, $t = 4$

$n\backslash k$	5	6	7	8	9	10	11	12	13	14
8	5	3	1	1						
9	9	3	3	1	1					
10	10–14	7	3	3	1	1				
11	17–22	8–10	5	3	3	1	1			
12	26–35	10–14	8	3	3	3	1	1		
13	37–48	13–21	9–10	6	3	3	3	1	1	
14	52–69	18–31	9–14	7	5	3	3	3	1	1
15	71–95	24–40	11–20	7–11	7	3	3	3	3	1
16	95–132	32–54	14–28	7–14	7–9	5	3	3	3	3
17	124–175	42–70	18–40	9–20	7–12	7	5	3	3	3
18	159–215	53–81	23–51	12–30	7–16	7–9	6–7	3	3	3
19	202–285	68–115	29–66	15–38	8–23	7–14	6–9	5	3	3
20	252–359	84–142	36–75	18–42	10–29	7–15	6–12	6–7	5	3

$p = 6$, $t = 4$

$n\backslash k$	5	6	7	8	9	10	11	12	13	14
9	4	3	1	1	1					
10	7	3	3	1	1	1				
11	8–10	5	3	3	1	1	1			
12	11–16	6	4	3	3	1	1	1		
13	15–23	8–10	5	3	3	3	1	1	1	
14	21–34	8–14	7	4	3	3	3	1	1	1
15	29–49	10–19	7–9	6	4	3	3	3	1	1
16	38–65	13–25	7–14	6	5	3	3	3	3	1
17	50–68	17–34	9–19	7–9	6	4	3	3	3	3
18	64–106	22–42	10–24	7–12	6–7	5	4	3	3	3
19	81–144	27–54	12–29	9–17	7–9	6	4	3	3	3
20	101–198	34–66	15–38	9–20	7–12	6	5	4	3	3

$p = 7$, $t = 4$

$n\backslash k$	5	6	7	8	9	10	11	12	13	14
11	5	2	2	1	1	1	1			
12	8	2	2	2	1	1	1	1		
13	8–12	5	2	2	2	1	1	1	1	
14	11–18	6	2	2	2	2	1	1	1	1
15	15–26	8–10	5	2	2	2	2	1	1	1
16	20–36	8–14	6	2	2	2	2	2	1	1
17	26–50	9–19	6–9	5	2	2	2	2	2	1
18	34–60	12–24	6–12	5	2	2	2	2	2	2
19	43–80	15–32	7–16	6–8	5	2	2	2	2	2
20	54–96	18–40	8–20	6–10	5	2	2	2	2	2

$p = 8$, $t = 4$

$n\backslash k$	5	6	7	8	9	10	11	12	13	14
12	4	2	2	1	1	1	1	1		
13	6	2	2	2	1	1	1	1	1	
14	8–10	4	2	2	2	1	1	1	1	1
15	8–13	4	2	2	2	2	1	1	1	1
16	10–18	7	4	2	2	2	2	1	1	1
17	14–23	7–10	4	2	2	2	2	2	1	1
18	17–31	7–14	6	4	2	2	2	2	2	1
19	22–42	8–17	6–9	4	2	2	2	2	2	2
20	27–52	9–21	6–11	4	4	2	2	2	2	2

$p = 9$, $t = 4$

$n\backslash k$	5	6	7	8	9	10	11	12	13	14
13	4	2	2	1	1	1	1	1	1	
14	5	2	2	2	1	1	1	1	1	1
15	8	4	2	2	2	1	1	1	1	1
16	8–10	4	2	2	2	2	1	1	1	1
17	9–14	6	4	2	2	2	2	1	1	1
18	10–18	6	4	2	2	2	2	2	1	1
19	13–23	7–10	5	4	2	2	2	2	2	1
20	16–28	7–13	6	4	2	2	2	2	2	2

$p = 10$, $t = 4$

$n\backslash k$	5	6	7	8	9	10	11	12	13	14
16	6	3	2	2	2	1	1	1	1	1
17	7–9	3	2	2	2	2	1	1	1	1
18	7–12	3	3	2	2	2	2	1	1	1
19	9–15	6	3	2	2	2	2	2	1	1
20	11–19	7	3	3	2	2	2	2	2	1

$p = 11$, $t = 4$

$n\backslash k$	5	6	7	8	9	10	11	12	13	14
17	5	3	2	2	2	1	1	1	1	1
18	7	3	2	2	2	2	1	1	1	1
19	7–10	3	3	2	2	2	2	1	1	1
20	8–13	5	3	2	2	2	2	2	1	1

32.38 Table [223] For $21 \le n \le 32$ and $k = 6$, the following table gives a selection of upper bounds for small $p - t$.

$n \backslash p, t$	4,3	5,3	6,3	7,3	5,4	6,4	7,4	6,5	7,5
21	40	21	13	9	169	80	52	1124	497
22	46	22	15	9	189	101	61	1456	632
23	54	26	17	11	229	127	73	1903	888
24	61	30	20	12	267	143	82	2402	1196
25	68	36	22	15	335	175	107	3043	1513
26	76	40	25	16	403	220	121	3832	1903
27	86	46	27	19	484	243	146	4800	2406
28	98	49	31	22	595	297	160	6191	3058
29	108	56	35	23	719	333	197	7675	3755
30	119	61	39	26	874	397	232	9027	4275
31	133	68	45	29	1028	442	268	11063	5373
32	149	73	50	32	1217	540	304	12823	6560

See Also

§VI.11	General covers with $\lambda = 1$ are equivalent to lotto designs.
§VI.61	Turán systems are special cases of lotto designs
§VI.11.2	Constant weight covering codes are lotto designs.
[797]	Constructions of constant weight covering codes and applications to quantizers.

References Cited: [163, 223, 350, 397, 797, 846, 1046, 1445]

33 Low Density Parity Check Codes

Ian F. Blake

33.1 Low Density Parity Check Codes

33.1 Remark Shannon [1891] formulated the capacity of a channel in terms of bits per channel use and showed that it is possible to encode a source with a rate r that is arbitrarily close to capacity in such a way that the probability of error decreases exponentially in block length. The subject of error correcting codes is a response to the challenge of designing codes that meet or come close to capacity. Three channels of particular interest and their capacities are

(a) the *binary symmetric channel* (BSC) with binary inputs and outputs and the probability of an error is p: $C = 1 + p\log_2 p + (1-p)\log_2(1-p)$;

(b) the *binary erasure channel* (BEC) with binary input and ternary output in which an input of 0 (resp. 1) is received as a 0 (resp. 1) with probability $1 - p$ and each has a probability of p of being received as an erasure E: $C = 1 - p$; and

(c) the binary input additive white gaussian noise (BIAWGN) channel. An input $X \in \{\pm 1\}$ is received as $Y = X + N$ where N is a gaussian random variable of mean 0 and variance σ^2: $C = -\frac{1}{2}\log_2(2\pi e\sigma^2) - \int \phi_\sigma(x)\log_2 \phi_\sigma(x)dx$ is the channel capacity, where $\phi_\sigma(x) = f(x+1)+f(x-1)$, $f(x) = \exp(-(x)^2/2\sigma^2)/\sqrt{2\pi\sigma^2}$.

Low density parity check (LDPC) codes are a particularly successful approach to meeting the challenge of approaching capacity in such channels.

33.2 An $m \times n$ *sparse* matrix is one with fewer than $c \cdot \max(m, n)$ nonzero entries for some small constant c. An *LDPC code* is one with a sparse parity check matrix.

33.3 Remarks

1. Although first proposed in [852] and explored in [2002], their further development was not seriously pursued for many years.
2. LDPC codes with a carefully chosen parity check matrix have good distance properties [852, 1494].
3. Sparseness leads to very efficient and parallelizable *iterative* decoding techniques.
4. For the channels described, there are examples of codes that either achieve capacity or come arbitrarily close to doing so.
5. Among the limitations of LDPC codes are that:
   - Decoding tends to give good performance only for large block lengths, resulting in high latency.
   - LDPC codes tend to have an *error floor*, a region of high signal-to-noise ratios where an increase of SNR results in a smaller decrease in probability of error than for lower SNRs.

33.2 Encoding of LDPC Codes

33.4 There is a natural association of an $m \times n$ binary matrix with a bipartite graph, the *Tanner graph* [2002]. Columns are identified with the left nodes of the bipartite graph (the *message nodes*) and rows with the right (or *check*) nodes of the graph. The variables associated with the check nodes are just the exclusive-OR of the variables associated with neighbor message nodes.

33.5 Remarks

1. The sparsity of the matrix leads to a graph where each node has relatively few neighbors. Decoding algorithms are best described in terms of the Tanner graph.
2. Reducing the parity check matrix of an LPDC code to standard form to allow systematic coding may render it nonsparse, leading to inefficient encoding. Better encoding techniques are given in [1802].
3. Numerous techniques for the construction of LDPC codes have been proposed. These include the original codes of Gallager [852], MacKay codes [1494], irregular degree sequence codes, and codes based on combinatorial structures such as finite geometries and designs.

33.6 A binary code with parity check matrix with d_c ones in each column and d_r ones in each row is a *regular* (or *bi-regular*) LDPC code. Otherwise it is an *irregular* LDPC code.

33.7 Remark Regular LDPC codes are used for the design of *redundant arrays of independent disks*, or *RAID* storage systems. Hellerstein et al. [1088] observe that bi-regularity is desirable to minimize the cost of the basic read and write operations while minimizing loss by erasure. They employ Kirkman triple systems to construct such codes for RAID architectures permitting two erasures. This is generalized in [469] using t-designs and Turán systems.

33.8 Remarks

1. An edge incident with a message (check) node is of *degree* i if it is incident with a message (check) node of degree i.
2. Define λ_i (ρ_i) to be the fraction of message (check) edges of degree i and let $\lambda(x) = \sum_i \lambda_i x^{i-1}$ ($\rho(x) = \sum_j \rho_j x^{j-1}$).
3. Techniques for the design of good irregular LDPC codes by finding good sequences $\{\lambda_i, \rho_i\}$ are given in [1898] for the BEC and in [1487] for more general channels.

33.3 Decoding of LDPC Codes

33.9 Remark Gallager [852] proposed two decoding algorithms for LDPC codes. A *maximum likelihood* decoding algorithm minimizes the probability of error but is too complex for implementation. The two algorithms achieve reasonable performance for much reduced complexity. For the hard decision algorithm, let ℓ_i and r_j denote the degrees of the ith variable node and jth check node, respectively.

33.10 Algorithm Gallager hard decision algorithm for binary irregular LDPC codes [399]:

For $k = 0, 1, \cdots$ do:

1. Variable to check messages: For all edges (i, j) do in parallel:
   If $k = 0$ set $g_{i,j}$ to $r_i \in \{0, 1\}$ - else:
   if more than $\beta(\ell_i - 1)$ of the messages from check nodes
   at the previous stage (excluding message from j from i)
   sent same value i then set $g_{i,j}$ to this value
   else set $g_{i,j}$ to r_j
2. Check to variable messages: for all edges (i, j) do in parallel:
   Check node i sends to variable node j the XOR of all values
   it receives in this round.

33.11 Remark Soft decision decoding algorithms that use direct channel information, rather than quantize the received signal, give better performance at the expense of greater complexity. If s_i is the received channel output for the ith codeword symbol, one often uses either *likelihood* or *log likelihood ratios* (LLR) for the input to the decoding algorithm. Thus $m_i = \log\{p(0|s_i)/p(1|s_i)\} = \log\{p(s_i|0)/p(s_i|1)\}$ where the last expression represents the a posteriori probabilities of receiving a given bit given s_i was received under the assumption of equal prior probabilities of the transmitted bits. Hard decisions quantize the channel output to yield decisions of 0 or 1.

33.12 Algorithm Gallager soft decision algorithm for binary irregular LDPC codes [399]:

For $k = 0, 1, \cdots$ do:

1. Variable to check messages: For all edges (i, j) do in parallel:
   If $k = 0$ set $g_{i,j}$ to m_i - else:
   set $g_{i,j} = m_i + \sum_{N(i)\setminus j} h_{i,k}$ else set $g_{i,j}$ to s_j and send $g_{i,j}$
2. Check to variable messages: for all edges (i, j) do in parallel:
   Check node j sends to variable node i $h_{i,j}$ where:

$$h_{i,j} = f(u) \quad \text{where} \quad u = \prod_{k \in \mathcal{N}(j)\setminus i} \frac{e^{g_{k,j}} - 1}{e^{g_{k,j}} + 1} \quad , \mathcal{N}(j) = \text{neighbors of} \quad j$$
$$\text{and} \quad f(u) = \log \frac{1+u}{1-u}.$$

33.13 Remarks

1. These are examples of *message passing algorithms* where decoding is accomplished by passing messages back and forth on the bipartite graph. The soft decoding algorithm is an example of a *belief propagation* algorithm, where the messages represent probabilities or beliefs as to the possible values.
2. Belief propagation algorithms are in general less powerful than maximum likelihood ones, but computationally more efficient.
3. The analysis of such algorithms yields good approximations to the probability of error. Typically, recursions for the density functions of messages passed along are obtained, techniques that are referred to as *density evolution* [1801].
4. The techniques usually require the various contributions at a node to be independent (this is usually only the case if the neighborhood of a message node to some level is a tree).
5. Such a requirement is only true out to level ℓ (ℓ iterations of the algorithm) if the graph has girth 2ℓ.
6. Even when this is not the case the analysis can still give useful insights and approximations.
7. While graphs with large girth aid in the analysis of message passing algorithms, there are examples of codes with good performance that have small cycles. The performance of many such codes is often only obtainable through simulation.
8. A useful analytical tool to visualize the density evolution process and its behavior in iterative decoding techniques is the EXIT (*extrinsic information transfer*) chart [1803].

33.4 Expander Codes

33.14 An irregular bipartite graph has *expansion* (α, β) if for all subsets S of size at most αn vertices on the left (of a total of n message nodes), the size of the neighborhood of S, $N(S)$, on the right satisfies $N(S) \geq \beta \mid \delta(S) \mid$ where $\delta(S)$ is the set of edges incident to nodes in S.

33.15 Algorithm Sequential decoding of expander codes ([1922, 1487]):

```
1.  If there is a message node with more unsatisfied than satisfied
    check neighbors, flip the value of that node.
2.  Repeat until no such message node remains.
```

33.16 Remark The parallel version of the algorithm considers the number of unsatisfied checks for each message node and then flips the appropriate ones at the same time.

33.17 Lemma [399, 1487, 1922] Let $\alpha > 0$ and $\beta > 3/4 + \epsilon$ for some fixed $\epsilon > 0$. Let B be an irregular (α, β) expander Tanner graph. Then the sequential and parallel decoding algorithms correct up to $\alpha n/2$ errors.

33.5 Coding for the Binary Erasure Channel

33.18 Remark The situation for encoding and decoding for the BEC is now quite a complete picture. The message passing algorithm for the BEC transmits the LLR of $+\infty$ if the (message or check) bit is not erased and 0 otherwise.

33.19 Algorithm Decoding algorithm for the BEC [1898].

For $k = 0, 1, \cdots$ do:

1. Initialize all check nodes to 0.
2. If a message is received, transfer its value to all adjacent check nodes and erase that message node and all incident edges, for all such message nodes.
3. If there is a check node of degree 1, transfer its value to all adjacent message nodes. If all message nodes are not resolved return to step 2.

33.20 Remark

1. The success of the algorithm depends, at each iteration, on the presence of at least one check node of degree 1. An important determination for this is the design of the degree distributions (λ, ρ).
2. [1898] A condition to successfully decode a fraction of δ errors with high probability is that $\delta\lambda(1 - \rho(1 - x)) < x$ for $x \in (0, \delta)$.

33.21 A *capacity-achieving sequence* for a BEC with probability p is a set of two functions $\lambda_n(x)$, $\rho_n(x)$ satisfying the above equation for all $n > n_0$ for a given $\delta < 1 - r$ where r is the code rate and δ the fraction of symbols erased.

33.22 Remark

1. Numerous techniques exist for the design of capacity-achieving sequences for both the BEC and BSC ([1898, 1487], for example); these are techniques for finding λ_i, ρ_i that lead to functions that satisfy the above condition.
2. The complexity of decoding is proportional to the number of edges in the graph. Incarnations of such codes include LT codes, raptor codes, and online codes. The complexity of decoding for online codes is proportional to the code length.
3. A useful notion in the analysis of codes for the BEC is that of a *stopping set*, a subset of the message nodes with the property that the induced subgraph has no neighbor node of degree 1. The existence of a stopping set corresponds to a set of erasures that results in decoding failure.

See Also

§II.§2	Triple systems with forbiddent configurations are used to construct LDPCs.
§II.§7	Resolvable designs are used to construct LDPCs.
§VI.§61	Turán systems are used to construct LDPCs.
§VII.1	Linear codes and parity check matrices.
[1803]	A text on all of the topics of this chapter.

References Cited: [399, 469, 852, 1088, 1487, 1494, 1801, 1802, 1803, 1891, 1898, 1922, 2002]

34 Magic Squares

Joseph M. Kudrle
Sarah B. Menard

34.1 Definitions and Examples

34.1 A *magic square* of order $n > 1$ with *magic constant* d is a $n \times n$ matrix $A = (a_{i,j})$ with integer entries satisfying the following properties:

1. $\sum_{i=1}^{n} a_{i,j} = d$ for all j,
2. $\sum_{j=1}^{n} a_{i,j} = d$ for all i,
3. $\sum_{i=1}^{n} a_{i,i} = d$, and
4. $\sum_{i=1}^{n} a_{i,(n-i+1)} = d$.

34.2 A magic square of order n is *normal* (or *traditional*) when the entries of A are the consecutive integers $\{1, 2, 3, \ldots, n^2\}$. In this case the magic constant $d = \frac{n(n^2+1)}{2}$.

34.3 Examples Magic squares of orders 4, 7 [1562], and 9 [433].

32	4	6	26
10	22	20	16
18	14	12	24
8	28	30	2

10	5	49	37	32	27	15
41	29	24	19	14	2	46
16	11	6	43	38	33	28
47	42	30	25	20	8	3
22	17	12	7	44	39	34
4	48	36	31	26	21	9
35	23	18	13	1	45	40

31	76	13	36	81	18	29	74	11
22	40	58	27	45	63	20	38	56
67	4	49	72	9	54	65	2	47
30	75	12	32	77	14	34	79	16
21	39	57	23	41	59	25	43	61
66	3	48	68	5	50	70	7	62
35	80	17	28	73	10	33	78	15
26	44	62	19	37	55	24	42	60
71	8	53	64	1	46	69	6	51

34.4 A *semi-magic square* is an $n \times n$ matrix satisfying properties 1 and 2 in Def. 34.1.

34.5 A normal magic square of order n is *symmetrical* if, for any pair of symmetric cells (i, j) and $(n + 1 - i, n + 1 - j)$, the sum of the entries in those cells is $n^2 + 1$.

34.6 A magic square is *pandiagonal* if all of the broken diagonals also sum to the magic constant d. These are also refered to as *nasik*, *perfect*, or *diabolic*.

34.7 Remark The normal 7×7 square in Example 34.3 is symmetrical and pandiagonal.

34.8 A magic square is *composite* if it is constructed of smaller magic squares.

34.9 Example A composite magic square of order 9 is given in Example 34.3.

34.10 Remark A quick search of the internet reveals numerous pages devoted to generalizations of magic squares such as magic circles, magic cubes, magic graphs, magic series, magic tesseracts, magic hexagons, magic hexagrams, magic diamonds, magic domino tilings, and magic stars. See, for example, `http://www.geocities.com/~harveyh/` or `http://mathworld.wolfram.com/topics/MagicFigures.html`.

34.2 History

34.11 Remarks The first known magic square dates from 4th century BCE China, but legend dates it to the 23rd century BCE. Known as the *Lo-Shu* (Example 34.12), Chinese myth says that the square was first seen by Emperor Yü on the back of a mystic turtle. There was great reverence for the Lo-Shu, and it became the basis for many of the Chinese constructions for squares of higher orders (such as the 9×9 square in Example 34.3).

In the 9th century CE, magic squares first appeared in the Islamic world. Many early squares are similar to those of the Chinese, but by the 13th century, the Islamic world had devised their own construction methods. The most popular square was of order 4×4. This square, given in Example 34.12 possesses many interesting properties, including being pandiagonal.

34.12 Examples The 3×3 Lo-Shu magic square and the 4×4 "Islamic" magic square.

8	1	6
3	5	7
4	9	2

8	11	14	1
13	2	7	12
3	16	9	6
10	5	4	15

34.13 Remarks After early Muslim invasions, magic squares appeared in India by the 13th century. In 1356, Narayana Pandita presented a group of magic squares along with construction methods in his work *Ganita Kaumudi*. One of the construction methods is today known as De la Hire's method (see Construction 34.19). The construction method known as De la Loubère's method also originated in India (see Construction 34.17).

Magic squares entered the Western World via the trade routes from Asia in the 14th century. They were studied by Jewish and Christian scholars in the *Kabbalah* and used as talismans. Slowly magic squares began to appear in Western art, most notably in the etching *Melencolia I* by Albrecht Dürer in 1514. This aided in attracting the attention of contemporary scholars, and within a short time, magic squares were viewed and studied in a more mathematical fashion. Notable scholars interested in magic squares include Pierre de Fermat, C.G. Bachet de Méziriac, Philipe de la Hire, Bernard Frénicle de Bessy (first to present all 880 essentially different magic squares of order 4), Leonhard Euler, and Benjamin Franklin.

More on the history of magic squares can be found at [433, 859].

34.3 Constructions of Odd Order

34.14 Construction (*Uniform Step Method* [154, 1562]) Assume n is odd. To construct an $n \times n$ normal magic square, let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 matrix where $a, b, c, d \in \mathbb{Z}$. Necessary conditions for this construction to yield a normal magic square are that

$$\gcd(a, n) = \gcd(b, n) = \gcd(c, n) = \gcd(d, n) = \gcd(\det M, n) = 1.$$

Begin the construction by placing the middle number of the sequence $\{1, 2, \ldots, n^2\}$ in the center cell of the array. The remaining numbers of the sequence are then placed consecutively according to the two following moves. After placing a number k that is *not* a multiple of n, the next number, $k+1$, is placed in the array by a *regular* move of a cells to the right and c cells up from the cell containing k. After placing a number k that *is* a multiple of n, the next number, $k+1$ (or 1 if $k = n^2$) is placed in the array

by a *break* move of $a+b$ cells to the right and $c+d$ cells up from the cell containing k. All moves are made as if the square were embedded in the torus.

34.15 Remark If $\gcd(a \pm c, n) = \gcd(b \pm d, n) = \gcd(n, 3) = 1$, then the magic square constructed by the uniform step method is pandiagonal.

34.16 Example A 5×5 magic square using $M = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$.

13 − 17

	15		**17**	
	16			**14**
		13		

18 − 22

	15		17	
	16			14
	22	13		**20**
		19		**21**
18				

23 − 2

24	15	**1**	17	
	16		**23**	14
	22	13		20
		19		21
18		**25**		**2**

3 − 7

24	15	1	17	
5	16	**7**	23	14
6	22	13	**4**	20
	3	19		21
18		25		2

8 − 12

24	15	1	17	**8**
5	16	7	23	14
6	22	13	4	20
12	3	19	**10**	21
18	**9**	25	**11**	2

34.17 Remark The matrix $\begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix}$ yields the method attributed to De la Loubère. The matrix $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ yields the method attributed to Bachet. The matrix $\begin{pmatrix} 1 & 1 \\ 2 & -3 \end{pmatrix}$ constructs a *knight's move* pandiagonal magic square for orders n, where $\gcd(n, 5) = 1$.

34.18 Construction *Orthogonal Latin Square Method.* Assume A and B are orthogonal latin squares of order n where A and B contain the numbers $\{1, 2, \ldots n\}$ and J is the $n \times n$ matrix of all 1's. Then the array $M = A + n(B - J)$ is a semi-magic square. M is a magic square if either

1. A and B are both double-diagonal latin squares, or
2. n is odd and two of the four main forward and back diagonals of A and B are constant and equal to $\frac{n+1}{2}$.

34.19 Remarks *De la Hire's Method* (see [154]) is Construction 34.18.2 where A has constant front diagonals and B has constant back diagonals. *Arnoux's Method* (see [154]) is Construction 34.18.1 for n odd where A and B are special double-diagonal latin squares (basically addition tables modulo n). This method can be used to construct magic squares of any odd order n and pandiagonal magic squares of any odd order n such that $\gcd(n, 3) = 1$. *Margossian's Method* (see [154]) extends Arnoux's method to construct pandiagonal magic squares of order n when $3 \mid n$.

34.20 Example A 5×5 magic square using De la Hire's method.

3	1	2	5	4
4	3	1	2	5
5	4	3	1	2
2	5	4	3	1
1	2	5	4	3

+

5	20	15	0	10
20	15	0	10	5
15	0	10	5	20
0	10	5	20	15
10	5	20	15	0

=

8	21	17	5	14
24	18	1	12	10
20	4	13	6	22
2	15	9	23	16
11	7	25	19	3

34.4 Constructions of Even Order

34.21 Construction [154] *Generalized Doubly Even Method.* Let $n = 4m$, for m any integer. Write the natural numbers in order in the rows of an $n \times n$ square. Then, starting in the upper left corner, divide the square into 4×4 sub-squares. In the main and back diagonal of each 4×4 sub-square, replace the number k by its complement, the number $n^2 + 1 - k$.

34.22 Example The generalized doubly even method to construct an an 8×8 magic square.

1	2	3	**4**	**5**	6	7	**8**
9	**10**	**11**	12	13	**14**	**15**	16
17	**18**	**19**	20	21	**22**	**23**	24
25	26	27	**28**	**29**	30	31	**32**
33	34	35	**36**	**37**	38	39	**40**
41	**42**	**43**	44	45	**46**	**47**	48
49	**50**	**51**	52	53	**54**	**55**	56
57	58	59	**60**	**61**	62	63	**64**

64	2	3	**61**	**60**	6	7	**57**
9	**55**	**54**	12	13	**51**	**50**	16
17	**47**	**46**	20	21	**43**	**42**	24
40	26	27	**37**	**36**	30	31	**33**
32	34	35	**44**	**45**	38	39	**25**
41	**23**	**22**	44	45	**19**	**18**	48
49	**15**	**14**	52	53	**11**	**10**	56
8	58	59	**5**	**4**	62	63	**1**

34.23 Remark *Margossian's Method* (see [154]) constructs *pandiagonal* magic squares of orders $n = 4m$.

34.24 Construction *Strachy's Method* (see [154]). This method constructs squares of singly even orders. Let $n = 2(2m + 1)$. Begin by dividing the square into four equal quarters, call these A, B, C, and D, as shown on the right.

A	C
D	B

Each of these quarters is a square of odd order. Use the method of De la Loubère (Remark 34.17) to construct a magic square in each of these quarters using the following numbers:

1. A is filled with the numbers $\{1, 2, \ldots, u^2\}$,
2. B is filled with the numbers $\{u^2 + 1, \ldots, 2u^2\}$,
3. C is filled with the numbers $\{2u^2 + 1, \ldots, 3u^2\}$, and
4. D is filled with the numbers $\{3u^2 + 1, \ldots, 4u^2\}$,

where $u = n/2$. In the middle row of A, interchange the m cells beginning at the center cell and working left with the corresponding cells in D. In all other rows of A, take the leftmost m cells and interchange these with the corresponding cells in D. Finally, interchange the cells in the rightmost $m-1$ columns of C with the corresponding cells of B.

34.25 Example A 6×6 square using Strachy's method. Here $m = 1$ and $u = 3$.

Starting with

8	1	6	26	19	24
3	**5**	7	21	23	25
4	9	2	22	27	20
35	28	33	17	10	15
30	**32**	34	12	14	16
31	36	29	13	18	11

the resulting square is

35	1	6	26	19	24
3	**32**	7	21	23	25
31	9	2	22	27	20
8	28	33	17	10	15
30	**5**	34	12	14	16
4	36	29	13	18	11

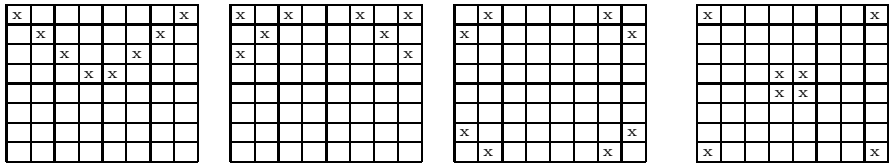
34.5 Ben Franklin's Square

34.26 Example *The Franklin Square.* Ben Franklin constructed this 8×8 semi-magic square in his youth.

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

34.27 Proposition The Franklin square satisfies the following properties:

1. Each row and each column of the square sums to 260,
2. Half rows (the first or last 4 cells in a row) and half columns sum to 130,
3. Any 2×2 sub-square of adjacent cells sums to 130, many other 2×2 sub-square also sum to 130, and
4. Any of the 8 vertical shifts (with wraparound) of the indicated cells in all four of these configurations adds to 260. Furthermore, the cells in any of the 4 cyclic spins of each of the 8 shifts also adds to 260.



34.28 Remark Ben Franklin also constructed a 4×4, a 6×6, another 8×8, and a 16×16 square with similar properties.

See Also

§III.3	Semi-magic squares can be made from orthogonal latin squares
[433]	A complete history of magic squares (through 1973).
[1696]	Contain the complete enumeration of 4×4 magic squares.
[176]	Gives a generating function for enumerating magic squares.

References Cited: [154, 176, 433, 859, 1562, 1696]

35 Mendelsohn Designs

Eric Mendelsohn

35.1 Definitions and Examples

35.1 The k-tuple $(x_0, x_1, x_2, \ldots, x_{k-1})$ *cyclically contains* the ordered pairs (x_0, x_1), $(x_1, x_2), \ldots, (x_{k-1}, x_0)$, and no others. The notation $(x_i, x_{i+1}) \subset_{\mathbb{Z}_k} (x_0, \ldots, x_{k-1})$ is used or, where no confusion arises, simply "$\subset$" is used. Elements x_i, x_{i+t} are *t-apart* in the k-tuple, where $i + t$ is taken modulo k.

35.2 A (v,k,λ)-*Mendelsohn design*, or MD(v,k,λ), is a set V together with a collection $\mathcal{B}$ (*blocks*) of ordered k-tuples of distinct elements from V, such that each ordered pair (x,y) with $x \neq y$ is cyclically contained in λ blocks. An M$(v,3,\lambda)$ is a *Mendelsohn triple system*, MTS(v,λ).

35.3 Example Any triple system can be made into a Mendelsohn triple system by replacing $\{a,b,c\}$ by both (a,b,c) and (a,c,b).

35.4 Example An MTS$(4,1)$. Let $\mathcal{B} = \{(0,1,2),(1,0,3),(2,1,3),\ (0,2,3)\}$ with $V = \{0,1,2,3\}$.

35.5 The *converse* of a Mendelsohn design is the design obtained by reversing the order of its blocks.

35.6 A *perfect Mendelsohn design* (PMD) is an MD(v,k,λ), such that for every $i = 1,2,3,\ldots,k-1$, each ordered pair (x,y) is i-apart in exactly λ blocks. Every MTS is perfect.

35.7 Remark This is the analogue of "perfect" for (undirected) cycle systems. See §VI.12.6

35.8 The *underlying design* of a PMD(v,k,λ) is the BIBD$(v,k,(k-1)\lambda)$ obtained by "forgetting" the order structure on the blocks.

35.9 A Mendelsohn design is *simple* if it has no repeated blocks. It is *pure* if its underlying design has no repeated blocks.

35.10 Example A pure MD$(5,3,3)$. Let $\mathcal{B} = [(0,1,2),(0,2,4),(0,3,1),(0,4,3)] \pmod 5$ with $V = \{0,1,2,3,4\}$.

35.11 Example Small $(v,4,2)$-PMDs.

$v=4:\quad \mathcal{B} = [(\infty,0,1,2),(\infty,0,2,1)] \pmod 3$

$v=6:\quad \mathcal{B} = \{(1,2,3,4),(1,2,5,3),(1,6,3,2),(1,4,2,6),(1,6,2,5),$
$(1,4,5,2),(1,5,6,3),(1,3,6,4),(1,3,4,5),(1,5,4,6),$
$(2,3,5,4),(2,4,3,6),(2,6,5,3),(2,4,6,5),(3,5,6,4)\}.$

$v=8:\quad \mathcal{B} = [(\infty,0,1,3),(\infty,0,-1,-3),(0,1,-2,2),(0,-1,2,-2)] \pmod 7$

$v=10:\quad \mathcal{B} = [(\infty,0,3,1),(\infty,0,4,8),(0,1,2,4),(0,3,5,1),(0,-3,3,1)] \pmod 9$

$v=12:\quad \mathcal{B} = [(\infty,0,1,5),(\infty,0,-1,-5),(0,1,3,8),(0,-1,-3,-8),$
$(0,-4,-2,-5),(0,3,1,5)] \pmod{11}$

$v=14:\quad \mathcal{B} = [(\infty,0,-1,-2),(\infty,0,-4,2),(0,1,3,6),(0,4,1,-5),$
$(0,6,1,3),(0,1,6,-4),(0,2,-4,4)] \pmod{13}$

35.12 A Mendelsohn design is *resolvable* (RMD) if either

(a) $v \equiv 0 \pmod k$ and its blocks can be partitioned into $\lambda(v-1)$ resolution classes or

(b) $v \equiv 1 \pmod k$ and its blocks can be partitioned into λv near-resolution classes.

35.13 Example A resolvable $(6,3,6)$-Mendelsohn design. Here $[(0,1,3),(\infty,4,2)]$; $[(0,2,1),(\infty,4,3)]$; and $[(0,3,4),(\infty,2,1)]$ give three resolution classes; develop modulo 5 for the remaining 12.

35.14 Example A resolvable MTS(10,1). The blocks are written as rows.

0	1	2	3	4	5	6	7	8	9
231	480	398	975	702	826	514	649	167	053
794	369	541	106	635	437	873	085	952	246
865	572	607	428	189	901	092	213	340	781

35.2 Relations with Quasigroups and Latin Squares

35.15 Theorem If $(Q, \cdot)$ is a quasigroup satisfying $x \cdot x = x$ and $x \cdot (y \cdot x) = y$ for all $x, y \in Q$ (an *idempotent semisymmetric* quasigroup), let $\mathcal{B} = \{(x, y, x \cdot y) : x, y \in Q\}$. Then $(Q, \mathcal{B})$ is a Mendelsohn triple system MTS$(|Q|, 1)$. Conversely, if $(Q, \mathcal{B})$ is an MTS, then $(Q, \cdot)$, defined by $x \cdot x = x$ for all $x \in Q$, and $x \cdot y = z$ whenever $(x, y, z) \in \mathcal{B}$, is an idempotent semisymmetric quasigroup.

35.16 Theorem Let $w_0(x, y) = x,\ w_1(x, y) = y,\ w_2(x, y) = x \cdot y$, and $w_n(x, y) = w_{n-2}(x, y) \cdot w_{n-1}(x, y)$. Suppose that $(Q, \cdot)$ exists such that

1. $x \cdot x = x$ for all $x \in Q$;
2. $w_k(x, y) = x$ for all $x, y \in Q$; and
3. for any a, b, $w_r(a, x) = b$ has a unique solution for $r = 1, 2, \ldots, k-1$.

Let $\mathcal{B} = \{(w_0(x, y), \cdots, w_{k-1}(x, y)) : x, y \in Q, x \neq y\}$. Then $(Q, \mathcal{B})$ is a PMD of order v, blocksize k, and index 1. The converse also holds.

35.17 Theorem Let v be an odd integer and (X, B) be a $(v, k, 1)$-PMD. Then if B^* is the matrix obtained by writing out the blocks of B and all their cyclic shifts as columns, and X^* is $[x, x, \cdots, x]^T, x \in X$, then $[B^* \mid X^*]$ is an orthogonal array corresponding to $k-2$ idempotent MOLS of side v.

35.18 If $(V, \mathcal{B})$ is a resolvable $(v, k, 1)$-PMD (RPMD) with $v \equiv 1 \bmod k$, then the quasigroups $(V, *_i)$ for $1 \leq i \leq k-1$ *associated with* $(V, \mathcal{B})$ are defined by $x *_i x = x$ and $x *_i z = y$ if (x, y) are i-apart in the block whose resolution class misses z.

35.19 Remark The $k-1$ quasigroups obtained have multiplication tables that are idempotent MOLS. Example 35.14 yields the following two MOLS(10).

0	4	7	6	2	1	9	8	3	5
2	1	5	0	8	9	4	3	6	7
3	5	2	8	7	6	0	1	9	4
1	6	9	3	5	7	8	2	4	0
7	8	1	2	4	3	5	9	0	6
8	7	4	9	6	5	1	0	2	3
5	9	0	1	3	8	6	4	7	2
9	2	6	5	0	4	3	7	1	8
6	0	3	4	9	2	7	5	8	1
4	3	8	7	1	0	2	6	5	9

0	8	6	1	7	9	2	5	4	3
3	1	4	6	9	0	5	2	7	8
1	7	2	4	0	8	9	3	5	6
2	9	8	3	6	4	7	1	0	5
9	0	5	8	4	7	1	6	3	2
6	2	1	7	3	5	4	8	9	0
8	3	7	0	5	2	6	9	1	4
4	5	0	9	2	3	8	7	6	1
5	4	9	2	1	6	3	0	8	7
7	6	3	5	8	1	0	4	2	9

As noted in [857], these two MOLS have four disjoint common transversals (each row specifies the ten cells of a transversal):

1.	(0,0)	(1,1)	(2,2)	(3,3)	(4,4)	(5,5)	(6,6)	(7,7)	(8,8)	(9,9)
2.	(0,1)	(1,0)	(2,4)	(3,9)	(4,6)	(5,3)	(6,5)	(7,8)	(8,2)	(9,7)
3.	(0,4)	(1,6)	(2,5)	(3,0)	(4,7)	(5,9)	(6,8)	(7,3)	(8,1)	(9,2)
4.	(0,9)	(1,8)	(2,0)	(3,2)	(4,1)	(5,6)	(6,7)	(7,4)	(8,5)	(9,3)

35.3 Mendelsohn Designs from BIBDs

35.20 Theorem If p is an odd prime and if a BIBD$(v, p, 1)$ exists, then a $(v, p, 1)$-PMD exists. If in addition $v \equiv 1 \pmod{p}$ and if the BIBD is near-resolvable, then the PMD is near-resolvable.

35.21 A BIBD$(v, k, (k-1)\lambda)$ is *orientable* if a cyclic order can be placed on its blocks to form a PMD(v, k, λ).

35.22 Theorem For every $v \equiv 0, 1 \pmod 3$, $v \geq 6$, there is a nonorientable BIBD$(v, 3, 2)$.

35.23 Remark Theorem 35.22 is in direct contrast with Theorem VI.20.31 (that *every* BIBD$(v, 3, 2)$ is directable).

35.24 Theorem There is an algorithm for determining whether a BIBD$(v, 3, 2)$ can be oriented that has $O(v^2)$ running time. It is NP-complete to determine whether a BIBD$(v, 3, 2\lambda)$ can be oriented if $\lambda > 1$.

35.25 Let $D = (V, \mathcal{B})$ be a Steiner triple system and let the map $f : V \to V$ be an involution with one fixed point. If f has the properties that the image of a block is never a block, that $(V, \mathcal{B} \cup f(\mathcal{B}))$ is orientable, and that f preserves cyclic order in this orientation, then D is an *antipodal* triple system.

35.26 Example Any cyclic $TS(v, 1)$, with $v \equiv 1 \pmod 6$ and $f : x \to -x \pmod v$, is antipodal.

35.27 Theorem There exists an antipodal $TS(v, 1)$ for all $v \equiv 1, 3 \pmod 6$ [904, 905].

35.4 Existence

35.28 Theorem A necessary condition for a MD(v, k, λ) to exist is that $\lambda v(v-1) \equiv 0 \pmod k$ (and $v \geq k$).

35.29 Table The basic existence results. Here, a stronger condition implies the weaker one; for example, an RPMD implies an RMD, an PMD, and an MD.

$k = 3$

λ	Type of Design	Existence Result	Reference
1	MTS	$v \equiv 0, 1 \pmod 3$, $v \neq 6$	[1586]
	pure MTS	$v \equiv 0, 1 \pmod 3$, $v \neq 3, 6$	see [578]
	RMTS	$v \equiv 0, 1 \pmod 3$, $v \neq 6$	see [578]
λ	MTS	$\lambda \equiv 0 \pmod{\gcd(v-2, 3)}$, $v \neq 6$	see [578]

$k \geq 4$

k	PMD	RMD	RPMD
4	$\lambda v(v-1) \equiv 0 \pmod 4$ except $v = 4, \lambda$ odd and $v = 8, \lambda = 1$ [207]	$\lambda = 1$, $v \equiv 0, 1 \pmod 4$, $v \neq 4, 12$	$\lambda = 1 : v \equiv 0, 1 \pmod 4$, $v \neq 4, 8, 12$ and at most 27 possible exceptions given in Table 35.30. $\lambda > 1$: all v admissible except $v = 4$, λ odd [2203].
5	$\lambda = 1$: $v \equiv 0, 1 \pmod 5$. $v \neq 6, 10$, also $v = 15, 20$ are possible exceptions, see [194]. $\lambda > 1$: no exceptions, see [194]		$\lambda = 1 : v \equiv 0 \pmod 5$, $v \neq 10, 15$, and 15 possible exceptions in Table 35.31. $\lambda = 1 : v \equiv 1 \pmod 5$, $v \neq 6$ and possible exception $v = 26$ [13].

$k \geq 4$ (cont.)

k	PMD	RMD	RPMD
6	$\lambda = 1$: $v \equiv 0, 1 \pmod 3$, $v \geq 7$, $v \neq 10$, possible exceptions in Table 35.32. [1601, 16, 12] $\lambda > 1$: all $v \geq 6$, except $(6, 6, \lambda)$-PMD do not exist when $\lambda = 2$ or is odd. [12]	$\lambda = 1 : v \equiv 1 \pmod 6$, $v \geq 7$ [16]	$\lambda = 1, v \equiv 1 \pmod 6$: possible exceptions in Table 35.33. [12]
7	$\lambda = 1$: $v \equiv 0, 1 \pmod 7$, $v \geq 7$, possible exceptions in Table 35.34. $\lambda > 1$: all admissible v.		

35.30 Table [2206] Values of v for which the existence of a $(v, 4, 1)$-RPMD is open.
16, 20, 24, 32, 36, 44, 48, 52, 56, 64, 68, 76, 84, 88, 92, 96, 104, 108, 116, 124, 132, 148, 152, 156, 172, 184, 188

35.31 Table [13, 15] Values of v for which the existence of a $(v, 5, 1)$-RPMD is open.
20, 26, 30, 90, 95, 100, 110, 115, 120, 130, 135, 140, 150, 160, 170, 190, 195, 210

35.32 Table Values of v for which the existence of a $(v, 6, 1)$-PMD is open.
$v \equiv 0 \pmod 6$: 12, 18, 24, 30, 48, 54, 60, 72, 84, 90, 96, 102, 108, 114, 132, 138, 150, 162, 168, 180, 192, 198
$v \equiv 1 \pmod 6$: no exceptions.
$v \equiv 3 \pmod 6$: 9, 15, ...,135, 153, 159, ...,183, 207, 213, 219, 237, 243, 255, 297, 375, 411, 435, 453, 459, 471, 489, 495, 513, 519, 609, 615, 621, 657
$v \equiv 4 \pmod 6$: 10, 16, 22, 34, 52, 58, ...,148

35.33 Table [12] Values of $v \equiv 1 \pmod 6$ for which the existence of a $(v, 6, 1)$-RPMD is open.
205, 235, 265, 319, 355, 391, 415, 451, 493, 649, 667, 697, 781, 1315

35.34 Table [194] Values of v for which the existence of a $(v, 7, 1)$-PMD is open.
14, 15, 21, 22, 28, 35, 36, 42, 70, 84, 98, 99, 126, 140, 141, 147, 148, 154, 182, 183, 196, 238, 245, 273, 294

35.35 Theorem [198, 1587, 2205] The necessary conditions are asymptotically sufficient for the existence of a (v, k, λ)-PMD and a $(v, k, 1)$-RPMD with $v \equiv 0, 1 \pmod k$.

35.36 Theorem Let p be an odd prime, then there exists a $(p^2, p, 1)$-RMD. If $p \equiv 1 \pmod k$, then there exists a $(p^r, k, 1)$-RPMD, for all $r > 1$.

35.5 Packings and Coverings

35.37 A (v, k, λ)-*perfect Mendelsohn packing design* is a set V together with a collection $\mathcal{B}$ (*blocks*) of ordered k-tuples of distinct elements from V, such that each ordered pair (x, y) with $x \neq y$ appears t-apart in *at most* λ blocks of $|\mathcal{B}|$ for all $t = 1, 2, \ldots, k-1$. If no other such packing has more blocks, the packing is *maximum*. The number of blocks in a maximum packing is the *packing number* and denoted $P(v, k, \lambda)$.

A (v, k, λ)-*perfect Mendelsohn covering design* is defined analogously. The *covering number* is denoted $C_M(v, k, \lambda)$.

35.38 Example A (9,5,1)-perfect Mendelsohn packing design.
$V = \mathbb{Z}_7 \cup \{x, y\}$, $\mathcal{B} = [(x, 0, 1, 3, 6), (x, 0, 6, 4, 1)] \pmod 7$

35.39 Example A (7,4,1)-perfect Mendelsohn covering design.
$V = \{0, 1, 2, 3, 4\} \cup \{x, y\}$, $\mathcal{B} = \{(x, y, 2, 3), (x, y, 2, 3), (x, y, 3, 4), (x, 0, 4, y), (x, 2, y, 0), (x, 1, 2, 0), (x, 3, y, 1), (x, 4, 1, 2), C, (0, 3, 1, 4), (0, 2, 4, 4)\}$

35.40 Lemma 1. $P(v, k, \lambda) \le \lfloor \lambda v(v-1)/k \rfloor = D(v, k, \lambda)$ and
2. $C_M(v, k, \lambda) \ge \lceil \lambda v(v-1)/k \rceil = C(v, k, \lambda)$.

35.41 Theorem [202] For all integers $v \ge 3$, $P(v, 3, \lambda) = D(v, 3, \lambda)$, except when
1. $v = 6, \lambda = 1$ in which case $P(6, 3, 1) = D(6, 3, 1) - 2 = 8$, or
2. $v \equiv 2 \pmod 3$ and $\lambda \equiv 2 \pmod 3$ in which case $P(v, 3, \lambda) = D(v, 3, \lambda) - 1$.

35.42 Theorem [202] For all integers $v \ge 3$, $C_M(v, 3, \lambda) = C(v, 3, \lambda)$, except when $v \equiv 2 \pmod 3$ and $\lambda \equiv 1 \pmod 3$ and $C_M(6, 3, 1)$. In these cases $C_M(v, 3, \lambda) = C(v, 3, \lambda) + 1$.

35.43 Theorem [202] For all integers $v \ge 4$,
1. $P(v, 4, 1) = D(v, 4, 1)$, except for $v \in \{4, 6, 7, 8\}$ and possibly excepting $v \in \{19, 27\}$; and
2. $C_M(v, 4, 1) = C(v, 4, 1)$, except for $v \in \{4, 8\}$ and possibly excepting $v \in \{6, 10, 11, 14, 15, 18, 19\}$.

35.44 Theorem [204] For all integers $v \ge 5$, $P(v, 5, 1) = D(v, 5, 1) - 1$ except for $v \in \{6, 7, 10\}$ and possibly $v \in \{8, 12, 15, 17, 20\}$.

35.6 Enumeration

35.45 Two MTSs are *equivalent* if they are isomorphic or if one is isomorphic to the converse of the other.

35.46 Table [697, 857] The number $M(v)$ of inequivalent MTS(v,1).

v	3	4	6	7	9	10	12
$M(v)$	1	1	0	3	18	143	4,905,693

35.47 Example The three inequivalent MTS(7,1).
1. [(0, 1, 3) (0, 3, 1)] (mod 7);
2. [(0, 1, 3) (0, 3, 2)] (mod 7);
3. {(0,1,2), (0,2,1), (0,3,4), (0,4,3), (0,5,6), (0,6,5) (1,3,5), (1,6,3), (1,5,4), (1,4,6), (2,5,3), (2,3,6) (2,4,5), (3,6,4)}.

35.48 Table The 18 inequivalent MTS(9)s. The numbering on the left indicates the underlying BIBD(9,3,2) from which this MTS was obtained by orienting the blocks (see Table II.1.23 for the list of BIBD(9,3,2)s).

MTSs of order 9												
1	012	102	034	304	135	315	238	328	147	417	246	426
	056	506	257	527	458	548	168	618	367	637	078	708
2	012	102	034	304	135	315	237	328	147	418	246	426
	056	506	258	527	457	548	168	617	367	638	078	708
4	012	102	034	304	135	317	237	326	148	415	246	428
	056	506	258	527	538	457	167	618	368	647	078	708
5	012	102	034	304	135	317	238	326	148	415	246	427
	056	506	257	528	537	458	167	618	368	647	078	708
7	012	102	034	304	136	315	237	328	145	418	246	427
	056	507	258	526	357	548	068	167	638	647	708	178

10a	012	102	034	304	135	317	236	328	146	418	245	427
	056	506	157	258	537	548	168	267	638	647	078	708
10b	012	102	034	304	135	317	238	326	148	416	247	425
	056	506	157	528	537	458	618	627	368	467	078	708
11	012	102	034	304	136	315	238	327	147	418	245	426
	056	507	516	257	358	548	068	628	637	467	708	178
12	012	102	034	304	136	315	237	328	147	418	245	426
	056	507	516	258	357	548	068	627	638	467	708	178
20	012	102	034	305	138	314	235	326	046	417	247	428
	507	157	516	258	456	548	068	618	627	367	708	378
21	012	102	034	305	138	314	235	328	046	417	247	426
	507	157	516	256	458	548	068	618	367	637	708	278
23a	012	102	034	305	138	314	236	327	046	417	245	428
	507	157	516	258	356	548	068	618	267	647	708	378
23b	012	102	034	305	138	314	236	327	046	417	248	425
	507	157	516	528	356	458	068	618	267	647	708	378
24	012	103	023	213	045	406	146	415	247	428	348	437
	057	517	258	526	356	538	608	168	627	367	078	718
30	012	103	023	214	135	328	045	406	417	246	347	438
	057	156	258	527	536	548	608	168	267	637	078	718
31	012	103	023	214	135	327	046	405	418	247	348	436
	507	156	258	526	538	457	068	167	628	637	708	178
33	012	103	024	215	304	135	237	328	146	418	426	347
	056	507	258	536	457	548	068	167	627	638	708	178
34	012	103	024	215	304	136	237	326	145	418	427	348
	056	507	258	357	538	546	068	167	628	647	708	178

35.49 Remark For $v > 12$, no exact value of $M(v)$ is known. Theorem 35.50 gives an asymptotic bound.

35.50 Theorem $M(v) = \exp(\frac{v^2 \ln v}{3}(1 + o(1)))$ as $v \to \infty$. This is the same bound as for $TS(v, 2)$s. It is not known what proportion of $TS(v, 2)$s are orientable.

See Also

§II.7	Resolvable and near-resolvable designs.
§III.2	Quasigroups; self-orthogonal Mendelsohn triple systems.
§VI.11	Coverings.
§VI.20	Directed designs.
§VI.40	Packings.
§VI.64	A directed whist tournament is a RPMD with block size four.
[1586]	The first paper written on Mendelsohn triple systems.
[193]	A survey of Mendelsohn packings and coverings.
[578]	A book on triple systems.
[194]	A survey of perfect Mendelsohn designs.
[203]	Incomplete and group divisible Mendelsohn designs and frames.
[1248]	Large and overlarge sets of Mendelsohn designs.
[697]	Hybrid triple systems.
[395]	Cayley designs, a generalization of Mendelsohn designs.

References Cited: [12, 13, 15, 16, 193, 194, 198, 202, 203, 204, 207, 395, 578, 697, 857, 904, 905, 1248, 1586, 1587, 1601, 2203, 2205, 2206]

36 Nested Designs

J. P. Morgan

36.1 NBIBDs: Definition and Example

36.1 If the blocks of a BIBD $(\mathcal{V}, \mathcal{D}_1)$ with v symbols in b_1 blocks of size k_1 are each partitioned into sub-blocks of size k_2, and the $b_2 = b_1k_1/k_2$ sub-blocks themselves constitute a BIBD $(V, \mathcal{D}_2)$, then the system of blocks, sub-blocks, and symbols is a *nested balanced incomplete block design* (nested BIBD or NBIBD) with parameters $(v, b_1, b_2, r, k_1, k_2)$, r denoting the common replication. $(V, \mathcal{D}_1)$ and $(V, \mathcal{D}_2)$ are the *component BIBDs* of the NBIBD.

36.2 **Example** An NBIBD(16,24,48,15,10,5). Sub-blocks are separated by |.

$\{0,1,2,3,4|5,6,7,8,9\}$ $\{0,1,2,3,5|4,6,10,11,12\}$ $\{0,1,2,3,6|4,5,13,14,15\}$
$\{0,1,10,11,12|2,3,7,8,9\}$ $\{0,2,13,14,15|1,3,7,8,9\}$ $\{0,3,13,14,15|1,2,10,11,12\}$
$\{0,4,5,7,11|1,8,10,13,14\}$ $\{0,4,5,9,10|1,7,12,13,15\}$ $\{0,4,5,8,12|1,9,11,14,15\}$
$\{0,6,7,10,13|2,4,8,11,14\}$ $\{0,6,9,12,15|2,4,7,10,13\}$ $\{0,6,8,11,14|2,4,9,12,15\}$
$\{0,7,8,10,15|3,5,6,12,14\}$ $\{0,7,9,12,14|3,5,6,11,13\}$ $\{0,8,9,11,13|3,5,6,10,15\}$
$\{1,5,7,12,14|2,6,8,10,15\}$ $\{1,5,9,11,13|2,6,7,12,14\}$ $\{1,5,8,9,15|2,6,9,11,13\}$
$\{1,4,6,7,13|3,8,11,12,15\}$ $\{1,4,6,9,15|3,7,10,11,14\}$ $\{1,4,6,8,14|3,4,8,12,13\}$
$\{2,5,7,11,15|3,4,8,12,13\}$ $\{2,5,9,10,14|3,4,7,11,15\}$ $\{2,5,8,12,13|3,4,9,10,14\}$

36.2 NBIBDs: Existence

36.3 **Proposition** The necessary conditions for existence of a NBIBD are those for the two component BIBDs $(V, \mathcal{D}_1)$ and $(V, \mathcal{D}_2)$. Together they are $b_1 \geq v$, $v|b_1k_1$, $v(v-1)|b_1k_1(k_1-1)$, and $v(v-1)|b_1k_1(k_2-1)$. The necessary conditions are sufficient for $k_1 = 4$ [1068].

36.4 **Remarks** There are 3 nonisomorphic BIBDs with $(v, b_1, k_1) = (10, 15, 6)$ and 960 nonisomorphic BIBDs with $(v, b_2, k_2) = (10, 30, 3)$, but there is no NBIBD$(10, 15, 30, 9, 6, 3)$ [1109]. Thus, the necessary conditions are not sufficient. This is the only case of nonexistence where suitable component designs do exist for $v \leq 16$ and $r \leq 30$.

36.5 **Table** Initial blocks for NBIBDs for $v \leq 16$ and $r \leq 16$. One solution, provided at least one exists, is listed for each set of parameters meeting the necessary conditions, except that multiples of r are not listed for fixed values of (v, k_1, k_2). Some initial blocks are taken through partial cycles, such as PC(5) $\Rightarrow$ subcycle of order 5.

$(v, b_1, b_2, r, k_1, k_2)$	Blocks
1. $(5, 5, 10, 4, 4, 2)$	{1 4 | 2 3} mod 5
2. $(7, 7, 21, 6, 6, 2)$	{1 6 | 2 5 | 4 3} mod 7
3. $(7, 7, 14, 6, 6, 3)$	{1 2 4 | 6 5 3} mod 7
4. $(8, 14, 28, 7, 4, 2)$	{0 1 | 4 2}{3 6 | 5 ∞} mod 7
5. $(9, 18, 36, 8, 4, 2)$	{01 02 | 10 20}{11 22 | 12 21} mod (3,3)
6. $(9, 12, 36, 8, 6, 2)$	{1 2 | 3 6 | 4 ∞}{5 6 | 7 2 | 0 ∞}{0 4 | 1 7 | 3 5} PC(4), mod 8
7. $(9, 12, 24, 8, 6, 3)$	{1 3 4 | 2 6 ∞}{5 7 0 | 2 6 ∞}{1 3 4 | 5 7 0} PC(4), mod 8
8. $(9, 9, 36, 8, 8, 2)$	{1 8 | 2 7 | 3 6 | 4 5} mod 9

$(v, b_1, b_2, r, k_1, k_2)$	Blocks
9. $(9, 9, 18, 8, 8, 4)$	{01 02 10 20 | 11 22 12 21} mod (3,3)
10. $(10, 15, 45, 9, 6, 2)$	$\{0_0\ 2_0 \mid 3_0\ 2_1 \mid 3_1\ 4_1\}\{2_0\ 3_0 \mid 0_0\ 3_1 \mid 4_0\ 0_1\}\{0_0\ 0_1 \mid 1_0\ 3_1 \mid 2_1\ 4_1\}$ mod 5
11. $(10, 15, 30, 9, 6, 3)$	No NBIBD exists, see Example 36.28 for $(10, 30, 60, 18, 6, 3)$
12. $(10, 10, 30, 9, 9, 3)$	$\{1_0\ 2_0\ 4_1 \mid 3_0\ 4_0\ 3_1 \mid 0_1\ 1_1\ 2_1\}\{2_0\ 3_1\ 0_0 \mid 1_0\ 2_1\ 3_0 \mid 1_1\ 4_0\ 4_1\}$ mod 5
13. $(6, 15, 30, 10, 4, 2)$	$\{0\ 2 \mid 1\ 3\}\{\infty\ 0 \mid 3\ 4\}\{\infty\ 4 \mid 1\ 2\}$ mod 5
14. $(11, 11, 55, 10, 10, 2)$	{1 10 | 2 9 | 3 8 | 4 7 | 5 6} mod 11
15. $(11, 11, 22, 10, 10, 5)$	{1 3 4 5 9 | 2 6 8 10 7} mod 11
16. $(12, 33, 66, 11, 4, 2)$	$\{0\ 1 \mid 3\ 7\}\{10\ 2 \mid 9\ 4\}\{8\ 6 \mid 5\ \infty\}$ mod 11
17. $(12, 22, 66, 11, 6, 2)$	$\{0\ 3 \mid 1\ 5 \mid 4\ 9\}\{8\ 10 \mid 7\ 6 \mid 2\ \infty\}$ mod 11
18. $(12, 22, 44, 11, 6, 3)$	$\{0\ 1\ 3 \mid 4\ 5\ 9\}\{10\ 7\ \infty \mid 6\ 8\ 2\}$ mod 11
19. $(7, 21, 42, 12, 4, 2)$	$\{0\ 1 \mid 4\ 2\}\{0\ 2 \mid 1\ 4\}\{0\ 4 \mid 2\ 1\}$ mod 7
20. $(13, 39, 78, 12, 4, 2)$	$\{1\ 12 \mid 5\ 8\}\{2\ 11 \mid 3\ 10\}\{4\ 9 \mid 6\ 7\}$ mod 13
21. $(13, 26, 78, 12, 6, 2)$	{3 10 | 4 9 | 1 12}{5 8 | 11 2 | 6 7} mod 13
22. $(13, 26, 52, 12, 6, 3)$	$\{1\ 3\ 9 \mid 4\ 12\ 10\}\{2\ 6\ 5 \mid 7\ 8\ 11\}$ mod 13
23. $(13, 13, 78, 12, 12, 2)$	$\{1\ \ 12 \mid 2\ 11 \mid 3\ 10 \mid 4\ 9 \mid 5\ 8 \mid 6\ 7\}$ mod 13
24. $(13, 13, 52, 12, 12, 3)$	$\{1\ 3\ 9 \mid 4\ 12\ 10 \mid 2\ 6\ 5 \mid 7\ 8\ 11\}$ mod 13
25. $(13, 13, 39, 12, 12, 4)$	$\{1\ 12\ 5\ 8 \mid 2\ 11\ 3\ 10 \mid 4\ 9\ 6\ 7\}$ mod 13
26. $(13, 13, 26, 12, 12, 6)$	$\{1\ 3\ 9\ 4\ 12\ 10 \mid 2\ 6\ 5\ 7\ 8\ 11\}$ mod 13
27. $(15, 35, 105, 14, 6, 2)$	$\{1_1\ 0_0 \mid 2_1\ 0_1 \mid 4_1\ \infty\}\{0_0\ 3_0 \mid 0_1\ 5_0 \mid \infty\ 6_0\}\{2_0\ 1_0 \mid 4_0\ 3_1 \mid 1_1\ 0_1\}$ $\{2_0\ 0_1 \mid 5_0\ 1_1 \mid 3_1\ 3_0\}\{4_0\ 1_1 \mid 5_0\ 0_0 \mid 0_1\ 3_1\}$ mod 7
28. $(15, 35, 70, 14, 6, 3)$	$\{1_1\ 2_1\ 4_1 \mid 0_0\ 0_1\ \infty\}\{0_0\ 0_1\ \infty \mid 3_0\ 5_0\ 6_0\}$ $\{2_0\ 4_0\ 1_1 \mid 1_0\ 3_1\ 0_1\}\{2_0\ 5_0\ 3_1 \mid 0_1\ 1_1\ 3_0\}\{4_0\ 5_0\ 0_1 \mid 1_1\ 0_0\ 3_1\}$ mod 7
29. $(15, 21, 105, 14, 10, 2)$	No $\mathcal{D}_1$ exists, but $(15, 42, 210, 28, 10, 2)$ does exist ([1638])
30. $(15, 21, 42, 14, 10, 5)$	No $\mathcal{D}_1$ exists, but $(15, 42, 84, 28, 10, 5)$ does exist ([1638])
31. $(15, 15, 105, 14, 14, 2)$	{1 14 | 2 13 | 3 12 | 4 11 | 5 10 | 6 9 | 7 8} mod 15
32. $(15, 15, 30, 14, 14, 7)$	$\{0_1\ 1_1\ 2_1\ 3_1\ 4_1\ 5_1\ 6_1 \mid 0_0\ 1_0\ 2_0\ 3_0\ 4_0\ 5_0\ 6_0\}$ fixed, $\{\infty\ 4_0\ 1_0\ 1_1\ 2_0\ 4_1\ 2_1 \mid 0_1\ 6_1\ 5_1\ 5_0 3_1\ 6_0\ 3_0\}$ $\{0_0\ 2_0\ 4_0\ 5_1\ 1_0\ 6_1\ 3_1 \mid \infty\ 6_0\ 5_0\ 4_1\ 3_0\ 2_1\ 1_1\}$ mod 7
33. $(16, 60, 120, 15, 4, 2)$	$\{\infty\ 0 \mid 5\ 10\}\{1\ 2 \mid 4\ 8\}\{6\ 9 \mid 7\ 13\}\{11\ 3 \mid 12\ 14\}$ mod 15
34. $(16, 40, 120, 15, 6, 2)$	$\{0\ 1 \mid 9\ 3 \mid 5\ 12\}\{0\ 3 \mid 1\ 12 \mid 6\ 2\}\{11\ 9 \mid 1\ 3 \mid 0\ 8\}$ mod 16 last block PC(8)
35. $(16, 40, 80, 15, 6, 3)$	$\{0_0\ 0_1\ 0_2 \mid 1_1\ 2_1\ 3_1\}\{1_0\ 3_0\ 0_2 \mid 1_2\ 0_1\ 2_1\}\{1_0\ 3_0\ 0_1 \mid 0_0\ 3_2\ 4_1\}$ $\{2_0\ 3_0\ 4_1 \mid 4_0\ 0_2\ 1_2\}\{0_0\ 0_1\ 0_2 \mid 1_2\ 2_2\ 4_2\}\{\infty\ 3_0\ 4_0 \mid 0_0\ 3_1\ 4_2\}$ $\{\infty\ 2_1\ 4_2 \mid 0_0\ 3_1\ 1_2\}\{\infty\ 3_1\ 1_2 \mid 0_0\ 1_1\ 3_2\}$ mod 5
36. $(16, 30, 120, 15, 8, 2)$	$\{\infty\ 0 \mid 3\ 14 \mid 1\ 4 \mid 9\ 7\}\{2\ 8 \mid 6\ 13 \mid 5\ 10 \mid 11\ 12\}$ mod 15
37. $(16, 30, 60, 15, 8, 4)$	$\{0\ 1\ 3\ 7 \mid 4\ 9\ 14\ \infty\}\{2\ 10\ 11\ 13 \mid 5\ 6\ 8\ 12\}$ mod 15
38. $(16, 24, 120, 15, 10, 2)$	$\{\infty_1 0_1 \mid \infty_2 0_2 \mid 1_2 1_3 \mid 2_2 2_4 \mid 2_3 1_4\}\{\infty_2 0_3 \mid \infty_3 0_2 \mid 1_1 2_4 \mid 2_1 2_3 \mid 1_3 1_4\}$ $\{\infty_1\ 0_3 \mid \infty_3\ 0_1 \mid 1_1\ 2_2 \mid 2_1\ 1_4 \mid 1_2\ 2_4\}\{\infty_2\ 2_4 \mid \infty_3\ 2_3 \mid \infty_4\ 0_2 \mid 0_1\ 2_2 \mid 1_1\ 1_2\}$ $\{\infty_1\ 0_2 \mid \infty_3\ 2_4 \mid \infty_4\ 0_3 \mid 2_1\ 1_3 \mid 1_2\ 2_3\}\{\infty_1\ 2_4 \mid \infty_2\ 1_1 \mid \infty_4\ 0_1 \mid 2_1\ 0_3 \mid 2_2\ 1_3\}$ $\{\infty_4\ 0_4 \mid 1_1\ 2_1 \mid 1_2\ 2_2 \mid 1_3\ 2_3 \mid 1_4\ 2_4\}$ mod 3, with $\{\infty_1\ \infty_2 \mid \infty_3\ \infty_4 \mid 2_1\ 2_4 \mid 2_2\ 1_4 \mid 2_3\ 0_4\}$ $\{\infty_1\ \infty_3 \mid \infty_2\ \infty_4 \mid$ $0_1\ 0_4 \mid 0_2\ 2_4 \mid 0_3\ 1_4\}\{\infty_1\ \infty_4 \mid \infty_2\ \infty_3 \mid 1_1\ 1_4 \mid 1_2\ 0_4 \mid 1_3\ 2_4\}$
39. $(16, 24, 48, 15, 10, 5)$	See Example 36.2
40. $(16, 20, 120, 15, 12, 2)$	$\{1\ 2 \mid 4\ 8 \mid 6\ 13 \mid 7\ 9 \mid 0\ 5 \mid 10\ \infty\}\{6\ 7 \mid 9\ 13 \mid 11\ 3 \mid 12\ 14 \mid 5\ 10 \mid 0\ \infty\}$ $\{11\ 12 \mid 14\ 3 \mid 1\ 8 \mid 2\ 4 \mid 10\ 0 \mid 5\ \infty\}$ $\{1\ 4 \mid 6\ 9 \mid 11\ 14 \mid 2\ 8 \mid 7\ 13 \mid 12\ 3\}$ PC(5), mod 15
41. $(16, 20, 80, 15, 12, 3)$	$\{0\ 1\ 5 \mid 2\ 8\ 10 \mid 6\ 7\ 9 \mid 13\ 4\ \infty\}\{5\ 6\ 10 \mid 7\ 13\ 0 \mid 11\ 12\ 14 \mid 3\ 9\ \infty\}$ $\{10\ 11\ 0 \mid 12\ 3\ 5 \mid 1\ 2\ 4 \mid 8\ 14\ \infty\}$ $\{2\ 7\ 12 \mid 1\ 4\ 8 \mid 6\ 9\ 13 \mid 3\ 11\ 14\}$ PC(5), mod 15
42. $\{16, 20, 60, 15, 12, 4)$	$[\{1\ 2\ 4\ 8 \mid 6\ 7\ 9\ 13 \mid 0\ 5\ 10\ \infty\}\{6\ 7\ 9\ 13 \mid 11\ 12\ 14\ 3 \mid 5\ 10\ 0\ \infty\}$ $\{11\ 12\ 14\ 3 \mid 1\ 2\ 4\ 8 \mid 10\ 0\ 5\ \infty\}$ $\{1\ 2\ 4\ 8 \mid 6\ 7\ 9\ 13 \mid 11\ 12\ 14\ 3\}]$ PC(5), mod 15

$(v, b_1, b_2, r, k_1, k_2)$	Blocks
43. $(16, 20, 40, 15, 12, 6)$	{0 5 1 4 7 13 | 2 6 8 10 9 ∞}{5 10 6 9 12 3 | 7 11 13 0 14 ∞} {10 0 11 14 2 8 | 12 1 3 5 4 ∞} {1 9 6 14 11 4 | 8 7 13 12 3 2} PC(5), mod 15
44. $(16, 16, 80, 15, 15, 3)$	{1 5 8 | 2 10 12 | 3 4 7 | 6 11 13 | 9 14 15} mod 16
45. $(16, 16, 48, 15, 15, 5)$	{3 14 10 2 1 | 12 5 8 6 11 | 9 15 4 7 13} mod 16

36.6 An NBIBD is *resolvable* if the superblock component design $(V, \mathcal{D}_1)$ is resolvable. An NBIBD is *near-resolvable* if the superblock component design $(V, \mathcal{D}_1)$ is near-resolvable and $k_1 < v - 1$.

36.7 Remarks Table 36.5 contains resolvable and near-resolvable NBIBDs whenever the necessary conditions for those designs are met. In Table 36.5, the following NBIBDs are resolvable: 4, 16, 17, 18, 33, 36, 37, and the following NBIBDs are near-resolvable: 5, 20, 21, 22.

36.3 Relationships between NBIBDs and Other Designs

36.8 Remark An NBIBD with $k_1 = v - 1$ is a near-resolvable BIBD.

36.9 Remarks A whist tournament design $\mathrm{Wh}(4n)$ is a $\mathrm{NBIBD}(4n, n(4n-1), 2n(4n-1), 4n-1, 4, 2)$ that is resolvable (see §VI.64). A whist tournament design $\mathrm{Wh}(4n+1)$ is (for $n > 1$) a near-resolvable $\mathrm{NBIBD}(4n+1, n(4n+1), 2n(4n+1), 4n, 4, 2)$. Any NBIBD with $k_1 = 2k_2 = 4$ is a *balanced doubles schedule* [1068].

36.10 Remarks Resolvable and near-resolvable NBIBDs are also known as *generalized whist tournaments* ([37]). A *pitch tournament design* is (for $v > 9$) a resolvable or near-resolvable $\mathrm{NBIBD}(v, v(v-1)/8, v(v-1)/4, v-1, 8, 4)$.

36.11 Remarks Table 36.5 contains these designs:

1. Near-resolvable BIBDs: 1, 2, 3, 8, 9, 12, 14, 15, 23, 24, 25, 26, 31, 32, 44, 45.
2. Whist tournaments: 1, 4, 5, 16, 20, 33.
3. Other balanced doubles schedules: 13, 19
4. Pitch tournaments: 9, 37.

36.12 Remark A partition of the rows of a perpendicular array $\mathrm{PA}_\lambda(t, k_1, v)$ into $\frac{k_1}{k_2}$ sets of size k_2 is a $\mathrm{NBIBD}(v, \lambda\binom{v}{t}, \lambda\binom{v}{t}k_1/k_2, \lambda\binom{v}{t}k_1/v, k_1, k_2)$.

36.4 General Nesting and Other Nested Designs

36.13 Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be two collections of equi-sized multisets (blocks) of elements from the same v-set $\mathcal{V}$. If there is a partition of each of the b_1 blocks of $\mathcal{D}_1$ into blocks of size k_2, so that the resulting collection of $b_2 = b_1 k_1/k_2$ blocks is $\mathcal{D}_2$, then the blocks of $\mathcal{D}_2$ are *sub-blocks* of the blocks of $\mathcal{D}_1$ and the system $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2)$ is a *nested block design*.

36.14 Remarks This definition of nested block design provides a general framework for the nesting concept. Excluded, among others, are notions of nesting for which sub-blocks do not fully partition blocks [1480].

36.15 Remark A resolvable BIBD (RBIBD) $(V, \mathcal{D})$ is a nested block design $(V, \mathcal{D}_1, \mathcal{D}_2)$ where the blocks of $\mathcal{D}_1$, of size $k_1 = v$, are the resolution classes of $\mathcal{D}$, and $\mathcal{D}_2 = \mathcal{D}$.

36.16 Remark Nested block designs may have more than two blocking systems and consequently more than one level of nesting. A doubly nested block design is a system

$(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ where both $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2)$ and $(\mathcal{V}, \mathcal{D}_2, \mathcal{D}_3)$ are nested block designs. This may be extended in a natural fashion.

36.17 A multiply nested BIBD (MNBIBD) is a nested block design $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_s)$ with parameters $(v, b_1, \ldots, b_s, r, k_1, \ldots, k_s)$ for which the systems $(\mathcal{V}, \mathcal{D}_j, \mathcal{D}_{j+1})$ are NBIBDs for $j = 1, \ldots, s-1$.

36.18 Remarks A resolvable NBIBD is a doubly nested block design. A near-resolvable NBIBD$(v, b_1, b_2, r, k_1, k_2)$ is a MNBIBD$(v, b_1k_1/(v-1), b_1, b_2, r, v-1, k_1, k_2)$.

36.19 Example (1 16, 13 4|9 8, 15 2||3 14, 5 12|10 7, 11 6) mod 17 is an initial block for a triply nested BIBD $(17, 17, 34, 68, 136, 17, 16, 8, 4, 2)$.

36.20 Remark For $v \le 20$ and $r \le 30$, there are 29 sets of parameters meeting the necessary conditions for existence of a doubly nested BIBD. Designs are known for all of these except $(v, b_1, b_2, b_3, r, k_1, k_2, k_3) = (16, 20, 40, 80, 15, 12, 6, 3)$ [1765].

36.21 Construction Let $\mathcal{M}_1$ be an MNBIBD $(\overline{v}, \overline{b}_1, \overline{b}_2, \ldots, \overline{b}_s, \overline{r}, \overline{k}_1, \overline{k}_2, \ldots, \overline{k}_s)$ with $s \ge 1$ component designs (if $s = 1$ then $\mathcal{M}_1$ is a BIBD; if $s = 2$ then an NBIBD; and if $s > 2$ then an MNBIBD). Let $\mathcal{M}_2$ be an MNBIBD $(\widehat{v}, \widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_t, \widehat{r}, \widehat{k}_1, \widehat{k}_2, \ldots, \widehat{k}_t)$ with $t \ge 2$ component designs, and with $\widehat{k}_1/\widehat{k}_q = \overline{v}$ for some $2 \le q \le t$. Select one block of size $\widehat{k}_1$ from $\mathcal{M}_2$ and label its sub-blocks of size $\widehat{k}_q$ with the symbols $1, 2, \ldots, \overline{v}$, which are the treatment symbols of $\mathcal{M}_1$. Now replace each symbol in $\mathcal{M}_1$ by the correspondingly labeled sub-block of the selected block from $\mathcal{M}_2$. Each large block of the so modified $\mathcal{M}_1$ is now of size $k_1 = \overline{k}_1\widehat{k}_q$ and contains successively nested blocks of sizes $k_2, k_3, \ldots, k_{s+t-q+1}$ where $k_j = \overline{k}_j\widehat{k}_q$ for $j = 1, \ldots, s$ and $k_j = \widehat{k}_{q+j-s-1}$ for $j = s+1, \ldots, s+t-q+1$. Repeat this process $\widehat{b}_1$ times, using a new copy of $\mathcal{M}_1$ for each of the $\widehat{b}_1$ blocks of $\mathcal{M}_2$. The resulting design $\mathcal{M}$ is an MNBIBD $(v, b_1, b_2, \ldots, b_{s+t-q+1}, r, k_1, k_2, \ldots, k_{s+t-q+1})$ with $v = \widehat{v}$, $r = \overline{r}\widehat{r}$, block sizes k_j as specified, and $b_j = \overline{b}_j\widehat{b}_1$ for $j \le s$, and $b_j = \overline{k}_s\overline{b}_s\widehat{b}_1\widehat{k}_q/\widehat{k}_{q+j-s-1}$ for $j > s$.

36.22 Theorem Let v be a prime power of the form $v = a_0a_1a_2\cdots a_n+1$ ($a_0 \ge 1$, $a_n \ge 1$ and $a_i \ge 2$ for $1 \le i \le n-1$ are integers). Then there is an MNBIBD with n component designs having $k_1 = ua_1a_2\cdots a_n$, $k_2 = ua_2a_3\cdots a_n$, $\ldots$, $k_n = ua_n$, and with a_0v blocks of size k_1, for any integer u with $1 \le u \le a_0$ and $u > 1$ if $a_n = 1$. If integer $t \ge 2$ is chosen so that $2 \le tu \le a_0$, then there is an MNBIBD with $n+1$ component designs, with the same number of big blocks but of size $k_0 = tk_1$, and with its n other block sizes being $k_1, \ldots, k_n$ as given.

36.23 Theorem With the conditions of Theorem 36.22, if a_0 is even and a_i is odd for $i \ge 1$, then MNBIBDs can be constructed with the same block sizes but with $a_0v/2$ blocks of size k_1.

36.24 Remarks NBIBD constructions arise as special cases of Construction 36.21 and Theorems 36.22 and 36.23. An example for Construction 36.21 is $s = 1$, $t = 2$. With mild abuse of terminology, Construction 36.21 also works if either $\mathcal{M}_1$ or $\mathcal{M}_2$ is taken as a RBIBD, for instance $s = 1$, $t = 2$ and $\hat{v} = \hat{k}_1$ so that $\mathcal{M}_2$ is RBIBD and $\mathcal{M}$ is NBIBD.

36.25 A *nested row-column design* is a system $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ for which (1) each of $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2)$ and $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_3)$ is a nested block design, (2) each block of $\mathcal{D}_1$ may be displayed as a $k_2 \times k_3$ row-column array, one member of the block at each position in the array, so that the columns are the $\mathcal{D}_2$ sub-blocks in that block, and the rows are the $\mathcal{D}_3$ sub-blocks in that block.

36.26 A (completely balanced) *balanced incomplete block design with nested rows and columns*, BIBRC(v, b_1, k_2, k_3), is a nested row-column design $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ for which each of $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2)$ and $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_3)$ is a NBIBD.

36.27 Example A BIBRC for five symbols in ten 2×2 nesting blocks.

1	2	2	3	3	4	4	5	5	1	1	3	2	4	3	5	4	1	5	2
3	4	4	5	5	1	1	2	2	3	2	4	3	5	4	1	5	2	1	3

36.28 Example A BIBRC for ten symbols in thirty 2×3 nesting blocks. Initial blocks (mod 10) are

1	2	4	1	2	7	1	2	4
5	6	9	3	5	8	3	9	5

36.29 Remark If $k_2 = k_3$, then a nested row-column design is a BIBRC if $(\mathcal{V}, \mathcal{D}_1)$ and $(\mathcal{V}, \mathcal{D}_2 \cup \mathcal{D}_3)$ are BIBDs, loosening the complete balance requirement that $(\mathcal{V}, \mathcal{D}_2)$ and $(\mathcal{V}, \mathcal{D}_3)$ are individually BIBDs. An example is the first five blocks of Example 36.27. Further relaxations are explained in [1636].

36.30 Theorem If $v = mpq+1$ is a prime power and p and q are relatively prime, then initial nesting blocks for a BIBRC(v, mv, sp, tq) are $A_l = x^{l-1}L \otimes M$ for $l = 1, \ldots, m$, where $L_{s\times t} = (x^{i+j-2})_{i,j}$, $M_{p\times q} = (x^{[(i-1)q+(j-1)p]m})_{i,j}$, s and t are integers with $st \le m$, and x is a primitive element of $\mathbb{F}_v$. If m is even and pq is odd, then $A_1, \ldots, A_{m/2}$ are intial nesting blocks for BIBRC$(v, mv/2, sp, tq)$

36.31 Theorem Write $x^{u_i} = 1 - x^{2mi}$ where x is a primitive element of $\mathbb{F}_v$ and $v = 4tm+1$ is a prime power. Let A be the addition table with row margin $(x^0, x^{2m}, \ldots, x^{(4t-2)m})$ and column margin $(x^m, x^{3m}, \ldots, x^{(4t-1)m})$, and set $A_l = x^{l-1}A$. If $u_i - u_j \not\equiv m \pmod{2m}$ for $i, j = 1, \ldots, t$, then $A_1, \ldots, A_m$ are initial nesting blocks for BIBRC$(v, mv, 2t, 2t)$. Including 0 in each margin for A, if further $u_i \not\equiv m \pmod{2m}$ for $i = 1, \ldots, t$, then $A_1, \ldots, A_m$ are initial nesting blocks for BIBRC$(v, mv, 2t+1, 2t+1)$.

36.32 A *bottom-stratum universally optimal nested row-column design*, BNRC(v, b_1, k_2, k_3), is a nested row-column design $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ for which (1) $(\mathcal{V}, \mathcal{D}_2)$ is a BIBD or, more generally, a BBD, and (2) the $\mathcal{D}_3$ sub-blocks within any block of $\mathcal{D}_1$ are identical as multi-sets.

36.33 Example A BNRC with 4 symbols in nesting blocks of size 2×4.

1	1	2	2	3	3	4	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
2	2	1	1	4	4	3	3	3	4	2	1	3	4	2	1	3	4	2	1	3	4	2	1	3	4	2	1	3	4	2	1

36.34 Theorem The existence of BNRC(v, b_1, k_2, k_{31}) and BNRC(v, b_1, k_2, k_{32}) implies existence of BNRC$(v, b_1, k_2, k_{31} + k_{32})$. The existence of BNRC$(v, b_1, k_2, k_3)$ for which b_1 is a multiple of s implies existence of BNRC$(v, b_1/s, k_2, sk_3)$. The column-wise juxtaposition of the nesting blocks of a BNRC into a $k_2 \times b_1 k_3$ array is a row-regular generalized Youden design (see §VI.65.6).

36.35 Theorem If $v = mq + 1$ is a prime power and $2 \le p \le q$, initial nesting blocks for a BNRC(v, mv, p, q) are $A_l = (x^{(i+j-2)m+l-1})_{ij}$ for $l = 1, \ldots, m$ and x a primitive element of $\mathbb{F}_v$. If m is even and q is odd, $A_1, \ldots, A_{m/2}$ generate BIBRC$(v, mv/2, p, q)$.

36.36 Remarks

1. BIBRCs and BNRCs are statistically optimal for competing models ([1636]).
2. The necessary conditions for existence of these designs are those of the component BIBDs. The necessary conditions are sufficient for $k_1 = 4$ ([135],[1952]).
3. Most work on BIBRCs and BNRCs has concentrated on constructing infinite series, often employing starter blocks and the finite fields ([1110],[1636],[135]) as illustrated in 36.30, 36.31, and 36.35.

See Also

§II.7	General treatment of resolvable and near-resolvable BIBDs.
§VI.38	Perpendicular arrays can be arranged into MNBIBDs and BIBRCs.
§VI.51	Various tournament designs, some of which are NBIBDs.
§VI.64	Many constructions for NBIBDs that are Whist tournaments.
§VI.65.6	Details on BBDs and Generalized Youden designs.
[1638]	Survey of NBIBDs, contains much of the information given here.
[1636]	Nested designs survey, includes NBIBDs, BIBRCs, and BNRCs.
[1637]	Exploration of nesting, crossing, and other relationships for blocking systems from an optimality perspective, with constructions.
[37]	Construction of resolvable and near-resolvable NBIBDs.
[1921, 998]	Uses of NBIBDs in constructing other combinatorial designs.

References Cited: [37, 135, 998, 1068, 1109, 1110, 1480, 1636, 1637, 1638, 1765, 1921, 1952]

37 Optimality and Efficiency: Comparing Block Designs

Deborah J. Street

37.1 Remark Often several essentially different designs of the same size can be found. Is there any sensible way to decide which design is to be preferred for various statistical applications? Resolvability is often a desirable feature, as it means that one or more resolution classes may be processed or harvested at a time and allowance made for this in the analysis. Another useful criterion is how well treatment differences are estimated. One reasonable measure of good estimation is small variance. Ways to compare designs based on this idea include the pairwise efficiency factors of the design and the optimality of the design.

37.2 Let Y_{ij} be the response observed in block j from treatment i (if treatment i is applied in block j). Write $E(Y_{ij}) = \mu + \tau_i + \beta_j$, where μ is the overall mean, τ_i is the effect of treatment i, and β_j is the effect of block j. This is the *linear model* for the design. One assumes that the variance of each response is a constant, $Var(Y_{ij}) = \sigma^2$, independent of every other response. The aim of the experiment is to estimate the treatment effects. This estimate is denoted by $\widehat{\tau}$. To do this, write the linear model as $E(\mathbf{Y}) = \mathbf{j}\mu + T\tau + B\beta$. Then $T^T B = N$, the $v \times b$ treatment-block incidence matrix. Solving for $\widehat{\tau}$ gives the *reduced normal equations* $A\widehat{\tau} = \mathbf{q}$, where $A = rI - NN^T/k$ is the *information matrix*, $\mathbf{T}$ is the vector of treatment totals, $\mathbf{B}$ is the vector of block totals, and $\mathbf{q} = \mathbf{T} - N\mathbf{B}/k$.

37.3 Remarks

1. The expressions above are correct for any incomplete block design in which all treatments are replicated equally often and all blocks have the same size. Otherwise let R be a diagonal matrix with the treatment replication numbers on the diagonal and let K be a diagonal matrix with the block sizes on the diagonal. Then, in general, $A = R - NK^{-1}N^T$ and $\mathbf{q} = \mathbf{T} - NK^{-1}\mathbf{B}$.
2. A is not of full rank; one requires a generalized inverse of A to get an expression for $\widehat{\tau}$. A *generalized inverse* of A is a matrix G such that $AGA = A$. To calculate G write A in *canonical form* as $A = \sum_i \lambda_i \mathbf{x}_i \mathbf{x}_i^T$, where λ_i is an eigenvalue of A with corresponding eigenvector $\mathbf{x}_i$ and the eigenvectors have been normalized.

Then $G = \sum_i \lambda_i^{-1} \mathbf{x}_i \mathbf{x}_i^T$, where this summation is over the nonzero eigenvalues only. Then $\widehat{\tau} = G\mathbf{q}$ and $Var(\widehat{\tau}) = \sigma^2 G$.

3. For a BIBD, it is possible to evaluate G in general. Since $NN^T = (r-\lambda)I + \lambda J$, by substituting, one obtains $A = \lambda v/k(I - J/v)$. Now $(I - J/v)^2 = (I - J/v)$, so $G = k/\lambda v(I - J/v)$.

37.4 Example Consider a BIBD(7,3,1) with blocks {1,2,4}, {2,3,5}, {3,4,6},{4,5,7},{5,6,1}, {6,7,2}, {7,1,3}. Then $E(Y_{11}) = \mu + \tau_1 + \beta_1$, $E(Y_{21}) = \mu + \tau_2 + \beta_1$, and Y_{31} does not exist as treatment 3 is not applied in block 1.

The matrix T is 21×7 and records which treatment generates each response. The matrix B is 21×7 and records in which block each response is observed. $A = 3I - (2I + J)/3$, $T_1 = Y_{11} + Y_{15} + Y_{17}$, $T_2 = Y_{21} + Y_{22} + Y_{26}$, and so on. $G = 3/7(I - J/7)$ and $\widehat{\tau} = 3/7(I - J/7)(T - NB/3)$.

37.5 A design is *connected* if, for any two treatments, it is possible to find a list of treatments, starting with one and ending with the other, such that adjacent treatments in the list are in the same block.

37.6 Proposition A design is connected if and only if the rank of A is $v - 1$ (see [1205]).

37.7 Remark BIBDs are connected. Group divisible PBIBDs with $\lambda_1 = 0$ (§VI.42.2) are disconnected.

37.8 Blocks are a grouping of the plots into homogeneous subsets. If there is no need to block the plots, then the design is a *completely randomized design*. In a completely randomized design, with each treatment replicated r times, $G = I/r$ so the variance of the estimate of any treatment difference, denoted $Var(\widehat{\tau}_i - \widehat{\tau}_j)$, is $2\sigma^2/r$. The *pairwise efficiency factor* of a connected block design is the ratio of $2\sigma^2/r$ to $Var(\widehat{\tau}_i - \widehat{\tau}_j)$ in the block design. The ratio of $2\sigma^2/r$ to the average variance of the treatment differences in a connected design is the *average efficiency factor*.

37.9 Remark In a BIBD, all estimates of treatment differences have the same variance, which is $2\sigma^2 k/\lambda v$. Thus, each pairwise efficiency factor is $\lambda v/rk$ and, hence, so is the average efficiency factor. This expression depends only on the parameters of the BIBD and not on the particular BIBD.

37.10 Since $Var(\mathbf{x}_i^T \widehat{\tau}) = \mathbf{x}_i^T G \mathbf{x}_i \sigma^2 = \sigma^2 \lambda_i$, the efficiency factor of the contrast $\mathbf{x}_i^T \tau$ is λ_i/r. The values λ_i/r are the *canonical efficiency factors* of the design with information matrix A. The *efficiency factor* of the design is the harmonic mean of the canonical efficiency factors.

37.11 Remarks

1. For a BIBD, the canonical efficiency factors are $\lambda v/kr$.
2. See [1190] for bounds on the efficiency factors of various designs.
3. The tables by Clatworthy [513] give the efficiency factors for the various PBIBDs that are tabulated.

37.12 Consider a set of possible block designs for v treatments, all with block size k. A design in the set is *A-optimal* if it has minimum trace $\mathrm{tr}(G)$, *D-optimal* if it has minimum determinant $\det(G)$, and *E-optimal* if the maximum eigenvalue of G is a minimum. *(M,S)-optimality* is a two-stage criterion based on the idea that the canonical efficiency factors should be as equal as possible. At the first stage, a class of designs that maximizes $\sum_i \lambda_i/r$ is formed. At the second stage, the design, or designs, within this class that minimize $\sum_i (\lambda_i/r)^2$ are obtained. These designs are the (M,S)-optimal designs.

37.13 Remarks

1. When the canonical efficiency factors are all equal, then the design is optimal under all four criteria. Hence, BIBDs are A-, D-, E- and (M,S)-optimal.
2. Other alphabetic optimality criteria have been discussed and the idea of universal optimality, which encompasses many of the alphabetic criteria, was introduced by Kiefer [1297].
3. Sometimes the treatments to be compared are of two types: the standard treatments and the test treatments. Comparisons between standard and test treatments are of the most interest. Optimal designs for this situation are given in [1180].
4. In many situations combinatorial designs do not exist. In such cases, designs with good estimation properties are obtained by computer search. Gosset [1058] has constructed designs for a wide-range of models and optimality criteria.
5. Row-column designs, which are extensions of latin squares and include generalized Youden designs (§VI.65.6), have optimality values associated with them. See [1205] for a discussion. Bounds for the values are given in [1204]. Some of the PBIBDs tabulated in [513] can be written as Youden designs and are so written in the tabulation when this is possible.
6. On occasion some row-column combinations may not be possible. Then the rows and columns have a *nonorthogonal structure* and the question arises as to the optimal structure for such designs. Shah and Sinha [1887] have developed some designs that balance the occurrence of each of the treatments as far as possible in both rows and columns; this is often referred to as *combinatorial balance*. Kunert [1367] has shown that these conditions are more restrictive than necessary and has developed some conditions for optimal designs based on the A matrix.

See Also

§IV.42	PBIBDs.
§VI.65.6	Generalized Youden designs.
[489]	Discusses the optimality of some PBIBDs.
[1075]	A discussion of approximations to BIBDs, with particular reference to parameters (22,8,4), for which a BIBD is unknown.
[1058]	Gives an algorithm for optimal response surface designs.
[1523, 1987]	Gives designs optimal for general dependence structures, including change-over designs
[1675]	Discusses exchange algorithms for constructing D-optimal designs.
[1886]	A good general introduction.
[1923]	Optimal designs when the responses are binary.
[2035]	An interchange algorithm to find optimal block designs.
[2098]	Contains a simulated annealing algorithm for optimal block designs.

References Cited: [489, 513, 1058, 1075, 1180, 1190, 1204, 1205, 1297, 1367, 1523, 1675, 1886, 1887, 1923, 1987, 2035, 2098]

38 Ordered Designs, Perpendicular Arrays, and Permutation Sets

Jürgen Bierbrauer

38.1 Definitions, Examples, and Constructions

38.1 An *ordered design* $\mathrm{OD}_\lambda(t,k,v)$ is a $k \times \lambda \cdot \binom{v}{t} \cdot t!$ array with v entries such that
1. each column has k distinct entries, and
2. each tuple of t rows contains each column tuple of t distinct entries precisely λ times.

38.2 A *perpendicular array* $\mathrm{PA}_\lambda(t,k,v)$ is a $k \times \lambda \cdot \binom{v}{t}$ array with v entries such that
1. each column has k distinct entries, and
2. each set of t rows contains each set of t distinct entries as a column precisely λ times.

38.3 **Remark** Often, ordered designs and perpendicular arrays are defined using the transpose of the definitions given.

38.4 For $0 \le s \le t$, a $\mathrm{PA}_\lambda(t,k,v)$ is an s-$\mathrm{PA}_\lambda(t,k,v)$ if, for each $w \le t$ and $u \le \min(s,w)$, the following holds: Let E_1, E_2 be disjoint sets of entries, $E_1 \cap E_2 = \emptyset$ with $|E_1| = u$ and $|E_2| = w-u$. Then the number of columns containing $E_1 \cup E_2$ and having E_2 in a given set U of $w-u$ rows is a constant, independent of the choice of E_1, E_2, and U. 1-PA are *authentication perpendicular arrays* (APA).

38.5 **Example** An $\mathrm{OD}_1(2,3,6)$ (equivalent to an idempotent latin square of order 6).

1	1	1	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5	6	6	6	6	6
2	3	4	5	6	1	3	4	5	6	1	2	4	5	6	1	2	3	5	6	1	2	3	4	6	1	2	3	4	5
3	5	2	6	4	3	1	6	4	5	4	6	5	1	2	2	5	6	3	1	6	4	2	1	3	5	1	4	3	2

38.6 **Example** A 3-$\mathrm{PA}_3(3,4,6)$ (at the same time $\mathrm{APA}_4(4,4,6)$) in compact form.

∞	∞	0	0	0	0	0	0	0	0	0	0	The 60 columns of the full 3-$\mathrm{PA}_3(3,4,6)$
0	0	∞	∞	4	2	4	2	1	4	3	2	are the images of the columns to the left
4	3	1	3	∞	∞	1	3	2	3	1	4	under the group generated by the permu-
2	4	2	1	3	4	∞	∞	3	2	4	1	tation $(\infty)(0\,1\,2\,3\,4)$ on the entries.

38.7 **Example** An APA(2,3,11) is given in Example V.52.43.

38.8 **Remark** OD and PA may be viewed as (multi-)sets of injective mappings from a k-set into a v-set by identifying them with the (multi-)set of their columns and interpreting each column as a mapping from the set of rows to the set of entries.

38.9 **Theorem** An $\mathrm{OD}_\lambda(2,k,v)$, $k \le v$, exists if and only if an idempotent $\mathrm{OA}_\lambda(2,k,v)$ exists. See §III.3 and §III.6.

38.10 **Theorem** [260]
1. If there is a t-wise balanced design t-(v,K,λ) and for every $\ell \in K$ an s-$\mathrm{PA}_\mu(t,k,\ell)$ exists, then an s-$\mathrm{PA}_{\lambda\cdot\mu}(t,k,v)$ exists.

2. If there is an $\mathrm{OD}_\lambda(t,k,v)$ and an $\mathrm{OD}_\mu(y,\ell,v-k)$, where $y=\min(\ell,t)$, then an $\mathrm{OD}_{\lambda\cdot\mu\cdot\binom{v-k}{y}\cdot y!}(t,k+\ell,v)$ exists.
3. If there is an s-$\mathrm{PA}_\lambda(t,k,v)$ and an x-$\mathrm{PA}_\mu(y,\ell,v-k)$, where $x=\min(\ell,s), y=\min(\ell,t)$, then an s-$\mathrm{PA}_{\lambda\cdot\mu\cdot\binom{v-k}{y}}(t,k+\ell,v)$ exists.
4. If an $\mathrm{OD}_\lambda(t,u,k)$, an $\mathrm{OD}_\nu(y,\ell,v-k)$, and a t-(v,k,μ) design exist, where $y=\min(\ell,t)$, then an $\mathrm{OD}_{\lambda\cdot\mu\cdot\nu\cdot\binom{v-k}{y}\cdot y!}(t,u+\ell,v)$ exists.
5. If an s-$\mathrm{PA}_\lambda(t,u,k)$, an x-$\mathrm{PA}_\nu(y,\ell,v-k)$, and a t-(v,k,μ) design exist, where $x=\min(\ell,s), y=\min(\ell,t)$, then an s-$\mathrm{PA}_{\lambda\cdot\mu\cdot\nu\cdot\binom{v-k}{y}}(t,u+\ell,v)$ exists.

38.2 Permutation Sets

38.11 A set $S\subseteq S_n$ of permutations is (uniformly) *t-homogeneous* if it is an $\mathrm{APA}_\lambda(t,n,n)$; it is *$t$-transitive* if it is an $\mathrm{OD}_\lambda(t,n,n)$.

38.12 Remark The notions of 0-$\mathrm{PA}_\lambda(t,n,n)$, $\mathrm{APA}_\lambda(t,n,n),\ldots,t$-$\mathrm{PA}_\lambda(t,n,n)$ all coincide.

38.13 Theorem Permutation *groups* yield special cases of t-transitive or t-homogeneous sets.

1. The groups $\mathrm{PGL}_2(q), q$ a prime power, form $\mathrm{OD}_1(3,q+1,q+1)$; the groups $\mathrm{PSL}_2(q), q\equiv 3 \pmod 4$ are $\mathrm{APA}_3(3,q+1,q+1)$. The special cases of this last family when the prime power $q\equiv 3,11 \pmod{12}$ form the only known infinite family of $\mathrm{APA}_\lambda(t,n,n)$ with $t>2$ and minimal λ.
2. The groups $\mathrm{AGL}_1(q)$, (q a prime power), of order $q\cdot(q-1)$ form an $\mathrm{OD}_1(2,q,q)$; the groups $\mathrm{ASL}_1(q)$, (q a prime power $\equiv 3 \pmod 4$) of order $q\cdot(q-1)/2$ form $\mathrm{APA}_1(2,q,q)$.
3. $\mathrm{AGL}_1(8)$ is an $\mathrm{APA}_1(3,8,8)$, $\mathrm{PSL}_2(8)$ is an $\mathrm{APA}_4(4,9,9)$, $A\Gamma L_2(32)$ is an $\mathrm{APA}_1(3,32,32)$, $\mathrm{P\Gamma L}_2(32)$ is an $\mathrm{APA}_4(4,33,33)$, and the alternating group A_7 in its doubly transitive action on 15 points is an $\mathrm{OD}_{12}(2,15,15)$. The Mathieu groups yield $\mathrm{OD}_1(4,11,11)$, $\mathrm{OD}_1(5,12,12)$, $\mathrm{OD}_{48}(3,22,22)$, $\mathrm{OD}_{48}(4,23,23)$, and $\mathrm{OD}_{48}(5,24,24)$.
4. The groups of Lie rank 1 are 2-transitive. The following are some small examples. The Ree groups ${}^2G_2(3)=\mathrm{P\Gamma L}_2(8)$ and ${}^2G_2(27)$ in their action on the Ree unitals are $\mathrm{OD}_2(2,28,28)$ and $\mathrm{OD}_{26}(2,19684,19684)$, respectively. The unitary group $U_3(5)=\mathrm{PSU}_3(5^2)$ is an $\mathrm{OD}_8(2,126,126)$, the Suzuki group $Sz(8)={}^2B_2(8)$ in its action on the Tits ovoid is an $\mathrm{OD}_7(2,65,65)$.

38.14 Remark See §VII.9 for further discussion of the groups mentioned in Theorem 38.13.

38.15 Theorem [2159] An $OD_1(2,n,n)$ is equivalent to a projective plane of order n.

38.16 Theorem [251] A conjugacy class of elements of S_n is t-homogeneous, $2t\le n+1$ if and only if the underlying partition π of the number n satisfies: each $i\le t$ can be written as a sum of parts of π in exactly one way.

38.17 Example The permutations of type $(1,2,\ldots,2^i)$ in S_n, where $n=2^{i+1}-1$, form a t-homogeneous set for all $t\le n$.

38.18 Example Special cases of the recursive constructions show that $\mathrm{APA}_\lambda(t,n,n)$ implies $\mathrm{APA}_{\lambda(n+1-t)}(t,n+1,n+1)$ (due to Tran van Trung, 1991) and $\mathrm{OD}_\lambda(t,n,n)$ implies $\mathrm{OD}_{\lambda(n+1-t)}(t,n+1,n+1)$. An application to M_{12} yields $\mathrm{OD}_8(5,13,13)$. This is Conway's M_{13} [597].

38.19 Theorem A method due to O'Nan [1700] based on group characters is used in [254] to show that the only 3-homogeneous proper subsets of $PGL_2(q)$ in its action on the projective line are $\mathrm{APA}_3(3, q+1, q+1)$ for $q \equiv 3 \pmod 4$ and for $q \in \{5, 8\}$.

38.20 Theorem [265, 261] $PSL_2(q)$ in its action on the projective line possesses a 2-homogeneous subset of half its size if and only if either q is a power of 2 or $q \equiv 1 \pmod 4$.

38.21 Theorem [266, 259] The following exist: $\mathrm{APA}_2(2, 6, 6) \subset PSL_2(5)$, $\mathrm{APA}_2(2, 10, 10) \subset S_6$, $\mathrm{APA}_2(2, 12, 12)$, $\mathrm{APA}_3(3, 7, 7)$, $\mathrm{APA}_4(4, 8, 8)$, and $\mathrm{APA}_4(3, 11, 11) \subset M_{11}$.

38.22 Remark See Table 38.33 for information on small t-homogeneous permutation sets.

38.3 Existence

38.23 Remark Deleting ℓ rows, $(t \le k - \ell)$, of an $\mathrm{OD}_\lambda(t, k, v)$ or $\mathrm{PA}_\lambda(t, k, v)$ results in an $\mathrm{OD}_\lambda(t, k-\ell, v)$ ($\mathrm{PA}_\lambda(t, k-\ell, v)$, respectively). The corresponding statement for s-$\mathrm{PA}_\lambda(t, k, v)$ is not true.

38.24 Remark Let $q \equiv 3 \pmod 4$ be a prime power, k odd. An $\mathrm{APAV}(q, k)$ (V stands for *vector*) is a tuple $(x_1, \ldots, x_k)$ where $x_i \in GF(q)$ and such that for each i the $x_i - x_j, j \neq i$ are evenly distributed on squares and nonsquares [886]. An $\mathrm{APAV}(q, k)$ implies the existence of $\mathrm{APA}_1(2, k, q)$. In [483] a theorem on character sums based on the Hasse–Weil inequality is used to prove existence of $\mathrm{APAV}(q, k)$ when q is large enough with respect to k.

38.25 Theorem [483] The following exist, for q prime power $\equiv 3 \pmod 4$,

1. $\mathrm{APAV}(q, 7)$ for $q \ge 7, q \neq 11, 19$,
2. $\mathrm{APAV}(q, 9)$ for $q \ge 19$,
3. $\mathrm{APAV}(q, 11)$ for $q \ge 11, q \neq 19, 27$,
4. $\mathrm{APAV}(q, 13)$ for $q \ge 13, q \neq 19, 23, 31$, and
5. $\mathrm{APAV}(q, 15)$ for $q \ge 31$.

Recall that the corresponding $\mathrm{APA}_1(2, k, q)$ exist as well.

38.26 Theorem The following exist, and λ is minimal in all cases:

1. $\mathrm{OD}_1(t, t, v), v \ge t$ (trivially).
2. $\mathrm{APA}_1(1, k, v), k \le v$ [1968].
3. $\mathrm{APA}_1(1, 1, v)$, $APA_2(2, 2, v)$, $APA_3(3, 3, v)$ for all v [260].
4. $\mathrm{APA}_2(2, q, q), q$ power of 2 [1776].
5. $\mathrm{APA}_1(2, q, q), q$ odd prime power [1776].
6. $\mathrm{APA}_1(2, 3, v), v \ge 7$ odd. There is no $\mathrm{APA}_1(2, 3, 5)$ [1968].
7. $\mathrm{OD}_1(2, 3, v), v \ge 3$ (equivalently: an idempotent latin square of order v).
8. $\mathrm{PA}_1(2, 4, v), v \ge 5$ odd [1654, 1459].
9. $\mathrm{APA}_2(2, 4, v), v \ge 4$ [1654].
10. $\mathrm{PA}_1(2, 5, v), v \ge 5$ odd,$v \neq 39$ [1654, 1459].
11. $\mathrm{APA}_1(2, 5, v), v \ge 5$ odd, with possible exceptions $v \in \{9, 13, 15, 17, 33, 39, 49, 57, 63, 69, 87, 97, 113\}$ [483].
12. $\mathrm{APA}_1(2, k, q), q \equiv 3 \pmod 4$ prime power, k odd, $q > 2^{k(k-1)}$ [260].
13. $\mathrm{APA}_1(2, k, q), q$ odd prime power, k odd, $k \mid q - 1$ [951].
14. $\mathrm{APA}_1(2, p^m, p^n), p$ odd prime, $m \le n$ [260].
15. $\mathrm{PA}_1(3, 4, v), v \equiv 1, 2 \pmod 3$ [1344].
16. $\mathrm{PA}_3(3, 4, v), v \equiv 0 \pmod 3$ [1344].
17. $\mathrm{OD}_1(3, 4, v), v \ge 4, v \neq 7$. There is no $\mathrm{OD}_1(3, 4, 7)$ [2016].
18. 3-$\mathrm{PA}_3(3, 4, v), v$ even, $v \ge 4$ (minimal even as APA) [260].
19. 3-$\mathrm{PA}_6(3, 4, v), v$ odd, $v \ge 5, v \neq 7$ (minimal even as APA) [260].

38.27 Theorem [260] $\mathrm{APA}_2(2, k, q)$ exist for every prime power q and $2 \le k \le q$. Here λ is minimal if kq is even.

38.28 Theorem [260] $\mathrm{APA}_3(3, k, q+1)$ exist for every prime power $q \equiv 3 \pmod 4$ and $k \le q+1$. Here $\lambda = 3$ is minimal unless $q \equiv 7 \pmod{12}$ and $k \equiv 2$ or $5 \pmod 6$.

38.29 Theorem [260] $\mathrm{APA}_{12}(4, 4, v)$ exists for all $v \ge 4$. This is minimal unless $v \equiv 0 \pmod 3$. Restrictions of the group $\mathrm{PGL}_2(8)$ yield $\mathrm{APA}_4(4, k, 9), 4 \le k \le 9$.

38.30 Theorem [2013] If a (class-)regular $\mathrm{OA}_\lambda(t, t+1, v)$ exists, then an $\mathrm{OD}_\lambda(t, t+1, v+t)$ can be constructed. If $v = \prod_i p_i^{a_i}$ is the expression of v as a product of prime powers and $a_i(p_i - 1) > t$ for all i, then a regular $\mathrm{OA}_1(t, t+1, v)$ exists.

38.31 Example As an illustration of Theorem 38.30, a regular $\mathrm{OA}_1(3, 4, 5)$ exists, and hence, an $\mathrm{OD}_1(3, 4, 8)$ exists.

38.32 Remark In Tables 38.33 and 38.34, italicized entries are those that are not known to be minimal.

38.33 Table (a) Smallest λ for which $\mathrm{APA}_\lambda(t, k, k)$ are known to exist and (b) smallest λ for which $\mathrm{APA}_\lambda(2, k, v)$ are known to exist.

(a)

$t\backslash k$	3	4	5	6	7	8	9	10	11	12	13
2	1	2	1	2	1	2	1	2	1	2	1
3	3	3	1	3	3	1	3	*6*	*4*	3	*30*
4		12	2	4	3	4	*4*	*24*	*24*	*192*	*1728*
5			10	10	5	5	*4*	*20*	*120*	*120*	*960*

(b)

$k\backslash v$	5	6	7	8	9	10	11	12	13	14
5	1	2	2	2	*2*	2	1	2	*2*	2
6		2	2	2	2	*8*	2	2	2	*12*
7			1	2	2	*8*	*2*	*10*	*2*	*6*

38.34 Table (a) Smallest λ for which $\mathrm{APA}_\lambda(3, k, v)$ are known to exist and (b) smallest λ for which $\mathrm{APA}_\lambda(4, k, v)$ are known to exist.

(a)

$k\backslash v$	5	6	7	8	9	10	11	12	13	14
5	1	3	*12*	*3*	*6*	3	*4*	3	*15*	*5*
6		3	*12*	3	6	*6*	*24*	3	*30*	*6*
7			3	3	*6*	*6*	*48*	3	*30*	*6*
8				1	6	*6*	*48*	3	*30*	*6*
9					3	*6*	*48*	3	*30*	*6*

(b)

$k\backslash v$	4	5	6	7	8	9	10	11	12
4	12	12	4	12	12	4	12	12	*12*
5		2	4	6	*24*	*4*	*24*	2	*16*
6			4	12	*24*	4	*24*	12	*16*
7				3	12	*4*	*24*	*24*	*96*
8					4	4	*24*	*24*	*192*

38.4 Large Sets

38.35 A *large set* $\mathrm{LOD}_\lambda(t, k, v)$ or $\mathrm{LPA}_\lambda(t, k, v)$ of $\mathrm{OD}_\lambda(t, k, v)$ and $\mathrm{PA}_\lambda(t, k, v)$, respectively, is a partition of the set of all v-ary k-tuples with distinct entries into $\mathrm{OD}_\lambda(t, k, v)$ (respectively, into $\mathrm{PA}_\lambda(t, k, v)$).

38.36 Theorem [452, 2016]

1. $\mathrm{LPA}_1(2, 3, v)$ exist if and only if $v \ge 3$ is odd.
2. $\mathrm{LOD}_1(2, 3, v)$ exist if and only if $v \ge 3$ and $v \ne 6$.

See Also

§VI.52.2	Describes the use of APA to construct authentication codes.
[260, 1968]	An application of PAs in the cryptographic theory of unconditional secrecy and authentication.
[1525]	A generalization of the notions of transitivity and homogeneity.
[260]	If there is an $\mathrm{APA}_1(2, k+2, v)$ that restricts to an $\mathrm{APA}_1(2, k, v)$, then a *Room k-cube of side v* exists.
[1847, 2037]	If a $\mathrm{PA}_1(2, k, v)$ admits an abelian automorphism group of order v in its operation on the entries, then $k-1$ MOLS of order v exist. See §IV.17.
[951]	A $\mathrm{PA}_1(2, k, v)$ admitting the cyclic group $\mathbb{Z}_k$ in its operation on the rows is equivalent with a *Steiner k-cycle system of order v*.
[2012]	Teirlinck's construction of large sets of t-designs for arbitrary t makes use of $\mathrm{OD}_1(t, t+1, v)$.

References Cited: [251, 254, 259, 260, 261, 265, 266, 452, 483, 597, 886, 951, 1344, 1459, 1525, 1654, 1700, 1776, 1847, 1968, 2012, 2013, 2016, 2037, 2159]

39 Orthogonal Main Effect Plans

Deborah J. Street

39.1 Definitions and Example

39.1 A *main effect plan* (MEP) has k *rows* (or *factors*), n *columns* (or *runs*) and s_i *symbols* (or *levels*) in row i, $1 \le i \le k$. Let n_{Ix} be the number of times that symbol x appears in row I and let n_{Jy} be the number of times that symbol y appears in row J. Let N_{IJ} be the $s_i \times s_j$ incidence matrix of rows I and J. The (x, y) position in N_{IJ} is the number of columns with x in row I and y in row J. The plan is *orthogonal* if the (x, y) position in N_{IJ} is $(n_{Ix} n_{Jy})/n$, for all pairs of rows I and J. An OMEP with these parameters is represented by $s_1 \times s_2 \times \ldots \times s_k//n$. OMEPs with the smallest possible number n of runs are *minimal*.

39.2 **Example** A $2 \times 3 \times 4//16$ OMEP.

$$\begin{array}{cccccccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 1 & 2 & 2 & 3 & 3 & 3 & 3 & 1 & 1 & 2 & 2 & 3 & 3 & 3 & 3 \\ 1 & 3 & 2 & 4 & 1 & 2 & 3 & 4 & 2 & 4 & 1 & 3 & 1 & 2 & 3 & 4 \end{array}$$

39.3 An OMEP is *partially replicated* (PROMEP) if it has at least one repeated run.

39.4 **Example** A $2 \times 3 \times 4//16$ PROMEP. (Replicated runs in boldface.)

$$\begin{array}{cccccccccccccccc} 1 & 1 & 1 & 1 & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & 2 & 2 & 2 & 2 & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ 1 & 1 & 2 & 2 & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & 1 & 1 & 2 & 2 & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} \\ 1 & 3 & 1 & 3 & \mathbf{2} & \mathbf{2} & \mathbf{4} & \mathbf{4} & 2 & 4 & 2 & 4 & \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{3} \end{array}$$

39.5 Consider a $s_1 \times s_2 \times \ldots \times s_k//n$ OMEP where $n = p_1^{m_1} p_2^{m_2} \ldots p_d^{m_d}$ is the prime factorization of n. Let $g_i = \gcd\{n_{Ix} |\ x \text{ a symbol in row } I\}$. For each prime p_t dividing n let ℓ_t be the greatest integer such that $p_t^{\ell_t} | g_j$ for each j. Choose c_t so that $p_t^{\ell_t}$ exactly divides g_{c_t}. Then by the definition of an OMEP, $p_t^{m_t - \ell_t}$ divides g_j for $j \ne c_t$. If $p_t^{m_t - \ell_t}$ exactly divides g_j for $j \ne c_t$ and if $s_j = n/g_j$ for each $j \in \{1, 2, \ldots, k\}$, then the OMEP is *tight*.

39.6 Example Consider the $2 \times 3 \times 4//16$ OMEP in Example 39.4. Here $n = 2^4 = p_1^{m_1}$, $g_1 = \gcd\{8, 8\} = 8$, $g_2 = \gcd\{4, 4, 8\} = 4$, and $g_3 = \gcd\{4, 4, 4, 4\}$. The largest power of $p_1 = 2$ to divide each g_i is 2 so $\ell_1 = 2$. Since 2^2 exactly divides g_2, let $c_1 = 2$. For the OMEP to be tight, one requires that 2^{4-2} exactly divides g_1 and g_3, which does not happen since $g_1 = 8$. Thus, the OMEP is not tight.

39.7 Theorem [853] If an $s_1 \times s_2 \times \ldots \times s_k//n$ OMEP is not tight then the parameters of the corresponding tight OMEP are given by $s_1' \times s_2' \times \ldots \times s_k'//n$ where $g_i' = n_{Ix} = \prod_{t:c_t \neq i} p_t^{m_t - \ell_t} \prod_{t:c_t = i} p_t^{\ell_t}$ and $s_i' = n/g_i'$.

39.8 Example Consider the $2 \times 3 \times 4//16$ OMEP in Example 39.4. The corresponding tight OMEP is a $4 \times 4 \times 4//16$ OMEP.

39.2 Existence

39.9 Theorem [1178, 1988] An $s_1 \times s_2 \times s_3//n$ OMEP, with $s_1 \leq s_2 \leq s_3$ and with the smallest entry of N_{23} equal to 1, exists if and only if

1. n is of the form $(s_2 + x)(s_3 + y)$ for some positive integers x and y, and
2. $s_1 \leq gcd(s_2 + x, s_3 + y)$.

39.10 Remarks

1. The extension of the necessity to more than three factors is straightforward, but there is then no guarantee that the OMEP exists.
2. When the smallest entry in N_{23} exceeds 1, a sufficient condition is given in [1988] for an OMEP to exist.

39.11 Theorem [398, 1988] Let N_{12} and $N_{k-2,k-1}$ be the incidence matrices of rows 1 and 2 and rows $k-2$ and $k-1$, respectively, of a $s_1 \times s_2 \times \ldots \times s_k//n$ OMEP, with $s_1 \leq s_2 \leq \ldots \leq s_k$.

1. A lower bound for the number of repeated runs is $\sum_{ij}(N_{12}(i,j) - s_k)$, where the summation is over the pairs (i, j) for which $N_{12}(i, j) > s_k$.
2. Let S and T be the sets of levels for factors $k-2$ and $k-1$, respectively, with replication greater than s_k. An upper bound for the number of repeated runs is
$$\sum_{i \in S} \sum_{j \in T} (N_{(k-2,k-1)}(i, j) - 1).$$

39.12 Theorem [853] For each fixed number k of rows, and with the exception of OMEPs of the form $2 \times 2 \times \ldots \times 2 \times 2d//4d$ with d odd and with more than three rows, there are only a finite number of tight OMEP parameters for which the tight OMEP does not exist.

39.3 Construction and Related Objects

39.13 Construction [1988] To construct an $s_1 \times s_2 \times s_3//(s_2 + x)(s_3 + y)$ OMEP with $s_1 \leq gcd(s_2 + x, s_3 + y)$, let r_{ij} be the number of times that level j appears in row i. Let $g = \gcd(s_2 + x, s_3 + y)$, $s_2 + x = gb$, and $s_3 + y = gc$. Choose the r_{3j} so that each $r_{3j} \geq gb$ and $gb \mid r_{3j}$ for all j. The third row of the OMEP consists of r_{31} 1s followed by r_{32} 2s and so on. It can be shown that $r_{2j} = b_j gc$. Let $\mathbf{b}$ be b_1 1s followed by b_2 2s and so on. The second row of the OMEP consists of gc copies of $\mathbf{b}$ placed side-by-side. It can be shown that $r_{1i} = a_i gbc$. Let $\mathbf{a}$ be $a_1 b$ 1s followed by $a_2 b$ 2s and so on. The first row of the OMEP consists of gc copies of $\mathbf{a}$ placed side-by-side with the entries of $\mathbf{a}$ being cycled by b each time that $\mathbf{a}$ is written down.

39.14 Example A $2 \times 4 \times 5//24$ OMEP. Here $x = 0, y = 1, g = 2$, **b**=(1,2,3,4), and **a**=(1,1,2,2).

1	1	2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2	1	1
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	5	5	5	5

39.15 Remarks

1. A new OMEP can be obtained from an existing OMEP by equating all occurrences of one level of a factor with those of another level of the same factor.
2. [64] A new OMEP can be obtained from two existing OMEPs by taking the direct product.

39.16 Construction [853] Suppose there is an $s_1 \times s_2 \times \ldots \times s_k//n$ OMEP and an $s_1 \times s_2 \times \ldots \times s'_k//n'$ OMEP with replication numbers n_{Ix} and n'_{Jy}, respectively. Suppose further that the symbol sets for the first $k-1$ rows are the same, that $n_{Ix}/n = n'_{Ix}/n'$ when $1 \le i \le k-1$, and that the symbols in the final two rows are all distinct. Then the concatenation gives an $s_1 \times s_2 \times \ldots \times (s_k + s_k)'//(n + n')$ OMEP.

39.17 Table Known minimal three-factor PROMEPs with at most 25 runs and associated bounds. L is the lower bound for the number of repeated runs, U is the upper bound, and KRR is the set of repeated runs for which an OMEP is known. Designs with $s_1 \le gcd(s_2, s_3)$ have $n = s_2 s_3$ and, hence, have no repeated runs and are not listed.

s_1	s_2	s_3	n	L	U	KRR	s_1	s_2	s_3	n	L	U	KRR	s_1	s_2	s_3	n	L	U	KRR
2	2	3	8	0	2	0, 2	2	2	11	24	0	2	0, 2	3	3	4	16	0	2	0,1,2
2	2	5	12	0	2	0, 2	2	3	4	16	0	4	0,2,4	3	3	5	18	0	3	0,1,3
2	2	7	16	0	2	0, 2	2	3	5	18	0	3	1,3	3	4	5	25	0	4	0,1,2,3
2	2	9	20	0	2	0, 2	2	4	5	24	0	4	0,2,4	4	4	5	25	0	2	0,1,2

39.18 Remarks

1. An $\mathrm{OA}_\lambda(k, s)$ is an $s \times \ldots \times s//\lambda s^2$ OMEP in which each level of each factor is replicated equally often.
2. An orthogonal array with a variable number of symbols of strength 2 (OAVS) is an OMEP but not vice versa.
3. A set of $k-2$ mutually orthogonal F-squares of order t can be used to construct a k-factor OMEP with $n = t^2$ runs and two factors each with t levels.
4. OMEPs form a class of fractionally replicated asymmetrical factorial designs.

See Also

§III.3	Orthogonal arrays give examples of OMEPs and are used extensively in their construction.
§III.6	Orthogonal arrays of higher index are used to construct OMEPs.
§VI.22	Orthogonal frequency squares.
§VI.21	Factorial designs.
[398]	Algorithms for constructing OMEPs.
[1178, 1179, 1988]	Constructions for OMEPs.
[1178, 1988]	Existence results for OMEPs.
[1989]	A survey of OMEPs and OAVS with extensive bibliography.

References Cited: [64, 398, 853, 1178, 1179, 1988, 1989]

40 Packings

Douglas R. Stinson
Ruizhong Wei
Jianxing Yin

40.1 Definitions and Examples

40.1 Let $v \geq k \geq t$. A t-(v,k,λ) *packing* is a pair $(X,\mathcal{B})$, where X is a v-set of elements (*points*) and $\mathcal{B}$ is a collection of k-subsets of X (*blocks*), such that every t-subset of points occurs in at most λ blocks in $\mathcal{B}$. If $\lambda > 1$, then $\mathcal{B}$ is allowed to contain repeated blocks.

40.2 The *packing number* $D_\lambda(v,k,t)$ is the maximum number of blocks in any t-(v,k,λ) packing. A t-(v,k,λ) packing $(X,\mathcal{B})$ is *optimal* if $|\mathcal{B}| = D_\lambda(v,k,t)$. If $\lambda = 1$, often one writes $D(v,k,t)$ for $D_1(v,k,t)$.

40.3 **Examples** For each of the given parameter sets t-(v,k,λ), one example of an optimal t-(v,k,λ) packing is given.

t-(v,k,λ)	Packing
2-$(6,3,1)$	{1,2,3} {1,4,5} {2,4,6} {3,5,6}
2-$(8,3,1)$	{1,3,5} {1,4,8} {1,6,7} {2,3,7} {2,4,6} {2,5,8} {3,6,8} {4,5,7}
2-$(11,3,1)$	{1,2,3} {1,4,5} {1,6,7} {1,8,11} {1,9,10} {2,6,8} {2,7,9} {2,10,11} {3,6,9} {3,7,11} {3,8,10} {4,6,10} {4,7,8} {4,9,11} {5,6,11} {5,8,9} {5,7,10}
2-$(9,4,1)$	{1,2,3,4} {1,5,6,7} {3,6,8,9}
2-$(10,4,1)$	{1,2,3,4} {1,5,6,7} {2,5,8,9} {3,6,8,10} {4,7,9,10}
2-$(14,5,1)$	{1,2,3,4,5} {1,6,7,8,9} {2,6,10,11,12} {3,7,10,13,14}
3-$(9,5,1)$	{1,2,3,4,5} {1,2,6,7,8} {3,4,6,7,9}
3-$(16,7,1)$	{1,2,3,4,5,6,7} {1,2,8,9,10,11,12} {3,4,8,9,13,14,15} {5,6,9,10,13,14,16}
4-$(10,6,1)$	{1,2,3,4,5,6} {1,2,3,7,8,9} {1,4,5,7,8,10} {2,4,6,7,9,10} {3,5,6,8,9,10}

40.4 **Remark** The survey paper [1614] covers much of the material in this chapter. For this reason, individual references prior to the publication of that paper are not given in general.

40.2 Equivalent Combinatorial Objects and Bounds

40.5 **Theorem** A t-(v,k,λ) packing with $\lambda\binom{v}{t}/\binom{k}{t}$ blocks is equivalent to a t-(v,k,λ) design or an $S_\lambda(t,k,v)$ (possibly containing repeated blocks).

40.6 **Theorem** A t-$(v,k,1)$ packing with b blocks is equivalent to a binary code of length v, size b, constant weight k, and minimum Hamming distance at least $2(k-t+1)$. (See §VII.1.)

40.7 **Theorem** (First Johnson bound) $D_\lambda(v,k,t) \leq \left\lfloor \frac{vD_\lambda(v-1,k-1,t-1)}{k} \right\rfloor$. Iterating this bound yields $D_\lambda(v,k,t) \leq U_\lambda(v,k,t)$, where

$$U_\lambda(v,k,t) = \left\lfloor \frac{v}{k} \left\lfloor \frac{v-1}{k-1} \cdots \left\lfloor \frac{\lambda(v-t+1)}{k-t+1} \right\rfloor \right\rfloor \right\rfloor .$$

Further, if $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\frac{\delta(k-1)}{2} > \lambda\frac{\delta(\delta-1)}{2}$, where $\delta = \frac{\lambda v(v-1)}{k-1} - kU_\lambda(v,k,2)$, then $D_\lambda(v,k,2) \le U_\lambda(v,k,2) - 1$.

40.8 Theorem (Complementing) By taking the complement of each block in a packing with $\lambda = 1$, one has that $D(v,k,t) = D(v, v-k, v-2k+t)$.

40.9 Theorem (Second Johnson bound) Suppose $d = D_\lambda(v,k,t) = qv + r$, where $0 \le r \le v-1$. Then $q(q-1)v + 2qr \le (t-1)d(d-1)$. From this it follows that

$$D_\lambda(v,k,t) \le \left\lfloor \frac{v(k+1-t)}{k^2 - v(t-1)} \right\rfloor .$$

40.3 Determination of Packing Numbers

40.10 Theorem If $v \equiv 2 \pmod 6$ and $\lambda \equiv 4 \pmod 6$, or if $v \equiv 5 \pmod 6$ and $\lambda \equiv 1 \pmod 3$, then $D_\lambda(v,3,2) = U_\lambda(v,3,2) - 1$. Otherwise, $D_\lambda(v,3,2) = U_\lambda(v,3,2)$.

40.11 Remark $D_\lambda(v,3,2) = U_\lambda(v,3,2)$ except when Theorem 40.9 applies.

40.12 Theorem $D(v,4,2) = U_1(v,4,2) - \epsilon$, where

$$\epsilon = \begin{cases} 1 & \text{if } v \equiv 7 \text{ or } 10 \pmod{12},\ v \ne 10, 19 \\ 1 & \text{if } v = 9 \text{ or } 17 \\ 2 & \text{if } v = 8, 10 \text{ or } 11 \\ 3 & \text{if } v = 19 \\ 0 & \text{otherwise.} \end{cases}$$

40.13 Theorem Suppose $\lambda > 1$. If $v = 9$ and $\lambda = 2$, or if $v = 3$ and $\lambda = 3$, then $D_\lambda(v,4,2) = U_\lambda(v,4,2) - 1$. Otherwise, $D_\lambda(v,4,2) = U_\lambda(v,4,2)$.

40.14 Theorem

1. If $v \equiv 1, 2, 3, \text{or } 4 \pmod 6$, then $D(v,4,3) = U_1(v,4,3)$.
2. If $v \equiv 0 \pmod 6$, then $D(v,4,3) = \left\lfloor \frac{vD(v-1,3,2)}{4} \right\rfloor$.
3. (Ji [1196]) If $v \equiv 5 \pmod 6$ and $v \notin E$, then $D(v,4,3) = U_1(v,4,3)$, where $E = \{6k+5 | k \text{ is odd}, 3 \le k \le 35 \text{ and } k \ne 17, 21\} \cup \{6k+5 | k = 45, 47, 75, 77, 79, 159\}$.

40.15 Theorem [117, 879, 880, 1657, 2190] Suppose that $v > 20$. Then $D(v,5,2) = U_1(v,5,2)$ if one of the following is satisfied:

1. $v \equiv 0 \pmod 4$ and $v \notin \{32, 48, 52, 72, 132, 152, 172, 232, 252, 272, 332, 352\}$;
2. $v \equiv 3, 15 \pmod{20}$;
3. $v \equiv 7, 11 \pmod{20}$ and $v \notin \{27, 47, 51, 67, 87, 187, 231, 251, 291\}$;
4. $v \equiv 2, 10 \pmod{20}$ and $v \notin \{22, 30, 70, 142, 150, 190, 222, 230, 390, 430\}$;
5. $v \equiv 6 \pmod{20}$ and $v \ne 20n+6$ with $n \in \{1, 3, 5, 7, 9, 11, 13, 17, 19, 21, 23, 29, 31, 33, 35, 37, 39, 43, 47, 51, 53, 55, 57, 59, 63, 69, 71, 73\} \cup \{2, 8, 14, 16, 18, 26, 38, 46\}$;
6. $v \equiv 14 \pmod{20}$ and $v \ge 20 \cdot 399 + 1334$; or
7. $v \equiv 18 \pmod{20}$ and $v \ge 20 \cdot 252 + 698$.

40.16 Theorem [1657] If $v \equiv 9, 13, \text{or } 17 \pmod{20}$, then $D(v,5,2) \le U_1(v,5,2) - 1$. Further, if $v \equiv 9 \text{ or } 17 \pmod{20}$, $v > 29$, and $v \ne 49$, then $D(v,5,2) = U_1(v,5,2) - 1$.

40.17 Remark No optimal 2-$(v,5,1)$ packing has been found in the congruence classes 13 and 19 (mod 20) yet.

40.18 Theorem [117, 2183] Let $\lambda > 1$ and $D_\lambda(v,5,2) = U_\lambda(v,5,2) - e$. Apart from the undecided cases of $(v,\lambda) = (19,2)$, $(27,2)$, $(28,3 \text{ or } 11 \bmod 20)$, $(29,3)$, $(32,3 \bmod 20)$, $(33,3)$, and $(44,7 \bmod 20)$, $e = 0$ except when:

1. $\lambda = 2$ and $v = 15$;
2. $\lambda = 2$ and $v = 13$;
3. $\lambda \equiv 2 \pmod{20}$ and $v \equiv 7,9 \pmod{10}$;
4. $\lambda = 3$ and $v \equiv 13 \pmod{20}$;
5. $\lambda = 4$ and $v = 7$;
6. $\lambda \equiv 4 \pmod{20}$ and $v \equiv 3 \pmod{5}$;
7. $\lambda \equiv 12 \pmod{20}$ and $v \equiv 2,4 \pmod{5}$; or
8. $\lambda = 14$ and $v = 7$.

In case 1, $e = 2$ and in cases 2 through 8, $e = 1$.

40.19 Theorem [2191] If $v \geq 6$ and $v \neq 8$, then $D_5(v,6,2) = U_5(v,6,2)$. Moreover, $D_5(8,6,2) = U_5(8,6,2) - 1$.

40.20 Table Known values $D(v,k,t)$ for $v \leq 20$, $2 \leq t \leq 5$, and $1 \leq k - t \leq 4$.

$t = 2$

$v\backslash k$	3	4	5	6
3	1			
4	1	1		
5	2	1	1	
6	4	1	1	1
7	7	2	1	1
8	8	2	1	1
9	12	3	2	1
10	13	5	2	1
11	17	6	2	2
12	20	9	3	2
13	26	13	3	2
14	28	14	4	2
15	35	15	6	3
16	37	20	6	3
17	44	20	7	3
18	48	22	9	4
19	57	25	12	4
20	60	30	16	5

$t = 3$

$v\backslash k$	4	5	6	7
4	1			
5	1	1		
6	3	1	1	
7	7	1	1	1
8	14	2	1	1
9	18	3	1	1
10	30	6	2	1
11	35	11	2	1
12	51	12	4	2
13	65	18	4	2
14	91	28	7	2
15	105	42	10	3
16	140	48	16	4
17	156	68	17	5
18	198		21	6
19	228		28	8
20	285		40	10

$t = 4$

$v\backslash k$	5	6	7	8
5	1			
6	1	1		
7	3	1	1	
8	8	1	1	1
9	18	3	1	1
10	36	5	1	1
11	66	11	2	1
12		22	3	1
13		26	4	2
14		42	8	2
15		70	15	3
16		112	16	4
17			24	6
18				9
19				12
20			80	17

$t = 5$

$v\backslash k$	6	7	8	9
6	1			
7	1	1		
8	4	1	1	
9	12	1	1	1
10	30	3	1	1
11	66	6	1	1
12	132	12	3	1
13		26	3	1
14		42	7	2
15			15	3
16			30	3
17			34	6
18				10
19				19

40.4 Structure of Optimal Packings

40.21 Let $(X, \mathcal{B})$ be a 2-$(v, k, 1)$ packing. The *leave graph* of $(X, \mathcal{B})$ is the graph (X, E), where E consists of all 2-subsets of X that occur in no blocks of $\mathcal{B}$.

40.22 Table Optimal 2-$(v, 3, 1)$ packings.

$v \equiv$	$D(v,3,2)$	Leave Graph	Construction
$1,3 \pmod 6$	$\frac{v^2-v}{6}$	empty	BIBD$(v,3,1)$
$0,2 \pmod 6$	$\frac{v^2-2v}{6}$	$\frac{v}{2}K_2$	BIBD$(v+1,3,1)$ with a point deleted
$4 \pmod 6$	$\frac{v^2-2v-2}{6}$	$K_{1,3} \cup \frac{v-4}{2}K_2$	Delete a point from the 4-cycle in an optimal packing on $v+1$ points
$5 \pmod 6$	$\frac{v^2-v-8}{6}$	cycle of length 4	PBD$(v, \{3, 5^*\})$ with the block of size 5 replaced by two blocks of size 3.

40.23 Table Optimal 2-$(v, 4, 1)$ packings, $v \notin \{8, 9, 10, 11, 17, 19\}$.

$v \equiv$	$D(v,4,2)$	Leave Graph	Construction
$1,4 \pmod{12}$	$\frac{v^2-v}{12}$	empty	BIBD$(v,4,1)$
$0,3 \pmod{12}$	$\frac{v^2-3v}{12}$	$\frac{v}{3}K_3$	BIBD$(v+1,4,1)$ with a point deleted
$2,8 \pmod{12}$	$\frac{v^2-2v}{12}$	$\frac{v}{2}K_2$	$\{4\}$-GDD of type $2^{v/2}$
$5,11 \pmod{12}$	$\frac{v^2-2v-3}{12}$	$K_{1,4} \cup \frac{v-5}{2}K_2$	$\{4\}$-GDD of type $2^{(v-5)/2}5^1$ with the group of size 5 replaced by a block of size 4
$7,10 \pmod{12}$	$\frac{v^2-v-18}{12}$	$K_{3,3}$	PBD$(v, \{4, 7^*\})$ with the block of size 7 replaced by two blocks of size 4
$6,9 \pmod{12}$	$\frac{v^2-3v-6}{12}$	$(K_6 \backslash K_4) \cup \frac{v-6}{3}K_3$	$\{4\}$-GDD of type $3^{(v-6)/3}6^1$ with the group of size 6 replaced by a block of size 4

40.24 Table Optimal 3-$(v, 4, 1)$ packings except the 21 undecided cases from Theorem 40.14.

$v \equiv$	$D(v,4,3)$	Construction
$2,4 \pmod 6$	$\frac{v^3-3v^2+2v}{24}$	3-$(v,4,1)$ design
$1,3 \pmod 6$	$\frac{v^3-4v^2+3v}{24}$	3-$(v,4,1)$ design with a point deleted
$0 \pmod 6$	$\frac{v^3-3v^2-6v}{24}$	$G(m,6,4,3)$ with every group replaced by three blocks of size 4 (a $G(m,6,4,3)$ is a $\{4,6\}$-3BD in which the blocks of size 6 form a parallel class). (See §VI.63.)

$v \equiv$	$D(v,4,3)$	Construction
5 (mod 12)	$\frac{v^3-4v^2+v-6}{24}$	A few small packing designs were constructed directly. Then a recursive construction using candelabra quadruple systems is applied. See [1196] for details.
11 (mod 12)	$\frac{v^3-4v^2+v-18}{24}$	

40.5 Resolvable Packings with $\lambda = 1$

40.25 A t-(v,k,λ) packing $(X,\mathcal{B})$ is *resolvable* if $\mathcal{B}$ can be partitioned into *parallel classes*, each of which consists of v/k disjoint blocks.

40.26 Theorem Suppose $v \equiv 0 \pmod k$. If $v-1 \equiv 0 \pmod{(k-1)}$, then a resolvable 2-$(v,k,1)$ packing with $U_1(v,k,2)$ blocks is equivalent to a RBIBD$(v,k,1)$. If $v-1 \not\equiv 0 \pmod{(k-1)}$, then a resolvable 2-$(v,k,1)$ packing with $U_1(v,k,2)$ blocks is equivalent to a resolvable $\{k\}$-GDD of type $g^{v/g}$, where $g = v - \lfloor \frac{v-1}{k-1} \rfloor (k-1)$.

40.27 Table Resolvable optimal 2-$(v,k,1)$ packings for $k = 3, 4$.

k	v	Equivalent Design	Existence Results
3	$\equiv 0 \pmod 6$	$\{3\}$-RGDD of type $2^{v/2}$	All admissible $v \neq 6, 12$
3	$\equiv 3 \pmod 6$	RBIBD$(v,3,1)$	All admissible v
4	$\equiv 0 \pmod{12}$	$\{4\}$-RGDD of type $3^{v/3}$	All admissible $v \geq 24$ [876]
4	$\equiv 4 \pmod{12}$	RBIBD$(v,4,1)$	All admissible v
4	$\equiv 8 \pmod{12}$	$\{4\}$-RGDD of type $2^{v/2}$	All admissible $v \geq 32$, except possibly for $v =$ 68, 92, 104, 140, 164, 188, 200, 236, 260, 284, 356, 368, 404, 428, 476, 500, 668, or 692 [876]

40.6 Pair Packings with Spanning Holes

40.28 Let $n \geq k$. A *holey packing* of block size k, index λ, and type g^n ((k,λ)-HP of type g^n), is a triple $(X,\mathcal{H},\mathcal{B})$, where X is a ng-set of elements (*points*), $\mathcal{H}$ is a partition of X into n subsets (*holes*) of cardinality g, and $\mathcal{B}$ is a collection of k-subsets (*blocks*) of X, such that every pair of points from distinct holes occurs in at most λ blocks and no block contains two distinct points from any hole. If $\lambda > 1$, then $\mathcal{B}$ is allowed to contain repeated blocks.

40.29 The *packing number* $D_\lambda(2,k,n,g)$ is the maximum number of blocks in any (k,λ)-HP of type g^n. A (k,λ)-HP of type g^n $(X,\mathcal{H},\mathcal{B})$ is *optimal* if $|\mathcal{B}| = D_\lambda(2,k,n,g)$. If $\lambda = 1$, the notation $D(2,k,n,g)$ is used.

40.30 Theorem [2187, 2192] Let $U_\lambda(2,k,n,g) = \left\lfloor \frac{gn}{k} \left\lfloor \frac{\lambda g(n-1)}{k-1} \right\rfloor \right\rfloor$. Then $D_\lambda(2,k,n,g) \leq U_\lambda(2,k,n,g)$. Further,

1. if $\lambda(n-1)g \equiv 0 \pmod{k-1}$ and $\lambda n(n-1)g^2 \equiv -1 \pmod k$, then $D_\lambda(2,k,n,g) \leq U_\lambda(2,k,n,g) - 1$;
2. if $(n-1)g \equiv 0 \pmod{k-1}$ and $n(n-1)g^2 \not\equiv 0 \pmod k$, then $D(2,k,n,g) \leq U_1(2,k,n,g) - 1$.

40.31 Remark A (k,λ)-HP of type g^n with $\frac{\lambda n(n-1)g^2}{k(k-1)}$ blocks is equivalent to a (k,λ)-GDD.

40.32 Theorem (Yin [2187]) Let n, g and λ be positive integers with $n \geq 3$. Then

1. $D_\lambda(2,3,n,g) = U_\lambda(2,3,n,g) - 1$ if $\lambda(n-1)g \equiv 0 \pmod 2$ and $\lambda n(n-1)g^2 \equiv -1 \pmod 3$;
2. $D_\lambda(2,3,n,g) = U_\lambda(2,3,n,g)$, otherwise.

40.33 A *maximum distance holey packing* MDHP$(2,k,n,g)$ is a $(k,1)$-HP of type g^n $(X, \mathcal{H}, \mathcal{B})$ that satisfies the following properties:

1. any two distinct blocks of $\mathcal{B}$ can meet at most two common holes if they share a common point, and at most three common holes if they are disjoint;
2. the number of blocks is

$$BN(2,k,n,g) = \begin{cases} \left\lfloor \frac{ng}{k} \left\lfloor \frac{(n-1)g}{k-1} \right\rfloor \right\rfloor - 1, & \text{if } (n-1)g \equiv 0 \pmod{k-1} \text{ and} \\ & n(n-1)g^2 \not\equiv 0 \pmod{k(k-1)}; \\ \left\lfloor \frac{ng}{k} \left\lfloor \frac{(n-1)g}{k-1} \right\rfloor \right\rfloor, & \text{otherwise.} \end{cases}$$

40.34 Theorem An MDHP$(2,k,n,g)$ can exist only if $n \geq (k-2)g + 2$.

40.35 Theorem [793, 2189, 2192] For any integer $g > 1$, an MDHP$(2,k,n,g)$ is equivalent to a maximum $(g+1)$-ary code of length n, constant weight k, and minimum Hamming distance at least $2(k-2)+1$.

40.36 Theorem [793, 2189] For all integers $n \geq 7$, there exists an MDHP$(2,3,n,2)$ and for all integers $n \geq 5$, there exists an MDHP$(2,3,n,3)$.

40.7 Cyclic Packings

40.37 An *automorphism* of a design is a permutation of its point set that preserves its block set. A t-(v,k,λ) packing $(X,\mathcal{B})$ is *cyclic* if it admits a cyclic automorphism group of order v that is spanned by a v-cycle. Hence, its point set X and the automorphism group can be identified with the additive group of $\mathbb{Z}_v$.

40.38 Let $B = \{b_1, \ldots, b_k\}$ be a block in a cyclic t-(v,k,λ) packing $(\mathbb{Z}_v, \mathcal{B})$. The *block orbit* containing B is defined to be the set of the distinct blocks $B+i = \{b_1+i, \ldots, b_k+i\}$ with $i \in \mathbb{Z}_v$, where the addition is performed in $\mathbb{Z}_v$. If a block orbit has v distinct blocks (its setwise stabilizer G_B is equal to the identity), then this block orbit is *full*, otherwise it is *short*. An arbitrary fixed block from a block orbit is a *base block*. A cyclic t-(v,k,λ) packing $(\mathbb{Z}_v, \mathcal{B})$ having only full block orbits is denoted by t-CP$(k,\lambda;v)$. If $t = 2$, the parameter t is often omitted. A cyclic packing with maximum possible number of blocks is *optimal*.

40.39 Theorem If $\lambda < k$, then a cyclic $(\lambda+1)$-$(v,k,1)$ packing of b full orbits is equivalent to an optical orthogonal code, $\mathcal{C}$, of length v, size b and constant weight k, (denoted (v,k,λ)-OOC), that satisfies the following two correlation properties:

1. $\sum_{0 \leq t \leq v-1} x_t x_{t+i} \leq \lambda$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$ and any integer $i \not\equiv 0 \bmod v$;
2. $\sum_{0 \leq t \leq v-1} x_t y_{t+i} \leq \lambda$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$, $\mathbf{y} = (y_0, y_1, \ldots, y_{v-1}) \in \mathcal{C}$ with $\mathbf{x} \neq \mathbf{y}$, and any integer i.

Here, the subscripts are taken modulo v.

40.40 Remark For the connection between optical orthogonal codes and cyclic packings, see [546] and references therein. See also §V.9.

40.41 Table Known optimal t-CP$(k, 1; v)$ for $t = 2, 3$ and $3 \le k \le 5$. In the table, g is a nonnegative integer, p is a prime, and $\prod_i p_i$ is a product of primes p_i.

t	k	v	
2	3	g	$g \neq 6t+2$ with $t \equiv 2, 3 \pmod 4$
2	4	g	$g \le 408, g \neq 25$ or $g \equiv 6 \pmod{12}$ or $g \equiv 0 \pmod{24}$
		$g\prod_i p_i$	$g \in \{2, 10, 2^n, 4^n, n \ge 3\}, p_i \equiv 1 \pmod 6$ or
			$g = 4, p_i \equiv 1 \pmod 6$, $(p_i - 1)/6$ has a prime factor at most 19 or
			$g \in \{12, 3^n, n \ge 1\}, p_i \equiv 1 \pmod 4$ or
			$g \in \{1, 4, 5, 7, 11\}, p_i \equiv 1 \pmod{12}$
		7p	$p \equiv 7 \pmod{12}, p < 10000$ or if ω is a primitive root unit in $\mathbb{Z}_p$ such that $3 \equiv \omega^i \pmod p, \gcd(i, (p-1)/6) < 20$
2	5	$g\prod_i p_i$	$g \in \{5 \cdot 3^n, n \ge 0\}, p_i \equiv 1 \pmod 4$ or
			$g \in \{60, 80, 100, 120, 140, 160, 180\}, p_i > 5$ or
			$g = 4, p_i \equiv 1 \pmod{10}, p_i > 11$ or
			$g \in \{1, 5, 7, 11, 13, 17, 19\}, p_i \equiv 1 \pmod{20}$ or
			$g \in \{8, 12\}, p_i \equiv 11 \pmod{20}$ or
			$g = 6, p_i \equiv 21 \pmod{40}$ or
			$g = 30, p_i \equiv 5 \pmod 8, p_i > 5$
3	3	g	$g \not\equiv 0 \pmod 3, g \ge 5$
3	4	g	$7 \le g \le 44, g \neq 24, 36, 42$ or
			$g = 2^n, n \ge 3$

40.42 Remark For the data of Table 40.41, see [23, 456, 459, 505, 841, 1491, 2001, 2188] and their references. Some results are obtained by using a recursive method from [2184].

40.43 Theorem ([590]) There exist optimal cyclic 2-$(v, 3, \lambda)$ packings with the following parameters:

1. $\lambda \equiv 1, 5, 7, 11 \pmod{12}$ and $v \equiv 1, 3 \pmod 6$ or
2. $\lambda \equiv 2, 10 \pmod{12}$ and $v \equiv 0, 1, 3, 4, 7, 9 \pmod{12}$ or
3. $\lambda \equiv 3, 9 \pmod{12}$ and $v \equiv 1 \pmod 2$ or
4. $\lambda \equiv 4, 8 \pmod{12}$ and $v \equiv 0, 1 \pmod 3$ or
5. $\lambda \equiv 6 \pmod{12}$ and $v \equiv 0, 1, 3 \pmod 4$ or
6. $\lambda \equiv 0 \pmod{12}$ and $v \ge 3$.

See Also

§II.1	BIBDs are packings with empty leave graph.
§II.1	A cyclic BIBD of block size k, order v, and index λ is an optimal CP$(k, \lambda; v)$.
§III.4	Incomplete transversal designs are used extensively in various constructions for packings.
§IV.1	Pairwise balanced designs.
§IV.1	An exact MDHP is a special GDD.
§VI.63	t-wise balanced designs.
§VI.20.6	Directed packings.
[1614]	Coverings and packings survey with an extensive bibliography.
[2189]	A survey of MDHP.

References Cited: [23, 117, 456, 459, 505, 546, 590, 793, 841, 876, 879, 880, 1196, 1491, 1614, 1657, 2001, 2183, 2184, 2187, 2188, 2189, 2190, 2191, 2192]

41 Partial Geometries

Joseph A. Thas

41.1 Definitions and Examples

41.1 A (finite) *partial geometry* is an incidence structure $\mathcal{S} = (P, B, \mathrm{I})$ in which P and B are disjoint (nonempty) sets of objects, *points* and *lines*, and for which I is a symmetric point-line incidence relation, $\mathrm{I} \subseteq (P \times B) \cup (B \times P)$, satisfying the following axioms:

1. each point is incident with $1 + t$ lines ($t \geq 1$) and two distinct points are incident with at most one line;
2. each line is incident with $1 + s$ points ($s \geq 1$) and two distinct lines are incident with at most one point;
3. if x is a point and L is a line not incident with x, then there are exactly α ($\alpha \geq 1$) points $y_1, y_2, \cdots, y_\alpha$ and α lines $M_1, M_2, \cdots, M_\alpha$ such that $x \mathrm{I} M_i \mathrm{I} y_i \mathrm{I} L$, with $i = 1, 2, \cdots, \alpha$.

The integers s, t, and α are the *parameters* of the partial geometry. Put $|P| = v$ and $|B| = b$.

41.2 Remarks

1. There is a point-line duality for partial geometries for which in any definition or theorem the words *point* and *line* are interchanged and the parameters s and t are interchanged.
2. R.C. Bose used r, k, t for the parameters $t + 1, s + 1, \alpha$ given above.

41.3 Examples

1. A *generalized quadrangle* is a partial geometry with $\alpha = 1$. (See §VI.23.)
2. Let P be the set of all points of the n-dimensional projective space $\mathrm{PG}(n, q)$ over the field $\mathbb{F}_q$, which are not contained in a fixed subspace $\mathrm{PG}(n-2, q)$, with $n \geq 2$. Let B be the set of all lines of $\mathrm{PG}(n, q)$ having no point in common with $\mathrm{PG}(n-2, q)$. Finally, let I be the natural incidence. Then (P, B, I) is a partial geometry with $s = q, t = q^{n-1} - 1, \alpha = q$. This geometry is denoted by H_q^n [2026].

41.2 Existence and Pseudo-Geometric Graphs

41.4 Theorem [1108] If $\mathcal{S} = (P, B, \mathrm{I})$ is a partial geometry with parameters s, t, α, then $v = (s+1)(st+\alpha)/\alpha$ and $b = (t+1)(st+\alpha)/\alpha$.

41.5 Theorem The point graph of a partial geometry with parameters s, t, α is a strongly regular graph with parameters $v, k = s(t+1), \lambda = s - 1 + t(\alpha - 1), \mu = \alpha(t+1)$. (See §VII.11.)

41.6 Each strongly regular graph Γ having the parameters of Theorem 41.5 with $t \geq 1, s \geq 1, 1 \leq \alpha \leq s+1$, and $1 \leq \alpha \leq t+1$ is a *pseudo-geometric* (t, s, α)-graph. If the pseudo-geometric graph Γ is the point graph of at least one partial geometry, then it is *geometric*.

41.7 Theorem Any pseudo-geometric $(s^2, s, 1)$-graph is geometric [420].

41.8 Theorem Let $\mathcal{S} = (P, B, \mathrm{I})$ be a partial geometry with parameters s, t, α. Then s, t and α satisfy:

1. the integer $\alpha(s + t + 1 - \alpha)$ divides $st(s + 1)(t + 1)$ [1108]; and
2. the Krein inequalities [420], namely,
   $(s + 1 - 2\alpha)t \leq (s - 1)(s + 1 - \alpha)^2$ and $(t + 1 - 2\alpha)s \leq (t - 1)(t + 1 - \alpha)^2$.

41.9 Partial geometries $\mathcal{S}$ can be divided into four (nondisjoint) classes.

1. $\mathcal{S}$ has $\alpha = s+1$ or, dually, $\alpha = t+1$; when $\alpha = s+1$, then $\mathcal{S}$ is a 2-$(v, s+1, 1)$ design.
2. $\mathcal{S}$ has $\alpha = s$ or, dually, $\alpha = t$; when $\alpha = t$, then $\mathcal{S}$ is a *net* of *order* $s + 1$ and *degree* $t + 1$.
3. When $\alpha = 1$, $\mathcal{S}$ is a generalized quadrangle.
4. When $1 < \alpha < \min(s, t)$, then $\mathcal{S}$ is *proper*.

41.10 Remark Example 41.3(2) is a dual net.

41.11 Remark The dual of a net of order $s + 1$ and degree $t + 1$ is a transversal design $\mathrm{TD}(t + 1, s + 1)$; see §III.3.

41.12 *Axiom of Pasch*: if $L_1 \mathrm{I} x \mathrm{I} L_2$, $L_1 \neq L_2$, $M_1 \not\mathrm{I} x \not\mathrm{I} M_2$, and if L_i has a point in common with M_j for all $i, j \in \{1, 2\}$, then M_1 and M_2 have a point in common. This axiom is also known as the *Axiom of Veblen* or the *Veblen–Young Axiom*.

41.13 Theorem [2026] Let $\mathcal{S}$ be a dual net of order $s+1$ and degree $t+1$, with $s < t+1$ (for such a dual net one has that $s \leq t + 1$ and $s = t + 1$ if and only if $\mathcal{S}$ is a dual affine plane of order s). Then $\mathcal{S}$ satisfies the axiom of Pasch if and only if it is isomorphic to a dual net H_q^n with $n \geq 3$ ($s = q$ and $t = q^{n-1} - 1$).

41.3 Maximal Arcs

41.14 In a projective plane $\mathcal{P}$ of order q any nonempty set of k points may be described as a $\{k; d\}$-*arc*, where d ($d \neq 0$) is the greatest number of collinear points in the set. For given q and d ($d \neq 0$), k can never exceed $dq - q + d$, and a $\{dq - q + d; d\}$-arc is a *maximal arc*. Equivalently, a maximal arc may be defined as a nonempty set of points in $\mathcal{P}$ meeting every line in just d points or in none at all.

41.15 Examples

1. The point set of $\mathcal{P}$ is a maximal arc with $d = q + 1$.
2. The point set of the affine plane $\mathcal{A}$ obtained by deleting a line from $\mathcal{P}$ is a maximal arc with $d = q$.
3. A single point is a maximal arc with $d = 1$.
4. A *hyperoval* of $\mathcal{P}$, that is, a set of $q + 2$ points no three of which are collinear, is a maximal arc with $d = 2$.

41.16 Theorem If K is a $\{dq-q+d; d\}$-arc (a maximal arc) of the projective plane $\mathcal{P}$, where $d \leq q$, then the set K'=$\{$lines L of $\mathcal{P} \mid L \cap K = \phi\}$ is a $\{q(q - d + 1)/d; q/d\}$-arc (a maximal arc) of the dual plane.

41.17 Corollary A necessary condition for the existence of a maximal arc, with $d \le q$, is that d is a factor of q.

41.18 Remark Theorem 41.19 contains the two most important results on the existence of maximal arcs.

41.19 Theorem

1. [151] In $\mathrm{PG}(2,q)$, with q odd, there are no $\{qd-q+d;d\}$-arcs for $1<d<q$.
2. (Denniston, see [1105]) For any factor d of q, q even, there exists a $\{dq-q+d;d\}$-arc in the plane $\mathrm{PG}(2,q)$.

41.20 Remark Maximal arcs in $\mathrm{PG}(2,q)$, q even, are constructed in [1027, 1105, 1542, 2024].

41.21 Construction Let K be a maximal $\{qd-q+d;d\}$-arc of a projective plane $\mathcal{P}$ of order q, $2 \le d < q$. Let P be the set of all points of $\mathcal{P}$ not in K, let B be the set of all lines of $\mathcal{P}$ having a nonempty intersection with K, and let I be the natural incidence. Then $\mathcal{S}(K) = (P, B, \mathrm{I})$ is a partial geometry with parameters

$$s = q-d, \quad t = q(d-1)/d, \quad \alpha = (q-d)(d-1)/d.$$

41.22 Remark Construction 41.21 is due independently to Thas and Wallis.

41.23 Construction (see [644]) Let $\mathcal{P} = \mathrm{PG}(2,q)$ and embed $\mathcal{P}$ in the projective space $\mathrm{PG}(3,q)$. Further, let P' consist of all points of $\mathrm{PG}(3,q)$ not in $\mathcal{P}$, let B' consist of all lines of $\mathrm{PG}(3,q)$ having a unique point in common with the maximal $\{qd-q+d;d\}$-arc K of $\mathcal{P}$, and let I′ be the natural incidence. Then $\mathcal{T}_2^*(K) = (P', B', \mathrm{I}')$ is a partial geometry with parameters

$$s = q-1, \quad t = (q+1)(d-1), \quad \alpha = d-1.$$

41.24 Corollary By Theorem 41.19 there exist partial geometries with parameters as follows:

Type 1: $s = 2^h - 2^m,\ t = 2^h - 2^{h-m},\ \alpha = (2^{h-m}-1)(2^m-1)$ with $1 \le m < h$;
Type 2: $s = 2^h - 1,\ t = (2^h+1)(2^m-1),\ \alpha = 2^m - 1$ with $1 \le m < h$.

Such a partial geometry has $\alpha = 1$ or is proper. A partial geometry of Type 1 is a generalized quadrangle if and only if $h = 2$ and $m = 1$; then $s = t = 2$ and $v = b = 15$. A partial geometry of Type 2 is a generalized quadrangle if and only if $m = 1$; then K is a hyperoval in $\mathcal{P}$, $s = 2^h - 1, t = 2^h + 1, v = 2^{3h}, b = 2^{2h}(2^h+2)$ with $h \ge 2$.

41.4 Partial Geometries in Projective and Affine Spaces

41.25 A *projective partial geometry* $\mathcal{S} = (P, B, \mathrm{I})$ is a partial geometry with parameters $s = q, t, \alpha$ for which the point set P is a subset of the point set of some projective space $\mathrm{PG}(n,q)$, for which the line set B is a set of lines of $\mathrm{PG}(n,q)$, and for which I is the natural incidence. In such a case the partial geometry $\mathcal{S}$ is *embedded* in $\mathrm{PG}(n,q)$. If $\mathrm{PG}(n',q)$ is the subspace of $\mathrm{PG}(n,q)$ generated by all points of P, then $\mathrm{PG}(n',q)$ is the *ambient space* of $\mathcal{S}$.

41.26 Similarly one may define an *affine partial geometry* by replacing the projective space $\mathrm{PG}(n,q)$ by the affine space $\mathrm{AG}(n,q)$.

41.27 Theorem [1108] If $\mathcal{S} = (P, B, \mathrm{I})$ is a partial geometry with parameters s, t, α that is projective with ambient space $\mathrm{PG}(n,s), n \ge 2$, then one of the following holds:

1. $\alpha = s+1$ and $\mathcal{S}$ is the 2-design formed by all points and all lines of $\mathrm{PG}(n,s)$;
2. $\alpha = 1$ and $\mathcal{S}$ is a classical generalized quadrangle;

3. $\alpha = t+1, n = 2$, P is the complement of a maximal $\{sd-s+d; d\}$-arc K of $\mathrm{PG}(2,s)$ with $d = s/\alpha$ and $2 \le d < s$, and B consists of all lines of $\mathrm{PG}(2,s)$ having an empty intersection with K;
4. $\alpha = s, n \ge 2$ and $\mathcal{S}$ is the dual net H_s^n.

41.28 Remark Part 2 of Theorem 41.27 is due to Buekenhout and Lefèvre, Parts 1, 3, and 4 to De Clerck and Thas.

41.29 Remark All partial geometries embedded in the affine space $\mathrm{AG}(n,q), n \ge 2$, were determined by Thas [2021]; the three-dimensional case with $\alpha = 1$ was independently settled by Bichara [2021]. For $\alpha = 1$ and $n \ge 3$, five interesting sporadic cases occur [2021].

41.30 Theorem If $\mathcal{S}$ is a proper partial geometry with parameters s, t, α that is affine with ambient space $\mathrm{AG}(n, s+1), n \ge 2$, then $n = 3$ and $\mathcal{S}$ is a partial geometry $\mathcal{T}_2^*(K)$ with K a maximal arc in the plane at infinity of $\mathrm{AG}(3, s+1)$ [2021].

41.5 Enumeration of Partial Geometries

41.31 Theorem Up to duality, the parameters of the known proper partial geometries are the following:

Type 1: $s = 2^h - 2^m, t = 2^h - 2^{h-m}, \alpha = (2^m-1)(2^{h-m}-1)$, with $h \ne 2$ and $1 \le m < h$;
Type 2: $s = 2^h - 1, t = (2^h+1)(2^m-1), \alpha = 2^m - 1$, with $1 < m < h$;
Type 3: $s = 2^{2h-1} - 1, t = 2^{2h-1}, \alpha = 2^{2h-2}$, with $h > 1$;
Type 4: $s = 3^{2m} - 1, t = (3^{4m}-1)/2, \alpha = (3^{2m}-1)/2, m \ge 1$;
Type 5: $s = 26, t = 27, \alpha = 18$;
Type 6: $s = t = 5, \alpha = 2$;
Type 7: $s = 4, t = 17, \alpha = 2$;
Type 8: $s = 8, t = 20, \alpha = 2$.

41.32 Remarks

1. Mathon proved by computer that there exist exactly two partial geometries with parameters $s = 6, t = 4, \alpha = 3$ [644]. For $(s,t,\alpha) \ne (6,4,3)$ all known partial geometries of Type 1 and 2 are given by the constructions of §41.3.
2. With each partition by $(2h-1)$-dimensional spaces (maximal singular subspaces) of the hyperbolic quadric $Q^+(4h-1,2)$ of $\mathrm{PG}(4h-1,2), h > 1$, there corresponds a partial geometry of Type 3; no other partial geometries with these parameters are known. The geometries of Type 3 are due to De Clerck, Dye, and Thas; for $h = 2$ the geometry was also constructed by Cohen, and by Haemers and van Lint (the three constructions are completely different) [644].
3. The partial geometries of Type 4 are due to Mathon [1541]; their strongly regular graphs arise from the hermitian two-graph.
4. With each partition by $(2h-1)$-dimensional spaces of the hyperbolic quadric $Q^+(4h-1,3)$ of $\mathrm{PG}(4h-1,3), h > 1$, there corresponds a partial geometry with parameters $s = 3^{2h-1} - 1, t = 3^{2h-1}, \alpha = 2.3^{2h-2}$. Up to now only $Q^+(7,3)$ is known to have such a partition; this yields the geometry of Type 5. This construction is due to Thas [644].
5. Spread derivation introduced by De Clerck [642] (generalizing [1552]) yields many nonisomorphic partial geometries having the same parameters of the partial geometries of Type 3 and Type 5.

6. The geometry of Type 6 is due to van Lint and Schrijver, the geometry of Type 7 to Haemers, and the geometry of Type 8 to Mathon; one geometry of each type is known [643, 644].

41.33 Table The parameters of possible partial geometries (PG) with $v < 100$, excluding designs and nets and their duals; of a dual pair, the one with $s \le t$ is given. All conditions in §41.2 are taken into account.

v	s	t	α	b	Comment
15	2	2	1	15	Unique PG exists [1723]
27	2	4	1	45	Unique PG exists [1723]
28	3	4	2	35	Does not exist [644]
40	3	3	1	40	Exactly two PG exist [1723]
45	4	6	3	63	Exactly two PG exist; Remark 41.32 (1)
64	3	5	1	96	Unique PG exists [1723]
66	5	8	4	99	Does not exist, Lam et al. [644]
70	6	6	4	70	Unknown
75	4	7	2	120	Unknown
76	3	6	1	133	Does not exist, Dixmier and Zara [1723]
81	5	5	2	81	One PG known; Remark 41.32 (6)
85	4	4	1	85	Unique PG exists [1723]
91	6	10	5	143	Unknown
95	4	9	2	190	Unknown
96	5	6	2	112	Unknown
96	5	9	3	160	Unknown

41.34 Remark For $v = 70$ and $v = 91$ pseudo-geometric graphs are known; for $v \in \{75, 96\}$ no pseudo-geometric graph is known.

See Also

§II.5	Partial geometries with $\alpha = s + 1$ are Steiner systems.
§III.3	Partial geometries with $\alpha = s$ are transversal designs; partial geometries with $\alpha = t$ are nets.
§VI.1	Pseudo-geometric graphs are particular association schemes.
§VI.23	Partial geometries with $\alpha = 1$ are generalized quadrangles.
§VII.11	Pseudo-geometric graphs are particular strongly regular graphs.
§VII.13	Two-graphs are used to construct partial geometries.
§VII.2	Classical geometries and nondesarguesian planes are used to construct partial geometries.
[348]	Excellent survey, without proofs, with extensive bibliography of strongly regular graphs and partial geometries.
[644]	A survey, without proofs, with extensive bibliography. This survey contains most of the information in this chapter.
[1105]	Contains extensive information on maximal arcs.
[1108]	Contains a section on projective partial geometries.
[1229]	Excellent survey on translation nets.
[1723]	Standard reference on generalized quadrangles.
[2021]	Determination of all affine partial geometries.
[2024]	Contains a survey of maximal arcs.

References Cited: [151, 348, 420, 642, 643, 644, 1027, 1105, 1108, 1229, 1541, 1542, 1552, 1723, 2021, 2024, 2026]

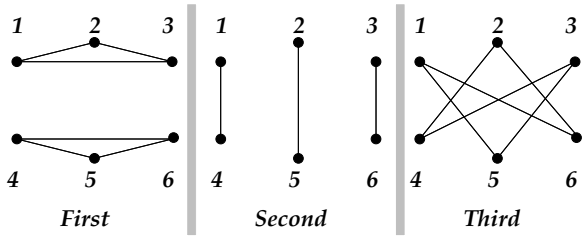
42 Partially Balanced Incomplete Block Designs

Deborah J. Street
Anne Penfold Street

42.1 Definitions and Examples

42.1 Let X be a v-set with a symmetric association scheme defined on it. A *partially balanced incomplete block design with m associate classes* (PBIBD(m)) is a design based on the v-set X with b blocks, each of size k, and with each treatment appearing in r blocks. Any two treatments that are ith associates appear together in λ_i blocks of the PBIBD(m). The numbers $v, b, r, k, \lambda_i (1 \le i \le m)$ are the *parameters* of the PBIBD(m). One writes PBIBD(v, k, λ_i) and lets N be the $v \times b$ (0,1) incidence matrix of the PBIBD(m).

42.2 Example Let $v = 6, b = 8, r = 4, k = 3, \lambda_1 = \lambda_2 = 2, \lambda_3 = 1$. Associate classes are shown as adjacencies in the following diagram.



Consider the design that contains the blocks $\{1,2,4\}, \{1,2,5\}, \{1,3,4\}, \{1,3,6\}$, $\{2,3,5\}$, $\{2,3,6\}$, $\{4,5,6\}$, $\{4,5,6\}$. Even though $\lambda_1 = \lambda_2$, the first and second associate classes cannot be combined since if they could, then 1 would have first associates 2, 3, and 4; 2 would have first associates 1, 3, and 5; 4 would have first associates 1, 5, and 6. Then $p_{11}^1 = 1$ for first associates 1 and 2, and is 0 for first associates 1 and 4. But this number must be a constant, from the definition of an association scheme. See §VI.1 for definitions pertaining to association schemes.

42.3 Remarks

1. PBIBDs were introduced as generalizations of BIBDs because of the ease of analysis. BIBDs are universally optimal designs. The optimality of some PBIBD(2)s is established in [489].
2. The structure that the association scheme imposes on the treatments is not necessarily an inherent attribute of the treatments, as is the case in a factorial design; see §VI.21.
3. A PBIBD(m) determines an association scheme, but the converse is not true.
4. A PBIBD(1) is a BIBD, and a PBIBD(2) in which $\lambda_1 = \lambda_2$ is a BIBD.
5. [1242] gives conditions for a PBIBD(m), with $\lambda_i = \lambda_j$, to become a PBIBD($m-1$).
6. PBIBDs are used in plant breeding work (see [631, 896]), in survey sampling [1869], and in group testing (see [2083] and §VI.46).

42.4 Theorem [1984] Let $A_0, \ldots, A_m$ be the matrices of an association scheme corresponding to a PBIBD(m). Then $NN^T = rI + \sum_i \lambda_i A_i$ and $JN = kJ$. Conversely, if N

is a (0,1) matrix that satisfies these conditions and the A_i are the matrices of an association scheme, then N is the incidence matrix of a PBIBD(m). See §VI.1.

42.5 Theorem [1984] Let each treatment in a PBIBD(m) have n_i ith associates, $1 \le i \le m$. Then the parameters of a PBIBD(m) satisfy $vr = bk$ and $\sum_i n_i\lambda_i = r(k-1)$, while the parameters of an association scheme satisfy $\sum_i n_i = v-1$, $\sum_u p^h_{ju} = n_j$, and $n_i p^i_{jh} = n_j p^j_{ih}$.

42.2 Two-Associate-Class PBIBDs

42.6 There are six types of PBIBD(2)s, based on the underlying association scheme. These are (see [513]) 1. group divisible, 2. triangular, 3. latin-square-type, 4. cyclic, 5. partial geometry type, and 6. miscellaneous.

42.7 Remarks

1. The GDDs of §IV.1 are PBIBD(2)s with $\lambda_1 = 0$ and $\lambda_2 = \lambda$.
2. The duals of the residual designs of symmetric BIBDs with $\lambda = 2$ are PBIBD(2)s; see Theorem 42.16 and §II.6.

42.8 Theorem [1984] Let N be the incidence matrix of a PBIBD($v, k, \lambda_1, \lambda_2$). Let $\gamma = p^2_{12} - p^1_{12}$, $\beta = p^2_{12} + p^1_{12}$, $\delta = \gamma^2 + 2\beta + 1$. Then the eigenvalues of NN^T are rk and $\theta_i = r + ((\lambda_1 - \lambda_2)(\gamma + (-1)^i\sqrt{\delta}) - (\lambda_1 + \lambda_2))/2$, $i = 1, 2$, with multiplicities 1 and $\alpha_i = (n_1 + n_2)/2 + (-1)^i((n_1 - n_2) - \gamma(n_1 + n_2))/(2\sqrt{\delta})$, $i = 1, 2$, respectively.

▷ Group Divisible PBIBDs

42.9 Let the v-set X be partitioned into m groups each of size n. Then in a *group divisible association scheme* the first associates are the treatments in the same group and the second associates are all the other treatments. The eigenvalues of NN^T are rk, $r - \lambda_1$, and $rk - v\lambda_2$ with multiplicities 1, $m(n-1)$, and $m-1$, respectively. A group divisible PBIBD is *singular* if $r = \lambda_1$; *semi-regular* if $r > \lambda_1$, $rk - v\lambda_2 = 0$; and *regular* if $r > \lambda_1$ and $rk > v\lambda_2$.

42.10 Remark In group divisible PBIBDs neither λ need be 0.

42.11 Examples A BIBD(7,3,1), a singular group divisible PBIBD(21,9,3,1) obtained by replacing each element of the BIBD by a set of three elements, and a semi-regular group divisible PBIBD(6,3,0,1) with groups obtained from the blocks of the BIBD containing 7.

BIBD	PBIBD(21,9,3,1)	PBIBD(6,3,0,1)
{1, 2, 4}	{1, 8, 15, 2, 9, 16, 4, 11, 18}	{1, 2, 4}
{2, 3, 5}	{2, 9, 16, 3, 10, 17, 5, 12, 19}	{2, 3, 5}
{3, 4, 6}	{3, 10, 17, 4, 11, 18, 6, 13, 20}	{3, 4, 6}
{4, 5, 7}	{4, 11, 18, 5, 12, 19, 7, 14, 21}	
{5, 6, 1}	{5, 12, 19, 6, 13, 20, 1, 8, 15}	{5, 6, 1}
{6, 7, 2}	{6, 13, 20, 7, 14, 21, 2, 9, 16}	
{7, 1, 3}	{7, 14, 21, 1, 8, 15, 3, 10, 17}	

42.12 Theorems [1770, 1984]

1. The parameters of a group divisible association scheme uniquely determine the scheme.
2. The existence of a singular group divisible PBIBD($mn, kn, \lambda_1 = r, \lambda_2 = \lambda$) is equivalent to the existence of a BIBD(m, k, λ).

3. In a semi-regular group divisible PBIBD, every block has k/m treatments from each group.
4. The dual of an affine resolvable BIBD$(ak, a(c(a-1)+1), ac+1)$ is a semi-regular group divisible PBIBD with $v = a(ca^2+a+1), b = a^2(c(a-1)+1), r = a(c(a-1)+1), k = a^2c+a+1, m = a^2c+a+1, n, \lambda_1 = 0, \lambda_2 = c(a-1)+1$.
5. Given a BIBD$(v, k, 1)$, then there exists a group divisible PBIBD$(v-1, k, 0, 1)$.

42.13 Remarks

1. Difference methods can be used to construct group divisible PBIBDs; see §VI.16.
2. The rectangular association scheme [1770] and the extended group divisible association scheme [449, 1770] are generalizations of the group divisible scheme. Both are examples of the factorial association scheme; see [136, 997].

▷ Triangular PBIBDs

42.14 Let $v = n(n-1)/2, n \geq 5$, and arrange the v elements of X in a symmetrical $n \times n$ array with the diagonal entries blank. In the *triangular association scheme* the first associates of a treatment are those in the same row or column of the array; all other treatments are second associates.

42.15 Example The triangular scheme with $n = 6$ and a triangular PBIBD with $v = b = 15, r = k = 3, \lambda_1 = 0, \lambda_2 = 1$. This is design T16 in [513].

Array					
*	1	2	3	4	5
1	*	6	7	8	9
2	6	*	10	11	12
3	7	10	*	13	14
4	8	11	13	*	15
5	9	12	14	15	*

PBIBD		
$\{1, 10, 15\}$	$\{15, 3, 6\}$	$\{5, 6, 13\}$
$\{11, 1, 14\}$	$\{8, 12, 3\}$	$\{7, 5, 11\}$
$\{12, 13, 1\}$	$\{3, 11, 9\}$	$\{10, 8, 5\}$
$\{2, 15, 7\}$	$\{6, 14, 4\}$	$\{13, 9, 2\}$
$\{14, 2, 8\}$	$\{4, 7, 12\}$	$\{9, 4, 10\}$

42.16 Theorems [1984] (1) The parameters of the triangular association scheme uniquely determine the scheme for $n \neq 8$. (2) If a symmetric BIBD$((n^2+3n+4)/2, n+2, 2)$ exists, then so does a triangular PBIBD with parameters $v = (n+1)(n+2)/2, b = n(n+1)/2, r = n, k = n+2, \lambda_1 = 1, \lambda_2 = 2$.

42.17 Remarks

1. There are three pseudo-triangular association schemes when $n = 8$; see [1770, 1984].
2. Triangular schemes and generalized triangular schemes are also known as Johnson schemes; see §VI.1.
3. The triangular scheme arises in diallel cross experiments in which the treatments are the crosses of n genotypes, there are no self-crosses, and the crosses (AB) and (BA) are not distinguished. First associates are then those that have one parental genotype in common [631, 896].

▷ Latin-Square-Type PBIBDs

42.18 Let $v = n^2$ and arrange the v treatments in an $n \times n$ array. Superimpose on this array a set of $i-2$ mutually orthogonal latin squares of order n. Let the first associates of any treatment be those in the same row or column of the array or associated with the same symbols in one of the latin squares. This is an *L_i-type association scheme*. If $i = n$, then the scheme is group divisible; if $i = n+1$, then all the treatments are first associates of each other.

42.19 Example Let $n = 4$. Then $v = 16$ and an L_3-type PBIBD(2) with $b = 16$, $r = k = 3$, $\lambda_1 = 0$ and $\lambda_2 = 1$ is given. It is design LS18 of [513].

Square			
1	2	3	4
4	1	2	3
3	4	1	2
2	3	4	1

PBIBD			
$\{10, 7, 16\}$	$\{7, 9, 4\}$	$\{13, 4, 6\}$	$\{2, 16, 9\}$
$\{11, 8, 13\}$	$\{8, 10, 1\}$	$\{14, 1, 7\}$	$\{3, 13, 10\}$
$\{12, 5, 14\}$	$\{5, 11, 2\}$	$\{15, 2, 8\}$	$\{4, 14, 11\}$
$\{9, 6, 15\}$	$\{6, 12, 3\}$	$\{16, 3, 5\}$	$\{1, 15, 12\}$

42.20 Remark $L_2(n)$ is also the 2-dimensional Hamming scheme; see §VI.1.

▷ Cyclic PBIBDs

42.21 Let $\{1, 2, \ldots, v-1\} = D \cup E$. A non-group divisible association scheme defined on $\mathbb{Z}_v$ is *cyclic* if $D = -D$, and if the set of $n_1(n_1 - 1)$ differences of distinct elements of D has each element of D p_{11}^1 times and each element of E p_{11}^2 times. The first associates of i are $i + D$.

42.22 Example Let $v = 17$, $D = \{3, 5, 6, 7, 10, 11, 12, 14\}$. Then the initial blocks {0,1,4,5} and {1,8,10,16} developed modulo 17 give a PBIBD(17,4,1,2).

42.23 Remark [1630] uses an optimization approach to construct cyclic PBIBDs.

▷ Partial-Geometry-Type PBIBDs

42.24 In a *partial-geometry-type association scheme*, two treatments are first associates if they are incident with a line of the geometry and second associates if they are not incident with a line of the geometry.

42.25 Remarks

1. Using the notation of §VI.41, if a partial geometry with parameters s, t, and α exists, then so does a PBIBD(2) with parameters $v = (s+1)(ts+\alpha)/\alpha$, $b = (t+1)(ts+\alpha)/\alpha$, $r = t+1$, $k = s+1$, $\lambda_1 = 1$, and $\lambda_2 = 1$; see [513].
2. A partial geometry with $\alpha = t$ is a PBIBD(2) with $k = r$ and $t+1$ replicates based on a L_{t+1} type association scheme, or a lattice design with $t+1$ replicates; see [513].

See Also

§II.1	BIBDs are PBIBD(1)s.
§III.6	More on affine resolvable designs.
§IV.4	GDDs form a class of PBIBDs.
§VI.1	Association schemes underlie PBIBDs.
§VI.41	Partial geometries underlie some PBIBDs.
§VI.46	PBIBDs are used in group testing.
[513]	Extensive tables of PBIBD(2)s.
[137]	Most recent overview of association schemes and related PBIBDs.
[999, 1639]	Extend nested row-column designs to PBIBDs.
[1984]	Chapter 11 gives a description of two class PBIBDs and contains proofs of most of the material in this chapter (and more).

References Cited: [136, 137, 449, 489, 513, 631, 896, 997, 999, 1242, 1630, 1639, 1770, 1869, 1984, 2083]

43 Perfect Hash Families

Robert A. Walker II
Charles J. Colbourn

43.1 Definitions and Applications

43.1 A *t-perfect hash family* $\mathcal{H}$, denoted PHF$(n; k, q, t)$, is a family of n functions $h : A \mapsto B$, where $k = |A| \geq |B| = q$, such that for any subset $X \subseteq A$ with $|X| = t$, there is at least one function $h \in \mathcal{H}$ that is injective on X. Thus, a PHF$(n; k, q, t)$ can be viewed as an $n \times k$-array $\mathcal{H}$ with entries from a set of q symbols such that for any set of t columns, there is at least one row having distinct entries in this set of columns.

43.2 **Remark** A perfect hash family can exist only for $q \geq t$.

43.3 **Examples** A PHF(6;12,3,3) and a PHF(8;8,6,6).

PHF(6;12,3,3):

1	0	0	2	2	2	1	1	2	1	0	2
2	0	1	1	2	0	2	0	1	1	2	1
2	0	2	1	2	1	0	2	2	1	1	0
0	1	2	2	1	2	2	0	1	1	0	0
2	0	1	2	1	1	2	2	0	1	2	1
0	2	1	0	2	2	2	1	0	1	2	1

PHF(8;8,6,6):

4	3	5	0	1	4	2	2
4	5	1	1	3	4	0	2
5	1	3	2	2	4	0	3
5	0	1	0	2	3	1	4
2	5	1	2	5	4	3	0
4	2	2	0	3	5	1	1
0	1	4	2	5	3	3	5
0	0	2	1	5	5	4	3

43.4 The smallest possible size of a perfect hash family is the *perfect hash family number* PHFN(k, q, t). A perfect hash family is *optimal* if it contains the minimum possible number of rows.

43.5 $\rho(N; v, t)$ is the largest k for which PHFN$(k, v, t) \leq N$.

43.6 **Remark** Mehlhorn introduced perfect hash families in 1984 [1584] as an efficient tool for the compact storage and fast retrieval of frequently used information, such as reserved words in programming languages or command names in interactive systems. Perfect hash families, and a variation known as "separating hash familes," can be used to construct separating systems, key distribution patterns, group testing algorithms, cover-free families, and secure frame proof codes [1974]. Perfect hash families have also recently found increasing applications in cryptography, specificially in the areas of broadcast encryption and threshold cryptography.

43.2 Constructions

43.7 **Theorems** (see [2103])

1. PHFN$(q, q, t) = 1$;
2. PHFN$(k, q, 2) = \log_q k$;
3. For $s \geq 1$, $m \geq 2$, PHFN$(ms + m, ms + 1, 2s + 1) = s + 1$.

43.8 Theorem (see [1978]) Suppose that there exists a q-ary code $\mathcal{C}$ of length K, with N codewords, having minimum distance D. Then there exists a PHF$(N; K, q, t)$, where $(N-D)\binom{t}{2} < N$.

43.9 Corollary (see [1978]) Suppose N and v are given, with v a prime power and $N \le v+1$. Then there exists a PHF$(N; v^{\lceil N/\binom{t}{2}\rceil}, v, t)$ based on a Reed–Solomon code.

43.10 Theorem [2073] For any prime power $v \ge 3$ and any $i \ge 1$, there exists a PHF$((i+1)^2; v^{i+1}, v, 3)$. For any prime power $v \ge 4$ and any $i \ge 1$, there exists a PHF$(\frac{5}{6}(2i^3+3i^2+i)+i+1; v^{i+1}, v, 4)$.

43.11 Theorem [1978] Suppose there are at least $s = \binom{t}{2} - 1$ MOLR (see Table III.3.118) of size $m \times n$. Then there exists a PHF$(s+2; mn, n, t)$. Particularly, if there are at least s MOLS of order n, there exists a PHF$(s+2; n^2, n, t)$. For $n \ge 3$ and $n \ne 6$, this gives a PHF$(4; n^2, n, 3)$. When $n = 4$ or $n \ge 7$, this is known to be optimal.

43.12 Theorem [1978] For any prime power q and for any positive integers n, m, i such that $n \ge m$ and $2 \le i \le q^n$, there exists a PHF$(q^n; q^{m+(i-1)n}, q^m, t)$ when $\binom{t}{2} < \frac{q^m}{i-1}$.

43.13 Remark The construction in Theorem 43.12 is based on orthogonal arrays from [255]. A more in-depth discussion of the use of orthogonal arrays to create perfect hash families can be found in [1978].

43.14 Theorem (see [1978]) There exists a PHF$(6; p^2, p, 3)$ for $p = 11$ or prime $p \ge 17$.

43.15 Theorem (see [2103]) For every integer $a \ge 2$, there exists a PHF(t, a^t, a^{t-1}, t).

43.16 Theorem [125] Suppose there exists an RBIBD(v, k, λ), where $r > \lambda\binom{t}{2}$. Then there exists a PHF$(r; v, \frac{v}{k}, t)$.

43.17 Theorem (see [1978]) Suppose there exist PHF$(N_0; k, x, t)$ and PHF$(N_1; x, q, t)$. Then there exists a PHF$(N_0 N_1; k, q, t)$.

43.18 Theorem [125] Suppose that a PHF$(N_1; k_0 k_1, q, t)$, a PHF$(N_2; k_2, k_1, t-1)$, and a PHF$(N_3; k_2, q, t)$ all exist. Then there is a PHF$(N_1 N_2 + N_3; k_0 k_2, q, t)$.

43.19 Theorems [2103] *Symbol increase:* PHFN$(k, q, t) \le$ PHFN$(k-1, q-1, t)$.
Symbol product: For $\ell \ge 1$ an integer, PHFN$(k\ell, q\ell, t) \le$ PHFN(k, q, t).
Column increase: (a) PHFN$(k+q-2, q, 3) \le$ PHFN$(k, q, 3) + 1$.
(b) For $t > 3$, PHFN$(k+1, q, t) \le$ PHFN$(k, q, t) +$ PHFN$(k-1, q-2, t-2)$.

43.20 Theorems [2103] Roux-type constructions:

1. PHFN$(2k, 4, 4) \le$ PHFN$(k, 4, 4) + 3$PHFN$(k, 3, 3) +$ PHFN$(k, 2, 2)$.
2. PHFN$(k\ell, q, t) \le$ PHFN$(k, q, t) +$ PHFN$(k, \lfloor \frac{q}{\ell} \rfloor, t-1)$ whenever $\ell(t-1) \le q$.
3. For q odd or a prime power,
PHFN$(k\ell, q, 3) \le$ PHFN$(k, q, 3) +$ PHFN$(\ell, q, 3) + 2$PHFN$(\ell, q, 2)$PHFN$(k, q, 2)$.

43.3 Tables

43.21 Remark Extensive tables with additional navigation and ranking features can be found at `http://www.phftables.com`.

43.22 Table The authorities used in Table 43.23.

b	Theorems 43.7 (Basics)	c	Theorem 43.17 (Composition)
i	Theorem 43.10	k	Theorem 43.18 (Kronecker-type Product)
m	Theorem 43.11 (MOLS)	r	Theorems 43.20 (Roux-type)
t	Tabu search result [2103]	$+$	Theorems 43.19 (Column Increase)

43.23 Table Known lower bounds on $\rho(N; v, t)$ for small parameters. Entries are of the form "$\underline{k}$ N^{α}". Select the smallest $\underline{k}$ for which $\underline{k} \geq k$, and let N be the corresponding size. Then $\mathrm{PHFN}(k, v, t) \leq N$, and the construction to establish this is specified by the authority α (given in Table 43.22).

$\rho(N;3,3)$					
3	1^b	4	2^b	6	3^r
9	4^m	10	5^+	12	6^t
16	7^t	19	8^t	27	9^i
29	10^t	30	11^+	36	12^c
37	13^+	48	14^r	57	15^r
81	16^i	82	17^+	83	18^+
87	19^r	100	20^c	108	21^r
111	22^r	144	23^r	171	24^r
243	25^i	244	26^+	245	27^+

$\rho(N;4,4)$					
4	1^b	5	3^+	6	5^t
8	6^t	9	8^t	10	12^+
11	16^+	12	17^k	16	21^r
18	24^r	19	29^+	20	31^r
21	36^+	22	38^r	24	39^r
27	40^c	64	42^c	65	48^+
66	55^+	81	56^c	82	63^+
83	70^+	84	77^+	85	84^+
96	89^k	128	96^c	130	103^r

$\rho(N;5,5)$					
5	1^b	6	3^t	7	6^t
8	8^t	9	11^t	10	13^t
11	18^t	12	23^t	13	28^t
14	35^+	15	42^+	16	49^+
17	56^+	18	64^+	19	72^+
20	78^k	21	87^+	22	96^k
23	105^+	24	114^+	27	121^c
28	130^+	29	140^+	30	150^+
31	161^+	40	169^c	41	183^c

$\rho(N;6,6)$					
6	1^b	7	4^t	8	8^t
9	13^t	10	18^t	11	30^+
12	46^+	13	63^+	14	84^+
15	105^+	16	126^+	17	147^+
18	171^+	19	195^+	20	224^+
21	255^+	22	291^+	23	329^+
24	368^+	25	407^+	26	447^+
33	480^c	34	522^+	35	564^+
36	606^+	37	648^+	38	690^+

See Also

§II.7	RBIBDs are used to make PHFs.
§III.3	MOLS and MOLR are used to make PHFs.
§VI.10	Covering arrays are made using perfect hash families.
§VII.1	Codes with large distance are used to make PHFs.
[125]	A discussion of lower bounds.
[1972]	Applications in cryptography.

References Cited: [125, 255, 1584, 1972, 1974, 1978, 2073, 2103]

44 Permutation Codes and Arrays

Peter J. Dukes

44.1 Definitions and Examples

44.1 Let X be a nonempty set of cardinality n. A *permutation code* (or *permutation array*) of length n and minimum distance d, denoted by $\mathrm{PA}(n, d)$ or simply PA, is an $m \times n$ array in which every row contains every symbol of X exactly once and any two distinct rows differ in at least d positions. The *size* of such a PA is the number of rows m. The maximum size of a $\mathrm{PA}(n, d)$ is denoted $M(n, d)$.

44.2 Remarks

1. The ordering of rows of a PA(n, d) is immaterial; a PA(n, d) is often presented as a set of words of length n forming a code of Hamming distance at least d.
2. $M(n, d) \geq \max\{M(n-1, d), M(n, d+1)\}$.
3. By taking all possible permutations as rows, $M(n, 1) = M(n, 2) = n!$.
4. From a latin square of order n, $M(n, n) = n$.

44.3 Example [700] $M(6, 5) = 18$. The following is a PA$(6, 5)$ of size 18.

125634	142365	164523	236514	251346	316425
354612	362154	413562	426351	435126	461235
512643	534261	546132	623145	631452	645213

44.2 Miscellaneous Results

44.4 Theorem $M(n, d) \leq nM(n-1, d)$. Therefore, $M(n, d) \leq n!/(d-1)!$.

44.5 Theorem Distinct permutations in the alternating group A_n have minimum distance 3. Therefore, $M(n, 3) = n!/2$.

44.6 Theorem [557] Suppose there exist k MOLS of order n. Then $M(n, n-1) \geq kn$.

44.7 Theorem [506] Suppose there are disjoint PA$(n_1, 4)$ of sizes $s_1, \ldots, s_p$ and disjoint PA$(n_2, 4)$ of sizes $t_1, \ldots, t_p$. If c is the size of a binary code of length $n = n_1 + n_2$, distance 4, and constant weight n_1, then there is a PA$(n, 4)$ of size $c\sum_{j=1}^{p} s_j t_j$.

44.8 Theorem Let D_k be the number of derangements of order k. Then

$$\frac{n!}{\sum_{k=0}^{d-1} \binom{n}{k} D_k} \leq M(n, d) \leq \frac{n!}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k} D_k}.$$

44.3 Algebraic Constructions

44.9 Let $\mathbb{F}_q$ be a finite field of order q. A polynomial f over $\mathbb{F}_q$ is a *permutation polynomial* if the mapping it defines is one-to-one. The number of permutation polynomials over $\mathbb{F}_q$ of degree l is denoted $N_l(q)$.

44.10 Remark See [1448] for a survey of results on $N_l(q)$ and §VI.45 for a summary of results on permutation polynomials.

44.11 Theorem [506] Let q be a prime power. Then $M(q, d) \geq \sum_{l=1}^{q-d} N_l(q)$.

44.12 Corollary If q is a prime power, then $M(q, q-1) = q(q-1)$.

44.13 Corollary [506] Let $n = 2^k$ with k odd. Then

1. $M(n, n-3) \geq (n+2)n(n-1)$, and
2. $M(n, n-4) \geq n(n-1)(n^2+3n+8)/3$.

44.14 A group G acting on a set X is *sharply k-transitive* if, for any two k-tuples u, v of distinct points of X, there is a unique $g \in G$ such that $gu = v$.

44.15 Theorem Let G be a sharply k-transitive group acting on an n-set X. For any permutation w of X, the set of words $\{g \cdot w : g \in G\}$ is a PA$(n, n-k+1)$ of maximum size $n!/(n-k)!$.

44.16 Corollary [700]

1. If q is a prime power, then $M(q+1, q-1) = (q+1)q(q-1)$ (from PGL$(2, q)$);

2. $M(11,8) = 11 \cdot 10 \cdot 9 \cdot 8$ (from the *Mathieu group* M_{11}, see §VII.9);
3. $M(12,8) = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ (from M_{12}).

44.4 Constant Composition Codes

44.17 A k-ary code C of length n and distance d on the alphabet $\{1,\ldots,k\}$ has *constant composition* $[n_1,\ldots,n_k]$ if every codeword in C has exactly n_i occurrences of symbol i for $i = 1,\ldots,k$. Denote such a code by CCC$([n_1,\ldots,n_k],d)$.

44.18 Remarks

1. CCCs are a common generalization of constant weight binary codes and PAs.
2. Various constructions for CCCs use design-theoretic techniques.

44.19 Example The set of cyclic shifts of the codeword $1234\ldots kk\ldots432$ form a (largest possible) CCC$([1,2,2,\ldots,2],2k)$ of size $2k+1$.

44.5 Equidistant Permutation Arrays

44.20 A PA(n,d) in which any two distinct rows differ in exactly d positions is an *equidistant permutation array* (EPA). The maximum size of an EPA(n,d) is denoted $M'(n,d)$.

44.21 Example $M'(7,6) = 13$. The following is an EPA$(7,6)$ of size 13.

1234567	1325476	1673245	1752634	2654371	7153462	7362541
3251746	3612457	3745261	4356217	5276431	7514236	

44.22 Theorems

1. $M'(n,d) \le M'(n+1,d), M(n,d)$;
2. $M'(n,n) = n, \quad M'(n,1) = 1, \quad M'(n,2) = 2$;
3. [292] For $n \ge 4$, $M'(n,3) = n-1$. For $n \ge 10$, $M'(n,4) = \lfloor \frac{n}{2} \rfloor$;
4. [1513] For $6 \le n \le 23$, $M'(n,5) = \max\{10, \lfloor \frac{n-1}{2} \rfloor\}$.

44.23 Theorem [1084] If there exist $k+2$ mutually orthogonal latin squares of order n, then $M'(n+k+2, n+2) \ge (k+1)n+1$.

44.24 Corollary If q is a prime power, then $M'(2q-1, q+2) \ge (q-1)^2$.

44.25 Remark See [1511] for several related results using latin squares.

44.26 Theorem [1555] If q is a prime power, then $M'(q^2+q+1, q^2+q) \ge q^3+q^2$.

44.27 Theorem [2092] $M'(n,d) \le \max\{M'(d+1,d), \frac{1}{2}(d+2)^2, d^2-5d+7, 2+\lfloor (n-d)/\lceil d/3 \rceil \rfloor\}$.

44.6 Equivalent Combinatorial Designs

44.28 Let X be a set of cardinality v. A *generalized Room square* [*packing*] of *side* n and *index* λ defined on X is an $n \times n$ array F having the following properties:

1. every cell of F contains a subset (possibly empty) of X,
2. each symbol of X occurs once in each row and column of F, and
3. any two distinct symbols of X occur together in exactly [at most] λ cells of F.

Denote such an array by GRS$(n,\lambda;v)$ [GRSP$(n,\lambda;v)$].

44.29 Remark Room squares are GRSs where $\lambda = 1$ and every nonempty cell contains exactly two elements. (See §VI.50.)

44.30 Theorems

1. There exists a GRS$(n, \lambda; v)$ if and only if there exists an EPA$(n, n-\lambda)$ of size v.
2. There exists a GRSP$(n, \lambda; v)$ if and only if there exists a PA$(n, n-\lambda)$ of size v.

44.31 Remark An (r, λ)-design (see §VI.49) [(r, λ)-packing] on v points that admits two orthogonal resolutions (see §II.7.7) is equivalent to an EPA$(r, r-\lambda)$ [PA$(r, r-\lambda)$] of size v.

44.7 Tables

44.32 Table [506] Lower bounds on $M(n, d)$ (bold entries are exact).

$d\backslash n$	4	5	6	7	8	9	10	11	12
4	**4**	**20**	**120**	349	2688	18144	86400	950400	11404800
5		**5**	**18**	77	560	1944	13680	60940	
6			**6**	**42**	**336**	1512	4320	9790	
7				**7**	**56**		**504**		
8					**8**	**72**	**720**	**7920**	**95040**
9						**9**	35	154	
10							**10**	**110**	**1320**
11								**11**	60
12									**12**

44.33 Table Lower bounds on $M'(n, d)$ (bold entries are exact).

$d\backslash n-d$	1	2	3	4	5	6	7	8	9	10	11	12
4	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**6**	**6**	**7**	**7**	**8**
5	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**
6	**13**	**13**	**13**	**13**	**13**	**13**	**13**	**13**	**13**	**13**	**13**	**13**
7	**16**	**16**	17	17	17	17	17	17	17	17	17	17
8	20	20	20	20	20	20	20	20	20	20	20	20
9	27	27	29	36	37	37	37	37	37	37	37	37
10	24	25	33	41	49	50	50	50	50	50	50	50
11	35	35	37	46	55	64	65	65	65	65	65	65
12	40	40	40	40	40	40	40	40	40	40	40	40
13	25	34	45	56	67	78	89	100	101	101	101	101
14	26	37	49	50	50	50	50	50	50	50	50	50
15	28	40	53	66	79	92	105	118	131	144	145	145

See Also

§III.3	MOLS now provide the most efficient constructions of EPAs.
§VI.49	Doubly resolvable (r, λ)-designs are equivalent to certain PAs.
§VI.50	Room squares are equivalent to certain PAs.
§VI.45	Permutation polynomials are useful in constructing PAs.
[2003]	Linear programming upper bounds for PAs and EPAs.
[507]	A brief survey and tables for CCCs.
[506, 557]	Coding theory applications.
[811]	More coding theory applications.

References Cited: [292, 506, 507, 557, 700, 811, 1084, 1448, 1511, 1513, 1555, 2003, 2092]

45 Permutation Polynomials

Gary L. Mullen

45.1 Definition and Examples

45.1 For q a prime power, let F_q denote the finite field containing q elements. A polynomial $f \in F_q[x]$ is a *permutation polynomial* (PP) if the function $f : c \to f(c)$ from F_q into itself is a permutation. Alternatively, $f(x)$ is a PP if the equation $f(x) = a$ has a unique solution for each $a \in F_q$.

45.2 **Remark** The set of all PPs on F_q forms a group under composition modulo $x^q - x$, isomorphic to the symmetric group S_q of order $q!$. For $q > 2$, the group S_q is generated by x^{q-2} and all linear polynomials $ax + b$, and if c is a primitive element in F_q, S_q is generated by $cx, x + 1$, and x^{q-2}.

45.3 **Remark** Given a permutation g of F_q, the unique PP $P_g(x)$ over F_q of degree at most $q-1$ representing the function g can be found by the Lagrange Interpolation formula; in particular

$$P_g(x) = \sum_{a \in F_q} g(a)(1 - (x - a)^{q-1}).$$

45.4 **Remark** If f is a PP and $a \neq 0,\ b \neq 0,\ c \in F_q$, then $af(bx + c)$ is also a PP. By suitably choosing a, b, and c, one can arrange to have f_1 in *normalized form* so that f_1 is monic, $f_1(0) = 0$, and when the degree n of f_1 is not divisible by the characteristic of F_q, the coefficient of x^{n-1} is 0.

45.5 **Remark** Hermite's criterion (Theorem 45.6) can be used to determine if a polynomial $f(x)$ is a PP, and was used to obtain all normalized PPs of degree at most 5 in Table 45.9.

45.6 **Theorem** (Hermite) Let p be the characteristic of F_q. A polynomial $f \in F_q[x]$ is a PP if and only if

1. f has exactly one root in F_q;
2. For each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q - 2$.

45.7 **Remark** A few classes of PPs on F_q.

- *Cyclic*: x^n is a PP on F_q if and only if $(n, q-1) = 1$;
- *Dickson*: For $a \neq 0 \in F_q$, $D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}$ is a PP on F_q if and only if $(n, q^2 - 1) = 1$;
- *Linearized*: $L(x) = \sum_{s=0}^{r-1} a_s x^{q^s} \in F_{q^r}[x]$ is a PP on F_{q^r} if and only if $det(a_{i-j}^{q^j}) \neq 0, 0 \leq i, j \leq r - 1$. These comprise the *Betti–Mathieu group* isomorphic to the group $GL(r, F_q)$ of all nonsingular $r \times r$ matrices over F_q under matrix multiplication;
- For odd q, $f(x) = x^{(q+1)/2} + ax$ is a PP on F_q if and only if $a^2 - 1$ is a nonzero square in F_q.
  - The polynomial $f(x) + cx$ is a PP on F_q for $(q-3)/2$ values of $c \in F_q$.
  - $x^r(f(x^d))^{(q-1)/d}$ is a PP when $(r, q-1) = 1$, d divides $q-1$, and $f(x^d)$ has no nonzero root in F_q.

45.8 Remark Cyclic and Dickson PPs play a vital role in the Schur Conjecture from 1922, which postulated that if f is a polynomial with integer coefficients, that is, a PP of F_p (when considered modulo p) for infinitely many primes p, then f must be a composition of binomials $ax^n + b$ and Dickson polynomials. This holds; see the Notes to Chapter 7 of [1448].

45.9 Table All normalized permutation polynomials of degree at most 5.

Normalized PPs of F_q	q
x	any q
x^2	$q \equiv 0 \pmod 2$
x^3	$q \not\equiv 1 \pmod 3$
$x^3 - ax$ (a not a square)	$q \equiv 0 \pmod 3$
$x^4 \pm 3x$	$q = 7$
$x^4 + a_1x^2 + a_2x$ (if its only root in F_q is 0)	$q \equiv 0 \pmod 2$
x^5	$q \not\equiv 1 \pmod 5$
$x^5 - ax$ (a not a fourth power)	$q \equiv 0 \pmod 5$
$x^5 + ax$ ($a^2 = 2$)	$q = 9$
$x^5 \pm 2x^2$	$q = 7$
$x^5 + ax^3 \pm x^2 + 3a^2x$ (a not a square)	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$ (a arbitrary)	$q \equiv \pm 2 \pmod 5$
$x^5 + ax^3 + 3a^2x$ (a not a square)	$q = 13$
$x^5 - 2ax^3 + a^2x$ (a not a square)	$q \equiv 0 \pmod 5$

45.10 Remark A polynomial f over F_q is *exceptional* if the only absolutely irreducible factors of $f(x) - f(y)$ in $F_q[x, y]$ are scalar multiples of $x - y$. Exceptional polynomials are intimately related to PPs; in fact, any exceptional polynomial is a PP, and the converse holds if q is large compared with the degree of f; see [1425].

45.11 Remark Carlitz conjectured that if f is even, there is a constant C_k so that for each finite field of odd order $q > C_k$, there does not exist a PP of degree k over F_q. This was proved in [832]; in fact, an even stronger result was obtained through the use of powerful group theoretic methods, including the classification of finite simple groups.

45.2 Several Variables

45.12 A polynomial $f \in F_q[x_1, \dots, x_n]$ is a *permutation polynomial (PP) in n variables* if the equation $f(x_1, \dots, x_n) = a$ has q^{n-1} solutions in F_q^n for each $a \in F_q$. More generally, a system $f_1, \dots, f_m \in F_q[x_1, \dots, x_n]$ is an *orthogonal system* if the system of equations $f_i(x_1, \dots, x_n) = a_i, i = 1, \dots, m$ has q^{n-m} solutions in F_q^n for each $(a_1, \dots, a_m) \in F_q^m$.

45.13 Theorem A system $f_1, \dots, f_m \in F_q[x_1, \dots, x_n]$ is an orthogonal system if and only if the polynomial $b_1f_1 + \cdots + b_mf_m$ is a PP in n variables for all nonzero vectors $(b_1, \dots, b_m)$.

45.3 Connections to Designs

45.14 Remark An *orthomorphism* is a mapping θ with $\theta(0) = 0$ so that θ and $\theta(x) - x$ are both PPs of F_q. See §VI.6.1 for connections among orthomorphisms, latin squares, and affine planes.

45.15 Remark For $i \geq 1$, the polynomials $a_1x_1 + \cdots + a_{2i}x_{2i}$ over F_q yield a complete set of mutually orthogonal frequency squares $F(q^i; q^{i-1})$ if neither $(a_1, \ldots, a_i)$ nor $(a_{i+1}, \ldots, a_{2i})$ is the zero vector and $(a'_1, \ldots, a'_{2i}) \neq e(a_1, \ldots, a_{2i})$ for any $e \in F_q^*$. (See §VI.22.) Any such linear polynomial is a PP in $2i$ variables and so the resulting square is an $F(q^i; q^{i-1})$ frequency square, and any two such polynomials form an orthogonal system in $2i$ variables, giving the fact that the squares are orthogonal.

See Also

§VI.6.1	Complete mappings are permutation polynomials.
§VI.22	Permutation polynomials are used to create MOFS.
§VI.44	Permutation polynomials are useful in making permutation arrays.
[1448]	Chapter 7 contains information on permutation polynomials.
[1646, 1648]	Survey papers on permutation polynomials.

References Cited: [832, 1425, 1448, 1646, 1648]

46 Pooling Designs

David C. Torney

46.1 Introduction

46.1 For a long DNA sequence, a *clone library* is formed by partitioning a number of copies of the sequence into shorter, consecutive subsequences, *clones*. The library *coverage* is the number of copies of the original sequence so partitioned. Often a *clone map* linearly orders the clones on the underlying sequence. A *probe* is a short DNA sequence expected to appear at most once in the original sequence. A probe matches a clone (the clone is *positive*) when the probe sequence appears within the clone sequence.

46.2 Remark The Human Genome Project rekindled interest in group testing designs (see §VI.56.4), as a result of their effectiveness for screening large collections of clones to identify all those containing any given DNA sequence (in particular, to locate the probe in the original sequence using the clone map). This application of group testing is *pooling*: clones are mixed to form *pools*. Pooling designs require a variety of additional properties, discussed here.

46.3 Remark Errors abound in pool construction and in the screening experiments. There are false positives and false negatives. Therefore, error correction is essential. Error correction strives to maximize the minimum Hamming distance between pool-incidence vectors for certain sets of positives, such as those with sufficiently large probability of occurrence.

46.4 Remark Optimality criteria for pooling designs often concern their expected behavior, distinguishing them from combinatorial designs [357]. A novel criterion is the *expected number of definite negative clones*, those negative clones in negative pools [357].

46.5 Remark Probabilistic "decoding" (the Markov chain Monte Carlo estimation of the probability that each clone is positive) is well suited to this application [1314]. This technique enables optimization of the pooling design based on, for instance, the average probability of positivity assigned to the positive clones.

46.6 Remark Linear ordering of clones implies that most subsets of the clones cannot correspond to sets of positives [148]. Clones may be different lengths, and sometimes, coordinates for the ends of the clones are known. Designs identifying a bounded number of consecutive positives are proposed in [529, 1837]. Nonadaptive designs are based on Gray codes.

46.7 Theorem [529] Nonadaptive group testing for at most r consecutive positives in a linearly ordered n-set of items can be accomplished with $\mathcal{O}(r + \log_2 n)$ pools.

46.8 Remark The human genome contains "repeated sequences," impacting the distribution of the number of clones containing an arbitrary genomic sequence. The distribution is "heavy tailed"; that is, there is a much greater probability of observing a large number of positive clones than there would be for a binomial distribution. This increases the challenge of implementing nonadaptive pooling designs. Consequently pooling designs should also reveal when the number of positives is too great for determination of the individual positives.

46.9 Theorem [1500] Consider the set $\{1, 2, \ldots, n\}$, and construct a $(0, 1)$-binary matrix M with $\binom{n}{r}$ rows and $\binom{n}{c}$ columns, one-to-one with the corresponding subsets; with $0 < r < c < n$. The entries of the matrix are 1 whenever the corresponding r-subset is included in the specified c-subset. The columns of M specify an r-cover free family on $\{1, 2, \ldots, \binom{n}{r}\}$.

46.10 Remark The principal advantage of the designs in Theorem 46.9 is their ease of construction. Error-correcting variants have also been proposed [1501].

46.11 Remark The collection of clones to be pooled usually resides in rectangular "microtiter" arrays such as 384 clones on a 16×24 array. As a practical matter, pools are constructed by mixing (the clones occurring in) its rows and columns [160]. With ℓ $m \times n$ arrays, consider the sets $\{1, 2, \ldots, \ell m\}$ and $\{1, 2, \ldots, \ell n\}$. Example 46.12 gives a constrained analogue of a t-design which could be constructed from these.

46.12 Example Let each pool contain k_r rows (indexed by $\{1, 2, \ldots, \ell m\}$) and k_c columns (indexed by $\{1, 2, \ldots, \ell n\}$) from the ℓ arrays. The t-subsets of the clones that do not occur together in a row or column are to occur in λ pools, and the $(t + 1)$-subsets of clones that do not occur together in a row or column are to occur in at most one pool. Furthermore, those t-subsets that occur together in a row or column contained in p pools are to occur in $\max(\lambda - p, 0)$ additional pools.

See Also

§VI.56.4	Pooling designs are *biologically motivated* group testing schemes.
[758]	Combinatorial group testing.

References Cited: [148, 160, 357, 529, 758, 1314, 1500, 1501, 1837]

47 Quasi-3 Designs

Gary McGuire

47.1 Definitions and Examples

47.1 A symmetric design $\mathcal{D}$ is a *quasi-3 design* with triple intersection numbers x and y ($x < y$) if any three blocks of $\mathcal{D}$ intersect in either x or y points.

47.2 **Remark** Any symmetric design with $\lambda \leq 2$ is a quasi-3 design with $x = 0$ and $y = 1$.

47.3 **Example** The point-hyperplane design in $PG(n, q)$ is a quasi-3 design with $x = (q^{n-2} - 1)/(q - 1)$ and $y = \lambda = (q^{n-1} - 1)/(q - 1)$.

47.4 **Example** A $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ design with the symmetric difference property (an *SDP design*, see §VII.1.9) is a quasi-3 design with $x = 2^{2m-3} - 2^{m-1}$ and $y = 2^{2m-3} - 2^{m-2}$.

47.5 **Example** Up to isomorphism there are three symmetric designs with parameters $(16, 6, 2)$. All three of these are quasi-3 designs by Remark 47.2, and exactly one is an SDP design.

47.6 A *quasi-3* (v, k, λ, x, y) *design* denotes a quasi-3 (v, k, λ) design with triple intersection numbers x and y.

47.7 **Remark** Sometimes quasi-3 designs are defined dually: A design is *quasi-3* if the number of blocks incident with three points takes two values.

47.8 **Proposition** A design $\mathcal{D}$ is a quasi-3 (v, k, λ, x, y) design if and only if the derived design of $\mathcal{D}$ with respect to *every* block is a $(k, \lambda, \lambda - 1)$ quasi-symmetric design with intersection numbers x and y.

47.9 **Proposition** The complementary design of a quasi-3 (v, k, λ, x, y) design is a quasi-3 $(v, v - k, v - 2k + \lambda, v - 3k + 3\lambda - y, v - 3k + 3\lambda - x)$ design.

47.2 Existence of Quasi-3 Designs

47.10 **Remark** The regular Hadamard (or Menon, see §V.1) designs with parameters $(4u^2, 2u^2 - u, u^2 - u, (u^2 - 2u)/2, (u^2 - u)/2)$ are of interest with regard to quasi-3 designs. The quasi-symmetric derived designs would give self-complementary codes meeting the Grey–Rankin bound (Theorem VII.1.147) [1567]. When $u = 2^{m-1}$, these are the parameters of SDP designs.

47.11 **Theorem** [329] Quasi-3 designs with regular Hadamard parameters $(4u^2, 2u^2 - u, u^2 - u, (u^2 - 2u)/2, (u^2 - u)/2)$ are closed under taking Kronecker products.

47.12 **Conjecture** Quasi-3 designs with parameters $(4u^2, 2u^2 - u, u^2 - u, (u^2 - 2u)/2, (u^2 - u)/2)$ exist for all even u.

47.13 **Remarks**

1. All known quasi-3 designs have the parameters (or complementary parameters) of the examples given so far.

2. There are many non-SDP quasi-3 designs with SDP parameters (see [330, 315]).
3. No examples are known of quasi-3 designs with parameters $(4u^2, 2u^2-u, u^2-u, (u^2-2u)/2, (u^2-u)/2)$ when u is not a power of 2. Examples are known of the quasi-symmetric derived designs.

47.14 Table Parameters where the existence of a quasi-3 design is unknown. Numbers 1 through 11 are all the cases with a value of $v \leq 400$ that are open.

Number	v	k	λ	x	y	Comment
1	144	66	30	12	15	Conjecture 47.12 $u = 6$ case
2	149	37	9	1	3	
3	155	56	20	5	8	
4	205	85	35	10	15	
5	209	65	20	5	8	
6	221	45	9	1	3	Quasi-symmetric derived design exists
7	233	88	33	8	13	
8	237	60	15	3	6	
9	266	106	42	14	18	
10	267	57	12	0	3	Theorem 47.16 (2), $y = 3$ case
11	400	190	90	40	45	Conjecture 47.12 $u = 10$ case
12	1350	285	60	15	10	Possible spin model, see Theorem 47.24

47.3 Classification Results

47.15 Theorem [414] If $\mathcal{D}$ is a quasi-3 design with $y = \lambda$, then $\mathcal{D}$ is isomorphic to $PG(n, q)$ or a projective plane.

47.16 Theorem [414] If $\mathcal{D}$ is a quasi-3 design with $x = 0$ and $\lambda > 2$, then one of the following holds

1. $(v, k, \lambda, x, y) = (2^{n+1}-1, 2^n, 2^{n-1}, 0, 2^{n-2})$ and $\mathcal{D}$ is the complement of $PG(n, 2)$ for some $n \geq 3$, and
2. $(v, k, \lambda, x, y) = (y(y^3+5y^2+6y-1), y(y^2+3y+1), y(y+1), 0, y)$ for some $y \geq 2$.

47.17 Theorem [414] If $\mathcal{D}$ is a quasi-3 Hadamard 2-design, then $\mathcal{D}$ is either $PG(n, 2)$ or the unique $(11, 5, 2)$ design.

47.18 Remark The $y = 2$ case of part 2 of Theorem 47.16 was ruled out by D. Hughes. All values $y > 2$ are an open problem.

47.19 Conjecture A quasi-3 design with $\lambda > 2$ and $y < \lambda$ has parameters $(4u^2, 2u^2-u, u^2-u)$.

47.4 The Dual Design

47.20 Remark In [414] Cameron asked whether the dual design of a quasi-3 design is necessarily a quasi-3 design. The question was answered in the negative by Bracken [315].

47.21 Theorem The dual design of a quasi-3 design with $x = 0$ is a quasi-3 design.

47.22 Theorem [329] If the dual design of a quasi-3 design is quasi-3, it must have the same triple intersection numbers.

47.5 The Connection to Spin Models

47.23 Remark Generalized spin models of a certain type are equivalent to quasi-3 designs of a certain type. For all details see [316]. The smallest open case of a quasi-3 design that would give a spin model is #12 in Table 47.14.

47.24 Theorem A four-weight spin model with two values on W_2 exists if and only if there exists a (v, k, λ) symmetric design $D(X, \mathcal{B})$ satisfying the following three properties:

1. $D(X, \mathcal{B})$ is quasi-3 with triple intersection numbers:
$$x = \frac{k\lambda - k + \lambda - (k-\lambda)\sqrt{k-\lambda}}{v}, \quad y = \frac{k\lambda - k + \lambda + (k-\lambda)\sqrt{k-\lambda}}{v}.$$
2. For any set $\mathcal{S} \subseteq \mathcal{B}$ of four blocks, an even number of the four 3-subsets of $\mathcal{S}$ have triple intersection size x.
3. There exists a bijection $\phi : X \to \mathcal{B}$ with the property that for any three points $a, b, c \in X$, the number of blocks containing $\{a, b, c\}$ is $|\phi(a) \cap \phi(b) \cap \phi(c)|$.

47.25 Remarks

1. The quasi-3 designs corresponding to spin models have not been classified. The SDP designs have been classified, see Theorem 47.26.
2. Condition 2 in Theorem 47.24 is connected to regular two-graphs (see §VI.13).
3. Condition 3 in Theorem 47.24 is satisfied if the design has a polarity.

47.26 Theorem [316] An SDP design $\mathcal{D}$ satisfies all the conditions of Theorem 47.24 and, thus, corresponds to a four-weight spin model, if and only if $\mathcal{D}$ is isomorphic to the symplectic SDP design (see [425]).

See Also

§V.1	Regular Hadamard (Menon) designs.
§VI.48	Necessary conditions for quasi-symmetric designs can be used.
§VII.1.9	SDP designs and the Grey–Rankin bound.
[1170]	Contains proofs of several theorems in this chapter.
[330]	Survey article covering material in this chapter.

References Cited: [315, 316, 329, 330, 414, 425, 1170, 1567]

48 Quasi-Symmetric Designs

Mohan S. Shrikhande

48.1 Definition and Examples

48.1 A t-(v, k, λ) design D is *quasi-symmetric* (q.s.) with intersection numbers x and y $(x < y)$ if any two blocks of D intersect in either x or y points.

48.2 Remark This concept originated in statistics in the investigation of duals of designs with $\lambda = 1$.

48.3 Example Any 2-$(v, k, 1)$ design with $b > v$ is quasi-symmetric with $x = 0$ and $y = 1$.

48.4 Example Let D be a multiple of a symmetric 2-(v, k, λ) design. Then D is quasi-symmetric with $x = \lambda$ and $y = k$.

48.5 Example The unique 3-$(8, 4, 1)$ design (Example II.5.28) is q.s. with $x = 0$ and $y = 2$.

48.6 Remark This is the smallest case of an infinite class of quasi-symmetric designs, known as Hadamard 3-designs (see Example II.6.33). More generally, affine designs provide further examples of quasi-symmetric designs.

48.7 Example Let D be a quasi-residual 2-(v, k, λ) design ($r = k + \lambda$) with $\lambda = 2$. Then D is quasi-symmetric with $x = 1$ and $y = 2$.

48.8 Example The 4-$(23, 7, 1)$ and 3-$(22, 6, 1)$ Witt designs are quasi-symmetric with $x = 1, y = 3$ and $x = 0$, $y = 2$, respectively.

48.2 The Connection to Strongly Regular Graphs

48.9 The *block graph* Γ of quasi-symmetric 2-(v, k, λ) design D is the graph with vertex set being the blocks of D, and where blocks B_i and B_j are adjacent if and only if $|B_i \cap B_j| = y$.

48.10 Theorem Let D be a quasi-symmetric 2-(v, b, r, k, λ) design with intersection numbers x and y. Then Γ is a strongly regular graph with parameters (n, a, c, d) where $n = b$, $a = [k(r-1) - x(b-1)]/(y-x)$, $c = a + \theta_1\theta_2 + \theta_1 + \theta_2$, $d = a + \theta_1\theta_2$, $\theta_1 = (r - \lambda - k + x)/(y - x)$, $\theta_2 = (x - k)/(y - x)$.

48.11 Remark Theorem 48.12 implies that not every strongly regular graph is a block graph of quasi-symmetric design.

48.12 Theorem There is no quasi-symmetric 2-design whose block graph is the lattice graph $L_2(n)$ or its complement.

48.13 Theorem Let D be a quasi-symmetric 2-(v, k, λ) design with intersection numbers x and y. Then

1. $y - x$ divides $k - x$ and $r - \lambda$;
2. $k(r-1)(x+y-1) + xy(1-b) = k(k-1)(\lambda-1)$;
3. if $x = 0$, then $(r-1)(y-1) = (k-1)(\lambda-1)$;
4. if D has no repeated blocks, then $b \leq \binom{v}{2}$, with equality if and only if D is a 4-design;
5. if $x = 0$, then $b \leq v(v-1)/k$, with equality if and only if D is a 3-design.

48.3 Quasi-Symmetric t-Designs (t $\geq$ 3)

48.14 Remark If a symmetric 2-(v, k, λ) design is extendible, then its extension is a quasi-symmetric 3-$(v+1, k+1, \lambda)$ design with $x = 0$ and $y = \lambda + 1$. Any quasi-symmetric 3-design with $x = 0$ is an extension of a symmetric 2-design.

48.15 Theorem If D is a quasi-symmetric 3-(v, k, λ) design with $x = 0$, then $y = \lambda + 1$ and one of the following holds:

1. $v = 4(\lambda+1)$, $k = 2(\lambda+1)$;
2. $v = (\lambda+1)(\lambda^2+5\lambda+5)$, $k = (\lambda+1)(\lambda+2)$; or
3. $v = 496$, $k = 40$, $\lambda = 3$.

48.16 Remark Designs in case 1 of Theorem 48.15 are the Hadamard 3-designs. In case 2, for $\lambda = 1$, it is the unique extension of PG$(2, 4)$ and nothing is known for $\lambda \geq 2$. The existence in case 3 is unknown.

48.17 Theorem If D is a quasi-symmetric 3-(v, k, λ) design with $x = 1$, then D is the 4-$(23, 7, 1)$ design or its residual, the 3-$(22, 7, 4)$ design.

48.18 Theorem If D is a quasi-symmetric 4-(v, k, λ) design, then D is the 4-$(23, 7, 1)$ design or its complement.

48.19 Theorem Quasi-symmetric t-designs do not exist for $t \geq 5$.

48.20 Conjecture All quasi-symmetric 3-designs up to complements are given by Theorems 48.15 and 48.17.

48.4 Quasi-Symmetric Designs and Codes

48.21 Remark The tools of coding theory are important in the study of quasi-symmetric designs. One of the connections is given by Lemma 48.22, which is used to prove Theorem 48.23. See §VII.1 for definitions.

48.22 Lemma Let N be a $b \times v$ incidence matrix of a quasi-symmetric 2-(v, k, λ) design with $k \equiv x \equiv y \pmod 2$.

1. If k is even, then the binary code of length v with generator matrix N is self-orthogonal.
2. Let B be the bordered $b \times (v + 1)$ matrix obtained by adding an extra column of 1s to N. If k is odd, then B generates a binary self-orthogonal code of length $v + 1$.

48.23 Theorem The quasi-symmetric designs 2-$(21, 6, 4)$, $x = 0$, $y = 2$, 2-$(21, 7, 12)$, $x = 1$, $y = 3$, and 2-$(22, 7, 16)$, $x = 1$, $y = 3$ are unique.

48.5 Classifying Quasi-Symmetric 2-Designs

48.24 Remark The classification of quasi-symmetric 2-designs is a difficult open problem. In [1674], four classes of quasi-symmetric designs were distinguished: multiples of symmetric 2-designs, Steiner systems with $v > k^2$, strongly resolvable designs (those quasi-symmetric designs having a complete multipartite block graph), and residuals of biplanes. If a quasi-symmetric design or its complement does not belong to one of these classes, it is referred to as *exceptional*.

48.25 Table An updated table of exceptional quasi-symmetric designs with $2k \leq v \leq 70$. References not given here can be found in [2049].

No.	v	k	λ	r	b	x	y	Existence	Ref.
1	19	7	7	21	57	1	3	No	[1674]
2	19	9	16	36	76	3	5	No	
3	20	10	18	38	76	4	6	No	
4	20	8	14	38	95	2	4	No	
5	21	9	12	30	70	3	5	No	[410]
6	21	8	14	40	105	2	4	No	[410]
7	21	6	4	16	56	0	2	Yes(1)	[2044]
8	21	7	12	40	120	1	3	Yes(1)	[2044]
9	22	8	12	36	99	2	4	No	
10	22	6	5	21	77	0	2	Yes(1)	
11	22	7	16	56	176	1	3	Yes(1)	[2044]
12	23	7	21	77	253	1	3	Yes(1)	
13	24	8	7	23	69	2	4	No	
14	28	7	16	72	288	1	3	No	[2044]
15	28	12	11	27	63	4	6	Yes(≥ 8784)	[1236, 1379, 2044, 710]

No.	v	k	λ	r	b	x	y	Existence	Ref.
16	29	7	12	56	232	1	3	No	[2044]
17	31	7	7	35	155	1	3	Yes(5)	
18	33	15	35	80	176	6	9	?	
19	33	9	6	24	88	1	3	No	
20	35	7	3	17	85	1	3	No	[410]
21	35	14	13	34	85	5	8	?	
22	36	16	12	28	63	6	8	Yes(≥ 8784)	[1235, 1379, 710]
23	37	9	8	36	148	1	3	?	
24	39	12	22	76	247	3	6	?	
25	41	9	9	45	205	1	3	?	
26	41	20	57	120	246	8	11	?	
27	41	17	34	85	205	5	8	No	[410]
28	42	21	60	123	246	9	12	?	
29	42	18	51	123	287	6	9	?	
30	43	18	51	126	301	6	9	No	[410]
31	43	16	40	112	301	4	7	?	
32	45	21	70	154	330	9	13	?	
33	45	9	8	44	220	1	3	Yes(1)	[2044, 1052]
34	45	18	34	88	220	6	9	?	
35	45	15	42	132	396	3	6	?	
36	46	16	72	216	621	4	7	?	
37	46	16	8	24	69	4	6	?	
38	49	9	6	36	196	1	3	Yes(≥ 44)	[1151, 312, 1051]
39	49	16	45	144	441	4	7	?	
40	49	13	13	52	196	1	4	?	
41	51	21	14	35	85	6	9	No	[410]
42	51	15	7	25	85	3	5	No	[410]
43	52	16	20	68	221	4	7	?	
44	55	16	40	144	495	4	8	?	
45	55	15	63	243	891	3	6	?	
46	55	15	7	27	99	3	5	?	
47	56	16	18	66	231	4	8	?	
48	56	15	42	165	616	3	6	?	
49	56	12	9	45	210	0	3	?	
50	56	21	24	66	176	6	9	?	
51	56	20	19	55	154	5	8	?	
52	56	16	6	22	77	4	6	Yes(≥ 2)	[2045, 1659]
53	57	27	117	252	532	12	17	No	[410]
54	57	9	3	21	133	1	3	?	
55	57	15	30	120	456	3	6	?	
56	57	12	11	56	266	0	3	?	
57	57	24	23	56	133	9	12	No	[410]
58	57	21	25	70	190	6	9	?	
59	57	21	10	28	76	7	9	No	[1007]
60	60	15	14	59	236	3	6	?	
61	60	30	58	118	236	14	18	No	
62	61	25	160	400	976	9	13	?	
63	61	21	21	63	183	6	9	?	
64	63	15	35	155	651	3	7	Yes	
65	63	24	92	248	651	8	12	?	
66	63	18	17	62	217	3	6	?	
67	64	24	46	126	336	8	12	Yes	[286]
68	65	20	19	64	208	5	8	?	
69	66	30	29	65	143	12	15	Yes	[317]
70	69	33	176	374	782	15	21	No	[410]
71	69	18	30	120	460	3	6	?	
72	70	10	6	46	322	0	2	?	
73	70	30	58	138	322	10	14	?	

See Also

§VII.1	The tools of coding theory are used in the study of q.s. designs.
§VII.11	The connection to strongly regular graphs is given in Theorem 48.10.
[1899]	A monograph on quasi-symmetric designs and related topics.
[1170]	A monograph on symmetric designs, contains some results on multiples of symmetric designs, quasi-3 designs, and SDP designs.
[329]	Paper on quasi-3 designs and Hadamard matrices. It connects certain q.s. designs, strongly regular graphs, and codes.
[1235, 1236]	Quasi-symmetric designs with the symmetric difference property.
[2044]	Links between quasi-symmetric designs and self-dual codes.
[2049]	For references in Table 48.25.

References Cited: [286, 312, 317, 329, 410, 710, 1007, 1051, 1052, 1151, 1170, 1235, 1236, 1379, 1659, 1674, 1899, 2044, 2045, 2049]

49 (r, λ)-designs

G.H. John van Rees

49.1 Definitions and Example

49.1 An (r, λ)-*design* is a pair $(V, \mathcal{B})$ where V is a set of v elements and $\mathcal{B}$ is a collection of b subsets (*blocks*) of V such that every distinct pair of elements occurs in precisely λ blocks and every element occurs in precisely r blocks. Let $r - \lambda = n$. Let k_i be the size of the ith block in the (r, λ)-design.

49.2 Example A (6,3)-design on 5 elements.

{12345}, {123}, {124}, {135}, {145}, {235}, {245}, {34}, {34}, {1}, {2}, {5}

49.3 A block containing all the elements is a *complete* block. A set of v blocks containing just one element (*singletons* or *singleton blocks*) whose union is V is a *complete set of singletons*.

49.4 An (r, λ)-design that is composed of λ complete blocks and consequently n complete sets of singletons is *trivial*. Nontrivial (r, λ)-designs are (r, λ)-*systems*. Further, if $k_i \geq 2$, the designs are *regular pairwise balanced designs*.

49.5 Designs that contain onlyblocks of cardinality 1, $v-1$, or v are *near-trivial*. An (r, λ)-design that contains a complete block or a complete set of singletons is *reducible*.

49.2 Connections and General Results

49.6 Remarks

1. Any (r, λ)-design can be changed into an $(r+1, \lambda)$-design or an $(r+1, \lambda+1)$-design by the addition of a complete set of singletons or the addition of a complete block, respectively. Often the non-near-trivial or irreducible (r, λ)-designs are the interesting designs.

2. Any pairwise balanced design (PBD) can be made into an (r, λ)-design by the addition of singleton blocks. Resolvable pairwise balanced designs are necessarily (r, λ)-designs (see §IV.1 and see §IV.5.
3. If all the blocks of a nontrivial (r, λ)-design have the same cardinality k, then the design is a (v, b, r, k, λ) BIBD. If v and b of an (r, λ)-design are such that v, b, r, λ could be the parameters of a BIBD, then all blocks have cardinality k and the (r, λ)-design is a BIBD.
4. The incidence matrix of an (r,λ)-design is a binary balanced equidistant $(v,2n,b)$-code.
5. All blocking sets of BIBDs are (r, λ)-designs. A *blocking set* is a set S of points of the design such that any block contains a point of S and a point outside S.
6. Many schedules of sporting events use (r, λ)-designs directly, use their dual, or incorporate an (r, λ)-design as part of their structure.

49.7 Theorem [699] In any (r, λ)-design, $b \geq vr^2/(r + \lambda(v - 1))$ and $k_i(n + \lambda v - \lambda k_i) \leq n(n + \lambda v)$.

49.8 Theorem If an (r, λ)-design is nontrivial, then $v \leq r(r - 1) + 1$ with equality if n is the order of a finite projective plane.

49.9 Theorem For a resolvable (r, λ)-design, $b \geq v + r - 1$. If $b = v + r - 1$, then it is an affine resolvable BIBD with 0, 1, or more complete blocks adjoined.

49.3 Doehlert–Klee Designs (DK designs)

49.10 An (r, λ)-design is *elliptic, parabolic, or hyperbolic* depending whether $\lambda(v - 1) - r(r - 1)$ is less than, equal to, or greater than 0.

49.11 Theorem All irreducible (r, λ)-designs for $\lambda = 1$ or 2 are elliptic or parabolic. This is *not* true for $\lambda \geq 3$.

49.12 A *Doehlert–Klee* (DK) design is an (r, λ)-design with $r^2 = \lambda b$.

49.13 Remarks The duals of DK designs are used as experimental designs. For a given b, $K(b)$ denotes the maximum v such that a DK design exists.

49.14 Table [1561] Lower and upper bounds for undetermined $K(b)$, $b \leq 100$.

b	45	50	54	63	90	98	99
$K(b)$	16–40	26–46	25–51	31–60	28–87	50–95	31–97

49.4 Embedding Results

49.15 Remark [1954] Given any (r, λ)-design, one can obtain a $(2n, n)$-design by complementing certain blocks. If the (r, λ)-design has $v > (n + 2)^2/2$, then an $(n + 1, 1)$-design can be obtained. For this reason most results are proved using $(2n, n)$-designs or $(r, 1)$-designs.

49.16 $v_0(r, \lambda)$ is the least integer such that if D is an (r, λ)-design on v elements with $v > v_0(r, \lambda)$, then D is trivial.

49.17 $v_1(r, \lambda)$ is the least integer such that if D is an (r, λ)-design on v elements with $v > v_1(r, \lambda)$, then D is reducible.

49.18 $v_p(r,1)$ is the largest integer such that there exists a nontrivial $(r,1)$-design D on $v_p(r,1)$ elements in which the number of blocks is less than or equal to n^2+n+1.

49.19 Theorem $v_1(r,\lambda) \le v_0(r,\lambda)$ and $v_p(r,1) \le v_1(r,1)$.

49.20 Theorem $v_0(r,\lambda) \le \max\{n^2+n+1, \lambda+2\}$ with equality if and only if there exists a finite projective plane of order n or $\lambda \ge n^2+n+1$.

49.21 Theorem If n is not the order of a projective plane, then $v_0(r,\lambda) \le \max\{\lambda+2, n^2-a\}$ if $r > 2n$, and $v_0(r,\lambda) \le \max\{\lambda+2, n^2-a-1\}$ if $r \le 2n$, where $n > 2a^2+3a+2$ and a is a positive integer.

49.22 Theorem $v_1(r,\lambda) = n^2+n+1$ if and only if n $(n \ge 3)$ is the order of a finite projective plane and $r = n+1,\ 2n$, or n^2, or if $\lambda = n^3+n^2-n$.

49.23 Theorem $v_0(7,1) = 31$, and $25 \le v_p(7,1) \le 28$.

49.24 Table v_1 for small values of (r,λ).

(r,λ)	(3,1)	(4,2)	(6,3)	(7,4)	(8,5)	(9,6)	(10,7)
$v_1(r,\lambda)$	7	7	13	12	9	13	7

See Also

§IV.1	PBDs that are regular (have constant replication number) are (r,λ)-designs.
§VI.44.5	Equidistant permutation arrays are closely related to (r,λ)-designs.

References Cited: [699, 1561, 1954]

50 Room Squares

Jeffrey H. Dinitz

50.1 Definitions, Examples, and Existence

50.1 Let S be a set of $n+1$ elements (*symbols*). A *Room square* of side n (on symbol set S), RS(n), is an $n \times n$ array, F, that satisfies the following properties:

1. every cell of F either is empty or contains an unordered pair of symbols from S,
2. each symbol of S occurs once in each row and column of F,
3. every unordered pair of symbols occurs in precisely one cell of F.

50.2 A Room square of side n is *standardized* (with respect to the symbol ∞) if the cell (i,i) contains the pair $\{\infty, i\}$.

50.3 A standardized Room square of side n is *skew* if for every pair of cells (i,j) and (j,i) (with $i \ne j$) exactly one is filled.

50.4 A standardized Room square of side n is *cyclic* if $S = \mathbb{Z}_n \cup \{\infty\}$ and if whenever $\{a,b\}$ occurs in the cell (i,j), then $\{a+1, b+1\}$ occurs in cell $(i+1, j+1)$ where all arithmetic is performed in $\mathbb{Z}_n$ (and $\infty + 1 = \infty$).

50.5 Examples Skew Room squares of side 7 and 9. The Room square of side 7 is cyclic.

∞0			15		46	23
34	∞1			26		50
61	45	∞2			30	
	02	56	∞3			41
52		13	60	∞4		
	63		24	01	∞5	
		04		35	12	∞6

∞1		49	37	28		56		
89	∞2				57	34		16
	58	∞3		69	24		17	
	36	78	∞4		19		25	
	79		12	∞5	38		46	
45					∞6	18	39	27
		26	59	13		∞7		48
67	14					29	∞8	35
23		15	68	47				∞9

50.6 Theorem A (skew) Room square of side n exists if and only if n is odd and $n \neq 3$ or 5.

50.7 Theorem [1447] A cyclic skew Room square of side n exists if $n = \prod {p_i}^{\alpha_i}$ where each p_i is a non-Fermat prime or if $n = pq$ with p, q distinct Fermat primes.

50.8 Let R be a skew RS(n) in standard position defined on a set $N \cup \infty$ and let L be the array of pairs formed by the superposition of R and R^T but with main diagonal (i, i) for all $i \in N$. R is *SOLS-ordered* if the pairs in L can be ordered so that L is formed by the superposition of a SOLS S and S^T. (See §III.5.)

50.9 Theorem [1390] There exists a skew SOLS-ordered RS(n) for n an odd positive integer, $n \geq 7$ except possibly for $n = 9, 15, 21, 33, 35, 39, 45, 57, 63, 69, 105$.

50.2 Equivalent Combinatorial Objects

50.10 Theorem The existence of the following are equivalent:

1. a Room square of side n,
2. a Room frame of type 1^n (§50.6),
3. two pairwise orthogonal-symmetric latin squares of order n (§III.3.8),
4. a Howell design $H(n, n+1)$ (§VI.29),
5. two pairwise orthogonal 1-factorizations of K_{n+1} (§VII.5), and
6. two orthogonal resolutions of a BIBD$(n+1, 2, 1)$ (§II.7).

50.11 Remark A Room square of side n can be used to schedule a round robin tournament with $n+1$ teams that has the following properties:

1. Every team plays every other team exactly once during the tournament.
2. Every team plays in exactly one game in each round (the rows).
3. Every team plays at every location exactly once (the columns).

50.3 Construction of Room Squares

50.12 Theorem If there exist two orthogonal starters in a group of order n, then there exists a Room square of side n. If the group is $\mathbb{Z}_n$, then the resulting Room square is cyclic. Conversely, given a cyclic Room square of side n, then there exist two orthogonal starters in the group $\mathbb{Z}_n$. (See §VI.55.)

50.13 Remark The construction of a Room square from a pair of orthogonal starters is given explicitly in Construction VI.55.13.

50.14 Theorem (Singular Direct Product) Suppose there is a Room square of side u, and a Room square of side v containing a Room subsquare of side w, where $v - w \neq 6$ (see

Theorem 50.29). Then, there exists a Room square of side $u(v-w)+w$ that contains Room subsquares of sides u, v, and w.

50.15 Remark Extremely powerful recursive constructions for Room squares use Room frames (§50.6) and transversal designs.

50.16 Remark A very effective method for constructing Room squares is by use of a *hill-climbing algorithm*. A description of this type of algorithm (for Steiner triple systems) is given in §VII.6.5. A description of the specific algorithm for Room squares can be found in [725].

50.4 Enumeration of Room Squares

50.17 Let F_1 and F_2 be Room squares of side n on a symbol set S.

1. F_1 and F_2 are *isomorphic* if F_2 can be obtained from F_1 by any sequence of permutations of the rows, the columns, or the symbols in S.
2. F_1 and F_2 are *equivalent* if they are isomorphic or if F_1 is isomorphic to the transpose of F_2.

50.18 Table [2110] The six inequivalent Room squares of order 7. The sizes of the automorphism group of the squares are 168, 21, 24, 8, 12, and 12, respectively.

R_1

01		45	67			23
57	02				13	46
	56	03	12		47	
	37		04	26		15
36	14	27		05		
24			35	17	06	
		16		34	25	07

R_2

01			25	67		34
46	02				37	15
27	56	03		14		
	13	57	04			26
	47		36	05	12	
35		24	17		06	
		16		23	45	07

R_3

01		45	67		23	
57	02		13			46
	56	03			47	12
	37		04	26	15	
36	14	27		05		
24				17	06	35
		16	25	34		07

R_4

01	67			23		45
	02	46			57	13
56		03		47	12	
	35	27	04	16		
			17	05	34	26
37	14		25		06	
24		15	36			07

R_5

01				67	23	45
57	02	46				13
	56	03		12	47	
	37		04		15	26
36	14		27	05		
24		17	35		06	
		25	16	34		07

R_6

01	37		25	46		
	02	15	36		47	
26		03	17			45
			04	27	35	16
	14	67		05		23
57		24		13	06	
34	56				12	07

50.19 $\mathrm{NR}(n)$ denotes the number of nonisomorphic Room squares of side n. $\mathrm{IR}(n)$ denotes the number of inequivalent Room squares of side n.

50.20 Theorem $\mathrm{NR}(n) \le 2\mathrm{IR}(n)$.

50.21 Table Nonisomorphic and inequivalent Room squares of side $n \le 9$.

n	3	5	7	9
Nonisomorphic	0	0	10	511562
Inequivalent	0	0	6	257630

50.22 Remark For $n > 10$, no exact values of $\mathrm{IR}(n)$ and $\mathrm{NR}(n)$ are known. Theorem 50.23 is a lower bound for these values when n gets large.

50.23 Theorem For odd $n \ge 153$, $\mathrm{NR}(n) > .19e^{.04n^2}$.

50.24 Remark There are three inequivalent skew Room squares of order 7; R_1, R_2, and R_6 in Table 50.18. The unique skew Room square of side 9 is given in Example 50.5.

50.5 Incomplete Room Squares

50.25 An (n, s)-*incomplete Room square* F is an $n \times n$ array for which

1. every cell of F is empty or contains an unordered pair of symbols from an $(n+1)$-set N;
2. there is an empty $s \times s$ subarray G of F;
3. every symbol of $N \setminus S$ occurs once in each row and column of F, where $S \subset N$ is an $(s+1)$-set;
4. each symbol of S occurs once in each row and each column not meeting G but in no row or column meeting G;
5. the pairs in F are precisely those $\{x, y\} \in (N \times N) \setminus (S \times S)$.

50.26 Remark If an (n, s)-incomplete Room square exists and a Room square of side s exists, then a Room square of side n exists.

50.27 Example An (11,3)-incomplete Room square. ($S = \{0, 1, 2, Y\}$.)

			48			37	6X			59
			69			5X	38			47
				39	4X			57	68	
67	8X		3Y			04	15	29		
58	79			4Y	03				2X	16
9X		78		06	5Y		24		13	
			05	7X	89	6Y		14		23
	46	3X		25		19	7Y			08
	35	49	1X		26			8Y	07	
34		56			17	28		0X	9Y	
			27	18			09	36	45	XY

50.28 Theorem Let s and t be odd positive integers. The necessary condition for the existence of an (s, t) incomplete Room square is that $s \geq 3t + 2$.

50.29 Theorem [729, 757] For every pair of odd positive integers (s, t) with $s \geq 3t + 2$, there exists an (s, t) incomplete Room square, except when $(s, t) = (5, 1)$ and with the possible exception of $(s, t) = (67, 21)$.

50.6 Room Frames

50.30 If $\{S_1, \ldots, S_n\}$ is a partition of a set S, an $\{S_1, \ldots, S_n\}$-*Room frame* is an $|S| \times |S|$ array, F, indexed by S, satisfying:

1. every cell of F either is empty or contains an unordered pair of symbols of S,
2. the subarrays $S_i \times S_i$ are empty, for $1 \leq i \leq n$ (these subarrays are *holes*),
3. each symbol $x \notin S_i$ occurs once in row (or column) s for any $s \in S_i$, and
4. the pairs occurring in F are those $\{s, t\}$, where $(s, t) \in (S \times S) \setminus \bigcup_{i=1}^{n} (S_i \times S_i)$.

50.31 If F is a Room frame, then

1. The *type* of a Room frame F is the multiset $\{|S_i| : 1 \le i \le n\}$. An "exponential" notation is used to describe types; a Room frame has type ${t_1}^{u_1}{t_2}^{u_2}\ldots{t_k}^{u_k}$ if there are u_i S_js of cardinality t_i, $1 \le i \le k$.
2. The *order* of the frame is $|S|$.
3. A Room frame of type t^u (one hole size) is *uniform*.
4. A Room frame is *skew* if cell (i, j) is filled implies that cell (j, i) is empty.
5. The definitions for two Room frames (of the same type) to be *isomorphic* or *equivalent* are analagous to those of Room squares.

50.32 Example Room frames of type $1^1 3^4$ and type 2^5.

	$9c$		$5b$	$2d$				36		$7a$	48	
				$8b$	ad			$5c$			79	16
				$1c$	$9b$		$5d$				$6a$	78
59						ac	$1b$		$7d$	68		
$2a$	18	$9d$						$4b$	$3c$			
		ab	$8d$				$4c$				13	29
$8c$								$1d$	$2b$	49		$3a$
	$6d$		$7c$			$3b$				12		45
$6b$		17			$2c$	$4d$				35		
$3d$	$7b$	$6c$			14						25	
		58	$1a$	39				27	46			
			69	$4a$		28	37		15			
47	$5a$				38	19	26					

			79	68		35	24	
	69	78			34			25
59	48						17	06
			16	07	58	49		
26					19	08		37
	27	18	09				36	
	39	04	15	28				
38					29		05	14
		57	46		13	02		
47	56			03			12	

50.33 Remark A Room square of side n is equivalent to a Room frame of type 1^n, and an (n, s)-incomplete Room square is equivalent to a Room frame of type $1^{n-s}s^1$.

50.34 Theorem Existence theorems for uniform Room frames.

1. There does not exist a Room frame of type t^u if any of the following conditions hold: (i) $u = 2$ or 3; (ii) $u = 4$ and $t = 2$; (iii) $u = 5$ and $t = 1$; (iv) $t(u-1)$ is even.
2. [716, 729, 885] Suppose t and u are positive integers, $u \ge 4$ and $(t, u) \ne (1, 5), (2, 4)$. Then there exists a uniform Room frame of type t^u if and only if $t(u-1)$ is even, except possibly when $u = 4$ and $t = 14$.

50.35 Theorem Existence theorems for Room frames with two hole sizes.

1. [729] There is a Room frame of type $2^u t^1$ with $t \ge 4$ if and only if t is even and $u \ge t + 1$, except possibly when $u = 19$ and $t = 18$.
2. [726] There is a Room frame of type $2^a 4^b$ for all $a+b \in \{6, 7, \ldots, 14, 31, 42, 43, 44\}$ or if $a + b \ge 48$.
3. [726] There is a Room frame of type $1^a 3^b$ for all $a + b \in \{5, 7, 9\}$ except for $(a, b) \in \{(2, 3), (3, 2), (4, 1), (5, 0), (5, 2), (6, 1)\}$.
4. [726] There is a Room frame of type $3^a 5^b$ for all $a + b = 7$, and one of type $4^c 6^d$ for all $c + d = 6$ or 7.

50.36 Theorem [480, 2201] The necessary conditions for the existence of a *skew* Room frame of type t^u, namely, $u \ge 4$ and $t(u-1)$ is even, are also sufficient except for $(t, u) \in \{(1, 5), (2, 4)\}$ and with possible exceptions:

1. $u = 4$ and $t \equiv 2 \pmod 4$;
2. $u = 5$ and $t \in \{17, 19, 23, 29, 31\}$.

50.37 Theorem [713] There are 64 inequivalent Room frames of type 2^5.

50.7 Maximum Empty Subarray Room Squares

50.38 A *maximum empty subarray Room square*, denoted MESRS(n), is an RS(n) containing an $\frac{n-1}{2} \times \frac{n-1}{2}$ subarray of empty cells.

50.39 Example A MESRS(9) is given on the right.

37					28	59	$4X$	16
	56				$1X$	47	29	38
		$2X$			67	18	35	49
			48		39	26	17	$5X$
				19	45	$3X$	68	27
12	$8X$	57	69	34				
46	13	89	$7X$	25				
58	79	14	23	$6X$				
$9X$	24	36	15	78				

50.40 Remark The existence of a MESRS($2n-1$) is equivalent to the existence of a partitioned balanced tournament design, a PBTD(n). (See §VI.3.)

50.41 Theorem [1387] There exists a MESRS($2n-1$) for all $n \geq 5$ except possibly for $n \in \{9, 11, 15\}$. (See Theorem VI.3.14.)

50.42 Remark [727] A MESRS(n) can be used to design a round robin tournament with $n+1$ players playing at n sites over n time periods with the property that the $\frac{n+1}{2}$ referees change fields a minimum number of times.

50.8 Higher Dimensions

50.43 A Room d-cube of side n is a d-dimensional cube of side n with the property that every 2-dimensional projection is a Room square of side n.

50.44 $\nu(n)$ denotes the maximum d for which a Room d-cube of side n exists.

50.45 Remark The existence of a Room d-cube of side n is equivalent to the existence of d pairwise orthogonal 1-factorizations of K_{n+1}. The construction goes as follows: Edge $\{x, y\}$ is in 1-factor f_{a_i} in 1-factorization F_i for $1 \leq i \leq d$, if and only if cell $(a_1, a_2, \ldots, a_d)$ contains the symbols x and y.

50.46 Example The unique set of three pairwise orthogonal 1-factorizations of K_8 (Room 3-cube of side 7).

F_1				F_2				F_3			
∞0	16	25	34	∞0	13	26	45	∞0	15	23	46
∞1	20	36	45	∞1	24	30	56	∞1	26	34	50
∞2	31	40	56	∞2	35	41	60	∞2	30	45	61
∞3	42	51	60	∞3	46	52	01	∞3	41	56	02
∞4	53	62	01	∞4	50	63	12	∞4	52	60	13
∞5	64	03	12	∞5	61	04	23	∞5	63	01	24
∞6	05	14	23	∞6	02	15	34	∞6	04	12	35

50.47 Example [730] The unique set of four pairwise orthogonal 1-factorizations of K_{10} (Room 4-cube of side 9).

F_1	F_2	F_3	F_4
01 23 45 67 89	01 29 36 48 57	01 26 39 47 58	01 25 34 68 79
02 13 46 58 79	02 15 34 69 78	02 14 37 56 89	02 18 35 49 67
03 12 47 59 68	03 16 28 45 79	03 17 25 48 69	03 15 27 46 89
04 16 25 39 78	04 17 26 35 89	04 18 27 36 59	04 13 28 57 69
05 18 24 37 69	05 14 27 39 68	05 19 28 34 67	05 16 29 38 47
06 19 27 35 48	06 12 37 39 58	06 15 24 38 79	06 14 23 59 78
07 15 28 36 49	07 19 25 38 46	07 13 29 45 68	07 12 39 48 56
08 17 29 34 56	08 13 24 59 67	08 16 23 49 67	08 19 26 37 45
09 14 26 38 57	09 18 23 47 56	09 12 35 46 78	09 17 24 36 58

50.48 Theorem $\nu(2n-1) \to \infty$ for $n \to \infty$.

50.49 Theorem For every odd $n \geq 3$, $\nu(n) \leq n-2$, and if $n \geq 17$, then $\nu(n) \geq 5$.

50.50 Theorem If $q = 2^k t + 1$ is a prime power with t odd, then $\nu(q) \geq t$.

50.51 Table (see [725]) Lower bounds for $\nu(n)$.

n	$\nu(n) \geq$	n	$\nu(n) \geq$	n	$\nu(n) \geq$	n	$\nu(n) \geq$
1	$= \infty$	27	13	53	17	79	39
3	$= 1$	29	13	55	5	81	5
5	$= 1$	31	15	57	5	83	41
7	$= 3$	33	5	59	29	85	5
9	$= 4$	35	5	61	21	87	5
11	5	37	15	63	5	89	11
13	5	39	5	65	5	91	5
15	4	41	9	67	33	93	5
17	5	43	21	69	5	95	5
19	9	45	5	71	35	97	5
21	5	47	23	73	9	99	5
23	11	49	5	75	5	101	31
25	7	51	5	77	5	103	51

See Also

§VI.29	Howell designs are generalizations of Room squares.
§VI.51	Room squares give a schedule of play for a round robin tournament.
§VI.55	Starters are used to construct Room squares.
§VII.5	A connection with 1-factorizations is given by Theorem 50.10.
[725]	A broad survey of Room squares with an extensive bibliography. This reference contains much of the information in this chapter.
[2110]	A textbook dealing with Room squares.
[84]	A survey of orthogonal factorizations.

References Cited: [84, 480, 713, 716, 725, 726, 727, 729, 730, 757, 885, 1387, 1390, 1447, 2110, 2201]

51 Scheduling a Tournament

Jeffrey H. Dinitz
Dalibor Froncek
Esther R. Lamken
Walter D. Wallis

51.1 Round Robin Tournaments

51.1 A *round robin tournament* is a tournament with the property that every team plays every other team precisely once during the tournament.

51.2 **Remarks** The underlying graph for a round robin tournament with n teams is K_n, the complete graph on n vertices. The number of games is $\binom{n}{2}$. If n is even, then it is possible to play the tournament in $n-1$ *rounds* each consisting of $n/2$ games involving all n teams. The underlying design of a round robin tournament played in rounds of $n/2$ games is a 1-factorization of K_n (see §VII.5). In applications to games and sports, often the schedule of play must satisfy a number of additional requirements. Many of these are addressed in this chapter.

51.3 A *tournament design* defined on a $2n$ set V is an arrangement of the $\binom{2n}{2}$ distinct unordered pairs of the elements of V into an $n \times (2n-1)$ array such that every element of V is contained in precisely one cell of each column.

51.4 **Example** A tournament design on eight teams, $\infty, 0, 1, \ldots, 6$ (the pairing $\{a, b\}$ is represented by ab).

0∞	1∞	2∞	3∞	4∞	5∞	6∞
16	20	31	42	53	64	05
25	36	40	51	62	03	14
34	45	56	60	01	12	23

51.5 **Remarks** A tournament design provides a schedule of play for a round robin tournament with $2n$ teams played in $2n-1$ rounds with the property that every team plays precisely once in each round (column).

51.6 An *odd tournament design*, OTD(n), defined on a $2n+1$ set V is an arrangement of the $\binom{2n+1}{2}$ distinct unordered pairs of the elements of V into an $n \times (2n+1)$ array such that every element of V is contained in at most one cell of each column.

51.7 **Example** An OTD(3), with teams named $0, 1, \ldots, 6$.

16	20	31	42	53	64	05
25	36	40	51	62	03	14
34	45	56	60	01	12	23

51.8 **Remarks** An OTD(n) is equivalent to a near 1-factorization of K_{2n+1}. An OTD(n) provides a schedule of play for a round robin tournament with the property that every team sits out (has a *bye*) precisely one round of the tournament.

51.9 **Remark** It is always possible to construct both a tournament design for $2n$ teams and an OTD(n). The easiest way is to use a starter in the cyclic group (§VI.55) as the first column and develop each subsequent column cyclically from the first. Examples

51.4 and 51.7 were constructed from the patterned starter $P = \{\{1,6\},\{2,5\},\{3,4\}\}$ in $\mathbb{Z}_7$.

51.10 Remark A *Swiss tournament* is an incomplete simple round robin tournament played in rounds. In the first round, matches are chosen at random or according to some prearranged seeding plan. After each subsequent round, players' scores are calculated (the method may be simply 1 point for each win, 1/2 for each tie, or it may involve the scores in the matches). In the next round, the two highest scoring players form the first match, then the next two, and so on, with the proviso that no repeated pairs are allowed. A random draw is used to decide between equal scores.

At any stage, let G be the underlying graph of the union of the rounds already held. In order for the tournament to continue, the complement of G must contain a 1-factor; in other words, the set of factors chosen so far must not be *premature* (see [1825]). In practice a limit of approximately $\log_2 n$ rounds is used for n teams.

51.11 Remark Suppose n teams are ranked from 1 to n with the strength of the ith ranked team defined by $s(i) = n+1-i$. The total strength of opponents that team i plays in a complete round robin tournament is $S_{n,n-1}(i) = n(n+1)/2 - s(i)$. A *fair incomplete tournament* of n teams with k rounds, $\mathrm{FIT}(n,k)$, is a tournament in which every team plays exactly k other teams and the total strength of the opponents that team i plays is $S_{n,k}(i) = n(n+1)/2 - s(i) - m$ for some fixed constant m. It follows that the total strength of the opponents that each team misses is the same. An *equalized incomplete tournament* of n teams with r rounds, $\mathrm{EIT}(n,r)$, is a tournament in which every team plays exactly r other teams and the total strength of the opponents that each team plays, $T_{n,r}(i)$, is the same. A $\mathrm{FIT}(n,k)$ exists if and only if an $\mathrm{EIT}(n,n-k-1)$ exists. For n odd, only partial results are known.

51.12 Theorem [835] For n even, an $\mathrm{EIT}(n,r)$ exists if and only if r is even and either $n \equiv 0 \pmod 4$ or $r \equiv 0 \pmod 4$. For n even, a $\mathrm{FIT}(n,k)$ exists if and only if k is odd and either $n \equiv 0 \pmod 4$ or $k \equiv 1 \pmod 4$.

51.13 Remark When a game (i,j) is scheduled for round m and (j,k) for round $m-1$, then team i receives a *carry-over effect* from team k in round m. The best possible schedule with respect to this property is one in which no team receives the carry-over effect from another team more than once. Such schedules are *schedules with perfect carry-over effect*; they are known to exist for the number of teams equal to powers of 2 [1157, 1834] and for 20 and 22 teams [95].

51.2 Oriented 1-Factorizations

51.14 Remark Oriented 1-factorizations can be used to satisfy several requirements for scheduling round robin tournaments in sports.

51.15 Example Home-Away schedules. In many sports, a team regularly plays at a specified location, its home stadium or field. If a game is played between team i and team j at team j's home location, then it is a *home* game for team j and an *away* game for team i, and the edge ij in the underlying graph is oriented by using the directed edge (i,j). A home-away schedule is often preferred that alternates, as much as possible, home and away games. A *home-away pattern* of a team i, $\mathrm{HAP}(i)$, is the sequence $p_1(i), p_2(i), \ldots, p_{n-1}(i)$ where $p_m(i) = H$ ($p_m(i) = A$) if i plays a home (away) game in round m. A *break* in a schedule is a pair of successive rounds in which a given team is at home, or away, in both rounds.

51.16 Example A home-away schedule for 6 teams with 4 breaks (for teams 2,3,4,5) [663].

Day	Matches			Teams 1	2	3	4	5	6
1	(1,6)	(2,5)	(4,3)	A	A	H	A	H	H
2	(6,2)	(3,1)	(5,4)	H	H	A	H	A	A
3	(3,6)	(4,2)	(1,5)	A	H	A	A	H	H
4	(6,4)	(5,3)	(2,1)	H	A	H	H	A	A
5	(5,6)	(1,4)	(3,2)	A	H	A	H	A	H

51.17 Theorem [663] (a) There is a home-away schedule for a tournament design on $2n$ teams with exactly $2n-2$ breaks (and this is best possible).

(b) There is a home-away schedule for an OTD(n) without breaks.

51.18 Remarks If two teams share the same home ground, then the two teams cannot both play at home at the same time, except when they play each other. A home-away schedule with the property that the teams can be paired so that only one member of a pair is at home in each round has *Property P*.

51.19 Theorem [2107] Given any 1-factorization of K_{2n}, there exists a way of pairing the vertices and a way of orienting the edges so that the resulting home-away schedule has Property P.

51.20 An RRT(n,k) is a round robin tournament of n teams in which the games are evenly divided into k rounds. An RRT($2n, 2n-1$) is the usual round robin tournament (or tournament design), and RRT($2n-1, 2n-1$) is an odd tournament design OTD($2n-1$). In this case, $p_m(i) = B$ in HAP(i) if i has a bye in round m, and a *break* in a schedule is any of the sequences AA, HH, ABA, HBH. An RRT(n,k) is *perfect* if it has no breaks.

51.21 Theorem [836] For every $n \geq 2$ there is a unique perfect RRT($2n, 2n$) and RRT($2n-1, 2n-1$) with the game (i,j) played in round $i+j-1$ and team i having a bye in round $2i-1$ (addition in $\mathbb{Z}_{2n}$ or $\mathbb{Z}_{2n-1}$, respectively). Moreover, it has *Property P*.

51.22 Example A perfect RRT(6, 6).

Day	Matches			Teams 1	2	3	4	5	6
1	(6,2)	(5,3)	–	B	H	H	B	A	A
2	(4,5)	(3,6)	(2,1)	H	A	A	A	H	H
3	(1,3)	(6,4)	–	A	B	H	H	B	A
4	(5,6)	(4,1)	(3,2)	H	H	A	A	A	H
5	(2,4)	(1,5)	–	A	A	B	H	H	B
6	(6,1)	(5,2)	(4,3)	H	H	H	A	A	A

51.23 Remark There are a number of other schedule requirements that can be satisfied by using oriented 1-factorizations; see [2107].

51.3 Balanced Tournament Designs

51.24 Remarks If the locations (courts, fields) are of unequal attractiveness, then a schedule is required that balances the effect of the locations. A tournament design or an OTD(n) with the additional property that no element of V is contained in more than two cells of any row is a *balanced tournament design*, BTD(n), or an *odd balanced tournament design*, OBTD(n), respectively. These designs provide schedules of play for the tournament with the additional property that no one plays more than twice at

any location. Balanced tournament designs can be constructed with additional structure. Existence results and examples of several different types of balanced tournament designs can be found in §VI.3.

51.25 Remark A balanced tournament design for $2n$ players is generally given as an $n \times (2n-1)$ array where each cell contains a pair of symbols from a set S of size $2n$ such that (1) every symbol is paired with every other symbol exactly once, (2) in each column each symbol appears exactly once, and (3) in each row every symbol appears twice except for two symbols that each appear only once. A similar array, a *stadium balanced array* can be defined as follows. The array is now an $n \times 2n$ array where each cell again contains a pair of symbols from a set S of size $2n$ such that (1) every symbol is paired with every other symbol exactly once except that it is paired with exactly one symbol twice, (2) in each column each symbol appears exactly once, (3) in each row every symbol appears twice, and (4) no pair can occur twice in any row.

If the symbols are teams, the columns are weeks and the rows are stadiums, then the array defined gives a schedule of play for $2n$ teams at n stadiums (n games at a time) satisfying the property that (1) each team plays at each stadium exactly twice, (2) each team plays every other team exactly once except for one team which they play twice, and (3) two teams that play twice play their two games in different stadiums. These schedules can be constructed for all $n \geq 4$ [1392]. (The schedules do not exist for $n = 2, 3$.)

51.4 Softball Balanced Tournament Designs

51.26 Remark In many applications, the tournament schedules have several different requirements that must be satisfied simultaneously. Scheduling softball league tournaments motivated the following definition; see [815].

51.27 Let $B_1, B_2, \ldots, B_m$ denote a collection of bias categories for a tournament design for $2n$ teams. Each B_k is an n_k-dimensional vector $(b_{k1}, b_{k2}, \ldots, b_{kn_k})$, $n_k \geq 1$. The b_{kj} are the *attributes*. Each team $i \in V$ has a frequency vector with respect to each B_k, $(\lambda^i_{k1}, \lambda^i_{k2}, \ldots, \lambda^i_{kn_k})$ where λ^i_{kj} denotes the number of times in the tournament design that team i has attribute b_{kj}. Team i has *balance with respect to bias category* B_k if $\max_{j,\ell} |\lambda^i_{kj} - \lambda^i_{k\ell}| \leq 1$. A tournament design is *balanced with respect to bias category* B_k if (1) each team $i \in V$ has balance with respect to B_k and (2) for each j, $\max_{i,p} |\lambda^i_{kj} - \lambda^p_{kj}| \leq 1$.

51.28 A *softball balanced tournament design for* $2n$ *teams*, SBTD(n), is a tournament design that is balanced with respect to each of its bias categories.

51.29 Example [815] An SBTD(6). This design is balanced with respect to B_1=(M,T,W,Th) (day of the week bias), B_2=(6:20PM, 7:25PM, 8:30PM) (time of day bias), B_3=(H,A) (home team bias), B_4=(number of games any given team plays in one week), and B_5=(number of games any given team plays in one day).

		M	T	W	TH
Week 1	6:20 PM	(4,11)	(10,6)	(8,10)	(2,3)
	7:25 PM	(3,12)	(9,7)	(11,5)	(7,1)
	8:30 PM	(1,2)	(5,8)	(12,4)	(6,9)
Week 2	6:20 PM	(8,2)	(12,5)	(5,4)	(7,11)
	7:25 PM	(9,1)	(4,3)	(3,9)	6,12)
	8:30 PM	(11,6)	(10,7)	(2,10)	(1,8)
Week 3	6:20 PM	(7,12)	(3,1)	(11,9)	(1,5)
	7:25 PM	(5,6)	(8,11)	(12,8)	(2,4)
	8:30 PM	(4,10)	(9,2)	(6,7)	(10,3)

		M	T	W	TH
Week 4	6:20 PM	(5,3)	(7,8)	(3,7)	(12,10)
	7:25 PM	(10,11)	(6,2)	(4,6)	(8,9)
	8:30 PM	(9,12)	(1.4)	(11,1)	(2,5)
Week 5	6:20 PM	(10,9)	(11,2)	(2,12)	(8,6)
	7:25 PM	(4,8)	(12,1)	(1,10)	(3,11)
	8:30 PM	(5,7)	(6,3)	(9,5)	(7,4)
Week 6	6:20 PM	(6,1)	(9,4)		
	7:25 PM	(7,2)	(5,10)		
	8:30 PM	(8,3)	(12,11)		

51.30 Remark Some infinite classes of SBTDs are described in [815]. Finizio also considers cases where interdivisional play is separated from divisional play and league schedules where the teams may play against each other more than once. Not all of the designs in [815] have the property that the games can be partitioned into rounds.

51.5 Tournament Arrays

51.31 Remarks If there are fewer than n locations for a tournament for $2n$ or $2n+1$ teams, then not every team can play in each round of the tournament. However, tournaments can still be scheduled for round robin tournaments with certain balance categories.

51.32 A *tournament array* $\mathrm{TA}(m,c)$ is a $c \times t$ array of the $\binom{m}{2}$ distinct unordered pairs of the elements of an m set V such that every element of V occurs at most once in each column of the array.

51.33 Remark The necessary conditions for the existence of a $TA(m,c)$ are $ct = \binom{m}{2}$ and $1 \le c \le \lfloor \frac{m}{2} \rfloor$.

51.34 A *court balanced tournament array*, $\mathrm{CBTA}(m,c)$, is a tournament array with the additional property that each element occurs exactly α times in each row. This requires that $c\alpha = m-1$.

51.35 Example A $\mathrm{CBTA}(10,3)$ [1585].

10	15	26	27	38	39	23	50	64	75	86	79	80	14	49
36	37	18	19	24	20	58	69	13	84	95	60	47	25	70
28	29	34	35	16	17	67	78	89	90	40	45	12	30	56

51.36 Theorem [1585] The necessary conditions for the existence of a $\mathrm{CBTA}(m,c)$ are also sufficient.

51.37 Remarks Tournament arrays can also be balanced with respect to the number of rounds that teams rest between matches. These designs are *interval-balanced*; see [1814].

51.38 Example An interval-balanced $\mathrm{TA}(9,2)$ [1814]. The number of rounds between two matches for team i is either 1 or 2.

12	56	91	45	89	52	96	35	49	15	92	61	39	46	95	62	79	36
34	78	23	67	13	74	81	27	68	73	84	57	28	17	83	41	58	24

51.39 Remark A particularly interesting instance of interval balance is when there is only one available court. In this case, a schedule of play is required that maximizes the minimum number of pairs occurring between any two appearances of any one team. For m teams, this minimum is $\lfloor \frac{m-3}{2} \rfloor$. When this is achieved in a schedule of m teams, the tournament (design) is a *pair design*, $\mathrm{PD}(m)$.

51.40 Theorem [1917] A PD(m) exists for all positive integers $m \geq 2$.

51.41 Construction A construction of pair designs for all m. First assume that m is odd. The sequence for the first m pairs is

$$Q_m = (\{1,2\},\{3,4\},\ldots,\{m-2,m-1\},\{m,1\},\{2,3\},\ldots,\{m-1,m\})$$

Let P be the permutation $(1)(3\ 5\ 7\ \cdots\ m-4\ m-2\ m\ m-1\ m-3\cdots 6\ 4\ 2)$ and $L = \frac{m-3}{2}$. The pair design PD(m) is $Q_m, PQ_m, P^2Q_m, \ldots, P^LQ_m$. When m is even, let $Q_m = (\{1,2\},\{3,4\},\ldots,\{m-1,m\})$, $L = n-2$, and $P = (1)(3\ 5\ 7\ \cdots\ m-3\ m-1\ m\ m-2\ m-4\cdots 6\ 4\ 2)$; again, the pair design is $Q_m, PQ_m, P^2Q_m, \ldots, P^LQ_m$.

51.42 Remark The PD(m) from Construction 51.41 can be used to construct an interval-balanced TA(m,c) by placing the pairs of the pair designs down a column of the TA until filled, then moving to the next column. The interval balanced TA(9, 2) of Example 51.38 was constructed from a PD(9) by this method (see [1814]).

51.6 Room Squares and Howell Designs

51.43 Remarks If there are n+1 teams (n+1 even) and n locations, a round robin tournament can be scheduled with the properties that every team plays in exactly one game in each round, and every team plays exactly once at each location. This tournament corresponds to a *Room square* of side n. See §VI.50. If this tournament also has the property that there are n referees and each team sees each referee exactly once, then the tournament corresponds to a Room cube of side n. See §VI.50.8.

Tournament schedules that use the minimum number of referees ($\frac{n+1}{2}$) such that for every team T, each referee is assigned to exactly one or two games involving team T are studied in [727]. These can be constructed from Room squares with maximum empty subsquares (see §VI.50.7) and hence exist when $n \geq 9$ is an odd integer, with the possible exceptions of $n \in \{17, 21, 29\}$

51.44 Remarks Howell designs, $H(s, 2n)$, can be used to schedule tournaments with the properties that every team plays in each round and every team plays at each of s locations precisely once. However, when $n \leq s \leq 2n-2$, the schedule no longer has the property that every team plays every other team once during the tournament. See §VI.29.

51.45 Example Spouse avoiding tournament. Suppose there are $2n$ players and n couples, and suppose every person is to play every person except his or her spouse precisely once in the tournament. A Howell design $H(2n-2, 2n)$ can be used to construct a schedule of play where every person plays in each round; every person plays at each of $2n-2$ locations precisely once; and every person plays each other person except his or her spouse precisely once. The underlying graph is the complete graph minus a 1-factor, the *cocktail party graph*.

51.46 Example An $H(4, 6)$. The columns correspond to the rounds, the rows to the locations and the 3 couples are $\{0,3\},\{1,2\},\{4,5\}$.

04		13	25
23	14	05	
	35	24	01
15	02		34

51.47 Example Suppose there are n people on each of two teams of a tournament. A pair of orthogonal latin squares of side n (equivalently, an $H^*(n, 2n)$) can be used to schedule a tournament with the properties that every person from team 1 plays each person on team 2; there are no games between two people from the same team; every person plays in each round; and every person plays at each of n locations precisely once during the tournament. To construct this schedule, let L_1 and L_2 be two orthogonal latin squares of side n with L_i on the symbols T_i (representing the players on team i) for

$i = 1, 2$. The schedule is constructed by superimposing the two latin squares. The pairs in the cells represent the games, the rows are the rounds, and the columns are the locations. A tournament of this type is a *bipartite tournament*.

51.48 Remark Many of the earliest examples of Howell designs (dating back more than 100 years) were constructed in order to schedule bridge tournaments. See [1933] and §51.10.

51.7 Golf Designs

51.49 Remarks There are often occasions when the teams or players may compete more than once against each other.

51.50 Let V be a set of $2n + 1$ elements. A *golf design of order* $2n + 1$ is a set of $2n - 1$ symmetric idempotent latin squares, $L_1, L_2, \ldots, L_{2n-1}$, defined on V such that L_i and L_j are disjoint off the main diagonal; that is, for $x, y \in V$, $L_i(x, y) \neq L_j(x, y)$ for $i, j = 1, 2, \ldots, 2n - 1$.

51.51 Remarks A golf design provides a schedule of play with the following properties: $2n+1$ teams play a round robin tournament in $2n + 1$ rounds; in each round one team does not play, and the others meet in $2n - 1$ matches all played at the home ground of the nonplaying team. In addition, $2n - 1$ round robin tournaments are to be played so that each pair of teams meets exactly once at each of the $2n - 1$ neutral grounds. (Such tournaments are scheduled in golf.)

51.52 Theorem [455, 572, 2107] There exists a golf design of order v if and only if $v > 0$ is odd and $v \neq 5$.

51.53 Example A golf design of order 7 [2106].

L_1

0	2	4	5	1	6	3
2	1	6	4	5	3	0
4	6	2	0	3	1	5
5	4	0	3	6	2	1
1	5	3	6	4	0	2
6	3	1	2	0	5	4
3	0	5	1	2	4	6

L_2

0	3	6	1	5	4	2
3	1	5	0	6	2	4
6	5	2	4	1	0	3
1	0	4	3	2	6	5
5	6	1	2	4	3	0
4	2	0	6	3	5	1
2	4	3	5	0	1	6

L_3

0	4	5	6	2	3	1
4	1	3	2	0	6	5
5	3	2	1	6	4	0
6	2	1	3	5	0	4
2	0	6	5	4	1	3
3	6	4	0	1	5	2
1	5	0	4	3	2	6

L_4

0	5	3	2	6	1	4
5	1	4	6	3	0	2
3	4	2	5	0	6	1
2	6	5	3	1	4	0
6	3	0	1	4	2	5
1	0	6	4	2	5	3
4	2	1	0	5	3	6

L_5

0	6	1	4	3	2	5
6	1	0	5	2	4	3
1	0	2	6	5	3	4
4	5	6	3	0	1	2
3	2	5	0	4	6	1
2	4	3	1	6	5	0
5	3	4	2	1	0	6

51.54 Example The golf design of Example 51.53 is used to construct five tournaments. The unordered cells that contain i in L_j provide the matches hosted by i in T_j.

Host	T_1			T_2			T_3			T_4			T_5		
0	23	16	45	13	25	46	14	26	35	15	24	36	12	34	56
1	04	25	36	03	24	56	06	23	45	05	26	34	02	35	46
2	01	35	46	06	15	34	04	13	56	03	16	45	05	14	36
3	24	15	06	01	26	45	05	12	46	02	14	56	04	16	25
4	02	13	56	05	16	23	01	25	36	06	12	35	03	15	26
5	03	14	26	04	12	36	02	16	34	01	23	46	06	13	24
6	12	05	34	02	14	35	03	15	24	04	13	25	01	23	45

51.8 Elimination Tournaments

51.55 An *elimination tournament* (or *knockout tournament*) on n teams is a tournament played in rounds in which only the winner of a match at each round can proceed to a match at the next round. In other words, the loser is eliminated at each round.

51.56 Proposition An elimination tournament on n teams can always be constructed in $\lceil \log_2 n \rceil$ rounds and this is the best possible.

51.57 Construction An elimination tournament on n teams can be constructed in $r = \lceil \log_2 n \rceil$ rounds by first adding s phantom teams where $s = 2^r - n$. Next construct a complete binary rooted tree with 2^r leaves and associate each leaf with a team so that no two phantom teams are paired. The teams paired with phantom teams automatically win their first match and essentially have a *bye* in the first round. The winner of a match in round k moves on to the next round and plays the winner of the match in round k that has minimum distance on the tree.

51.58 Remark Elimination tournaments with exactly 2^k teams for some k have the nicest schedules. Major tournaments such as the NCAA basketball tournament (64 teams) and the U.S. Open tennis tournament (128 men) use this format. In an elimination tournament with n teams there are always $n-1$ games, no matter how the tournament is scheduled. (Each game has a loser and the tournament has $n-1$ losers.)

51.59 Remark A common variant of the (single) elimination tournament is the *double elimination* tournament. In this tournament the first time a team loses it is placed in the losers bracket. The team continues to play until its second loss, at which time it is out of the tournament. The winners of the two brackets meet in the final championship with the team from the losers bracket required to win two games in order to be champion.

51.9 Whist Tournaments

51.60 Remarks A whist tournament, Wh($4n$), for $4n$ players is a schedule of games each consisting of two players opposing two others such that the games are arranged in $4n-1$ rounds with the following properties: each round consists of n games; each person plays in exactly one game in each round; each person partners every other person exactly once; and each person opposes every other person exactly twice. Whist tournaments can also be played with $4n+1$ players; in this case there are $4n+1$ rounds and each person sits out during exactly one round of play. Additional structure is required for directed whist tournaments and triplewhist tournaments. These designs date back to the 1800s. Whist tournaments are now used in bridge for *individual* competitions with the property that each player has a variety of partners instead of fixed partnerships. See §VI.64 for a more extensive discussion of whist tournaments including many constructions.

51.10 Bridge Tournaments

51.61 Remark In bridge tournaments, the most common form of competition is where the competitors are fixed partnerships or *pairs*. The competition is a simple round robin consisting of spanning rounds. Each deal of the cards is known as a *board* (because the deals were originally preserved using wooden containers) and is played in several rounds. The two pairs who play against each other in a match are allocated a (num-

bered) table, and the two pairs are designated by the directions north-south (NS) and east-west (EW).

51.62 Example A bridge tournament for eight pairs on four tables $\{1,2,3,4\}$ playing boards $\{a,b,c,d,e,f,g\}$ in seven rounds. For example, in Round 1, pair 8 (NS) plays board a against pair 7 (EW) at Table 1. (In practice $a, b, \ldots$ would each represent a set of three or four boards.)

Round	1	2	3	4	5	6	7
Table	1234	1234	1234	1234	1234	1234	1234
NS	8241	8352	8463	8574	8615	8726	8137
EW	7653	1764	2175	3216	4327	5431	6542
Boards	$abce$	$bcdf$	$cdeg$	$defa$	$efgb$	$fgac$	$gabd$

51.63 Remarks There are two combinatorial aspects to these competitions. The *movement* is the arrangement that assigns boards to each table, assigns directions to each pair, and directs pairs to tables in each round. (For practical purposes, the number of boards in each set must be equal.) Example 51.62 is a movement for eight pairs.

The second aspect is the *scoring*. The scores of all east-west pairs on the same set of boards are compared, as are the scores of all north-souths. In Example 51.62, the boards in set a lead to comparisons between the sets $\{8,4,2,1\}$ and $\{7,6,3,5\}$. The whole tournament gives rise to 14 sets:

$$\{8421\},\{2853\},\{4386\},\{5487\},\{1658\},\{2768\},\{3178\},$$
$$\{7635\},\{6174\},\{5721\},\{6132\},\{3724\},\{4135\},\{5246\}.$$

These sets constitute the *underlying block design* of the tournament. The tournament is *balanced* if the underlying design is (pairwise) balanced. For example, the tournament is balanced because its underlying design is a BIBD(8,4,3).

51.64 Example The most common bridge tournament is the *Mitchell movement* for $2n$ pairs (n odd). The pairs are split into two groups of size n, NS and EW. Pairs in NS always play north-south. The tournament consists of n rounds, played at n tables, using n sets of boards. Tables, board-sets, rounds, and both sets of players are labeled with the integers modulo n. In round i, pair j NS and pair $j+i$ EW meet at table j and play board-set $j-i$. The comparisons are balanced within sets NS and EW, but members of different sets are never compared, so this tournament produces two winners. Another "balance" feature is that all pairs meet the same set of opponents; this produces a fairer tournament.

51.65 Remark The Mitchell movement is equivalent to a pair of orthogonal latin squares: a circulant and a back-circulant square of side n. If n is even, these squares are not an orthogonal pair, and the movement does not work, but minor adjustments can be made that result in playable tournaments that are close to balanced (see [977]).

51.66 Example Another common movement used in bridge tournaments is the *Howell movement*. This movement on $2n$ pairs satisfies the following properties:

1. every board is played by at most one pair of teams (one in each direction) in each round;
2. every team plays every other team exactly once during the tournament;
3. every team plays exactly one set of boards in each round;
4. every team plays each board exactly once;
5. every team competes equally often against any other team.

The movement in Example 51.62 is an eight-pair, seven-table Howell movement.

51.67 Let R be a Room square (§VI.50) of order $2n$ (side $2n-1$) with each entry considered as an ordered pair. From each row of R construct a pair of complementary blocks—one block consisting of the elements that occur as the first coordinate of an ordered pair in that row, and one block consisting of the elements that occur as the second coordinate. If the resulting set of $2(2n-1)$ blocks is the set of blocks of a BIBD$(2n, n, n-1)$, then the (ordered) Room square is a *balanced* Room square and is denoted BRS$(2n)$.

51.68 Construction Let R be a balanced Room square of order $2n$ (side $2n-1$). The rows, columns, and symbols of R correspond respectively to the boards, rounds, and teams of a Howell movement on $2n$ teams.

51.69 Theorems (see [725, 1717])

1. If a BRS$(2n)$ exists, then $2n$ is a multiple of 4.
2. A BRS$(q+1)$ exists for all prime powers $q \equiv 3 \pmod 4$.
3. A BRS$(2q+2)$ exists for all odd prime powers q other than Fermat primes.
4. There exists a BRS(2^n) if n is odd, or if n is even and $4 \le n \le 18$.
5. BRS(n) exist for all $n \equiv 0 \pmod 4$ such that $8 \le n \le 100$, with the two possible exceptions $n = 36$ and $n = 92$.

51.70 Remark If the number of boards in each set is at least k, then it is possible for k tables to play the same set of boards in the same round ("sharing boards"), allowing a relaxation of condition 1 in Example 51.66.

51.71 Example Since there does not exist a Room square of side 5, no Howell movement for six pairs is possible. In this case, the following generalized Howell design can be used. There are five sets of boards; set e is shared between all three tables in round 5.

Round	1	2	3	4	5
Table	123	123	123	123	123
NS	623	634	645	651	612
EW	154	215	321	432	543
Boards	*adb*	*bdc*	*cab*	*dac*	*eee*

51.72 Remark Construction 51.68 can be generalized by using a Howell design (§VI.29). Such a movement is a *three-quarter Howell movement*. Because of the imbalance between the sets of opponents, these designs are used primarily in club games, when the number of pairs is small, and seldom in serious competition.

51.73 Remark For extensive discussions of bridge tournaments including explicit master sheets for Mitchell and Howell movements, see [977, 1580].

51.74 Suppose there are n bridge teams each consisting of two pairs (the two pairs are *teammates*). A match is a triple (i, j, b) where pair i opposes pair j on a board b; here i and j are not teammates and "oppose" is an ordered relation. A *complete coupling round robin schedule of order* n, a CCRRS(n), is a tournament for the n teams that satisfies the following conditions with a minimum of boards.

1. Every pair must play against every other pair not on its team exactly once.
2. Every pair must play one match at every round.
3. Every pair must play every board exactly once except for odd n where each team skips two boards.
4. If pair i opposes pair j on a board, then the teammate of j must oppose the teammate of i on the same board.
5. Every board is played in at most one match at a round.

51.75 Example A CCRRS(4) is displayed as a Howell design $H(6,8)$ with a special property. The teams are $\{1,2\},\{3,4\},\{5,6\},\{7,8\}$. There are 6 rounds of play (the columns) and 6 boards (the rows) used in the tournament. The pairs are ordered to display Property 4.

13	68		42		75
67	14		85		32
48		15	73	62	
25		47	61	83	
	35	28		71	64
	27	36		54	81

51.76 Theorem [877] For n a positive integer, $n \geq 3$, there exists a CCRRS(n) except possibly for $n \in \{54, 62\}$

51.77 Remarks A bridge tournament with Property 4 is in *team-of-four format*; the basic unit of competition is a team formed by two pairs. In the team-of-four format a match between two teams is decided only by the play of the two teams and not by the play of any other team. More on this type of tournament can be found in [877].

In actual bridge tournaments Property 5 is often replaced by the requirements that the two matches are played in the same round in which pair i opposes pair j, the teammate of j opposes the teammate of i, and these two matches share the same boards; but these boards are not played elsewhere in the round. Also, the minimality of the number of boards is not important. For tournaments satisfying these requirements, see [977, 1580].

51.11 Spouse Avoiding Doubles Tournaments

51.78 A *spouse avoiding mixed doubles round robin tournament for n couples*, a SAMDRR(n), is a tournament with the following properties: (1) a match consists of two players of different genders playing against two players (of different genders), (2) every two players of the same gender play against each other exactly once, (3) every player plays with each player of the opposite gender (except his or her spouse) exactly once as a partner and exactly once as an opponent.

51.79 Construction An idempotent self-orthogonal latin square (SOLS) ($S = s_{ij}$) of order n can be used to schedule the $n(n-1)/2$ matches in the spouse avoiding mixed doubles round robin tournament as follows: In the unique match in which Mr. i opposes Mr. j ($i \neq j$), the partner of Mr. i is Mrs. s_{ij} (and the partner of Mr. j is Mrs. s_{ji}).

51.80 Example The array S is a SOLS(4), and the array M is a symmetric orthogonal mate for M. S and M are used to construct the matches listed.

S

1	4	2	3
3	2	4	1
4	1	3	2
2	3	1	4

M

4	1	2	3
1	4	3	2
2	3	4	1
3	2	1	4

Cell	Match	Cell	Match
(1,2)	H_1W_4 vs H_2W_3	(3,4)	H_3W_2 vs H_4W_1
(1,3)	H_1W_2 vs H_3W_4	(2,4)	H_2W_1 vs H_4W_3
(1,4)	H_1W_3 vs H_4W_2	(2,3)	H_2W_4 vs H_3W_1

51.81 Remark This schedule has the additional property that it can be played in three rounds where each person plays in one game in each round. This can be guaranteed by using a SOLS with a symmetric orthogonal mate, a SOLSSOM. The symmetric orthogonal mate M is used to construct the rounds. The unordered cells that contain the 1s, $\{1,2\}$ and $\{3,4\}$, provide the matches in round 1; the cells that contain the 2s

provide the matches in round 2 and the cells that contain the 3s provide the matches in round 3. See §IV.5.6.

51.12 Resolvable Coverings of Pairs

51.82 Example A schedule of play can be constructed for 24 people with the following properties: the game is played at tables of size 4, every person plays at a table with every other person at least once, and each person plays in every round (a round is six tables of size four). The minimum number of rounds required for this tournament is 8. A solution is constructed using a resolvable minimum cover with block size 4 [1393] and is displayed as Example VI.11.44.

51.83 Remark Example 51.82 is a special case of a more general tournament structure with the following properties: the game is played at tables of size k, there are nk players, every person plays at a table with every other person at least (most) once, and each person plays in every round (a round is n tables of size k). In addition, the tournament must be completed in the smallest (largest) number of rounds possible. The existence of such a tournament is equivalent to a resolvable minimum cover (maximum packing) of pairs by k-sets. When $nk \equiv 1 \pmod{k(k-1)}$ both the minimum cover and maximum packing are equivalent to a resolvable BIBD$(nk, k, 1)$. For results on resolvable BIBDs, see §II.7; for results on resolvable packings, see §VI.40.5; and for results on resolvable coverings see [1393] and §VI.11.6.

51.84 Example [779] A tournament for 12 competitors can be constructed with the following properties: the game is played in groups of size 4, there are eight rounds (a round is three groups of size 4), every competitor plays in a group with every other competitor either two or three times, and each competitor plays in every round. There are exactly two nonisomorphic solutions [1830]. One is

0123	017T	0359	4791	8E15	0678	47E0	8234
4567	245E	148T	5802	9046	134E	5783	9E07
89TE	3689	267E	6TE3	T237	259T	6912	T156

51.85 Remark Example 51.84 is a tournament where the condition on the number of times pairs of competitors play has been relaxed. To generalize the example, consider a game played in groups of size k with nk players and r rounds, each round being a partition of the players into n disjoint groups and every person plays at a table with every other person either λ or $\lambda + 1$ times ("approximate balance"). This design is a *resolvable regular graph design*, RRGD$(n, k : r)$, with $\lambda = \lfloor \frac{r(k-1)}{n-1} \rfloor$. There is an RRGD$(12, 4 : r)$ unless $2 \leq r \leq 7$ (see [1358] and §VI.24).

51.86 Remark In many instances, it is necessary to schedule a league with a fixed number of games played per week and a fixed number of weeks n. In this case bye weeks are often necessary and as in Remark 51.85 it is advantageous to maintain approximate balance of opponents. Generally one constructs this tournamment by finding base blocks and developing these modulo n.

51.87 Example A schedule for 17 players playing in foursomes at three available sites. Each player plays for 12 weeks and has 5 bye weeks. Each player plays with every other player exactly two times, except for four players that they play three times. Each player plays at each site exactly 4 times, and no player has two bye weeks in a row.

Develop the following three blocks $\{0, 5, 7, 8\}, \{3, 9, 13, 14\}$, and $\{2, 10, 12, 16\}$ modulo 17. The ith translate of block k $(1 \leq k \leq 3)$ are the players playing at site k in week i.

51.13 Tournaments for Trios or More

51.88 Example Suppose $3n$ golfers wish to play for n weeks. There are n starting times available and the golfers play in groups of three, so that (1) each golfer plays exactly once per week, (2) no golfer has the same starting time twice, and (3) no two golfers play in the same trio twice.

If condition 2 is ignored, then an RBIBD$(3n, 3, 1)$ could be used and the tournament could extend for $\frac{3n-1}{2}$ weeks with every pair of golfers in a trio exactly once. However, a solution to the problem as given is even easier to construct using MOLS. Let L_1, L_2, and L_3 be three MOLS of side n where L_i is on the symbol set P_i for $i = 1, 2, 3$ (the $3n$ players). Now superimpose the three squares. The triples in each cell are the trios, the columns correspond to the weeks, and the rows correspond to the n starting times.

If $n = 2$, 3, 6, or perhaps 10, this construction cannot be used. There is no solution for 2 or 3, and 10 is undecided. There are precisely six solutions for $n = 6$, up to isomorphism [1742]; one is

	Week 1			Week 2			Week 3			Week 4			Week 5			Week 6		
Time 1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Time 2	9	12	15	0	6	13	1	3	10	4	14	16	7	11	17	2	5	8
Time 3	3	7	14	8	10	12	2	11	16	1	13	17	5	6	15	0	4	9
Time 4	4	8	17	1	11	15	5	9	14	2	6	12	0	3	16	7	10	13
Time 5	5	11	13	7	9	16	0	12	17	3	8	15	2	4	10	1	6	14
Time 6	6	10	16	2	14	17	4	13	15	0	5	7	1	8	9	3	11	12

51.89 Remark Many times it is not the most important aspect of the tournament that every player plays against every other player. For example, if a tournament is played during the weeks of the summer, it may be more important that the number of rounds be fewer than 12. An example is Joyce Cook's golf league; thirty-nine golfers wish to play for ten weeks, under the conditions in 51.88. A solution exists using the first ten columns of three MOLS of side 13.

51.90 An r-tournament is a contest in which players meet r at a time in a race-type format, all r competing against each other and every r-set occurring as a race exactly once. With each race there is associated an ordering, reflecting the finishing order in the race. An r-tournament is *regular* if every player finishes in every position equally often.

51.91 Remark It is shown in [159] that a regular r-tournament exists if $n \geq r \geq 2$, $n \mid \binom{n}{r}$ and $\gcd(n, r)$ is a prime power. The other cases where $n \mid \binom{n}{r}$ are undecided. The ordering on the races could also represent starting position, which is important in many sports.

51.92 Remarks Resolvable r-tournaments have been closely studied in the case where $r = 3$. In this case, the races are triads (ordered triples) and the matches are partitioned into rounds. A round is *regular* if every team plays exactly once in each position in a round. (Regular rounds must contain n races.) A *triad design* is a partitioning of the set of triads into regular rounds. In particular, a *single triad design* STD(n) is a way of ordering the $\binom{n}{3}$ triples on an n-set and partitioning the resulting triads into $\frac{(n-1)(n-2)}{6}$ regular rounds, so it is a special kind of regular 3-tournament, and a *complete triad design* CTD(n) is a partitioning of all the $n(n-1)(n-2)$ triads on an n-set into $(n-1)(n-2)$ regular rounds. There is an STD(n) if and only if $(n,3) = 1$; there is a CTD(n) for every n [2109].

In one particular game, the desirable properties are (1) triples meet equally often in the tournament; (2) each player races two or three times per round; (3) each team races equally often in each position in the tournament; (4) no two players race twice in the same round; (5) there are about 15 rounds. A census of tournaments with these properties appears in [2109]. Condition (4) may be applied to triad designs in general; no STD(n) satisfying (4) exists for $n = 7$, and examples are known for $n = 8$, 10, 11, 13 [1160].

51.93 Remark In 1989, R.L. Graham offered \$100 for the solution to the following problem. Given n and r such that $n \mid \binom{n}{r}$, can one find a sequence $a_1, a_2, \ldots, a_{\binom{n}{r}}$ of members of $\{1, 2, \ldots, n\}$ such that the $\binom{n}{r}$ consecutive subsets $\{a_i, a_{i+1}, \ldots, a_{i+r-1}\}, 1 \le i \le \binom{n}{r}$, are distinct? (Indices are reduced modulo $\binom{n}{r}$.) It is pointed out in [159] that a positive answer implies a regular r-tournament for n players.

51.14 Miscellaneous Examples

51.94 Example World Motorcycle Speedway Championships. Until the late 1990s, the final was 20 heats for 16 riders (4 in a race) and the schedule was precisely the affine plane AG(2, 4), divided into parallel classes. So there were five rounds where each round consisting of 4 heats is a parallel class in the affine plane. See [824, 369].

This schedule is still used for many major tournaments, but the championship itself is now based on the following complicated multiple-elimination. Sixteen riders compete in heats of four. In the first four heats each rides once. Then the following schedule is followed.

Heats 1 to 4	1st, 2nd to heats 7, 8	Heats 11 and 12	1st to final (heat 14)
	3rd, 4th to heats 5, 6		2nd, 3rd to heat 13
Heats 5 and 6	1st, 2nd to heats 9, 10		4th eliminated
	3rd, 4th eliminated	Heat 13	1st, 2nd to final
Heats 7 and 8	1st, 2nd to heats 11, 12	Heat 13	1st, 2nd to final
	3rd, 4th to heats 9, 10		3rd, 4th eliminated
Heats 9 and 10	1st, 2nd to heats 11, 12	Heat 14	final
	3rd, 4th eliminated		

Some variation can occur at the end—for example, the first and second in heats 11 and 12 could go directly to the final, with the others eliminated.

In the world championship itself, the top eight competitors are seeded to a second round; 16 more compete in a copy of heats 1 to 10 to select the best eight; these eight and the eight seeds compete in a copy of the elimination.

51.95 Example World Cup Soccer. Contested over every four years, 24 teams qualify for the tournament after two years of preliminary matches. The teams are then divided into six groups (of four teams each) in the first round and play round robin (three games). The top 16 teams then advance to a single elimination tournament.

51.96 Example National Football League. In 2002 the National Football League expanded to 32 teams and as a result realigned its divisional structure. In the NFL there are two conferences (the NFC and AFC), each composed of four divisions (North, South, East, West) containing four teams each. Each team plays a 16-game season (one game per week) and has exactly one bye week. Each pair of teams within a division plays 14 common opponents as follows: a home-and-away round robin within the division (6

games); each team plays the four teams from another division within its conference on a rotating three-year cycle (4 games); each team plays the four teams from a division in the other conference on a rotating four-year cycle (4 games). For the final two games, each team plays a pair of intraconference games based on the prior year's standings (first-place teams in a division play against the first-place teams from another division within the conference, and so on).

The schedule must also satisfy a number of other properties such as: when two teams play twice during the season, one should be in the first 8 weeks, the other should be in the last 8 weeks; no team should have 3 consecutive home or away games during the first 5 weeks or the last 3 weeks; no team should have three 3 consecutive home or away games more than once during the season and the entire league should have no more than 4 such runs; there are 4 byes per week for the weeks 3 through 10; other important constraints arise from television network scheduling.

In 2004, the National Football League awarded a multi-year contract to Optimal Planning Solutions, Inc. to assist in the creation of the league's regular season schedule. Their software package is based on a mathematical programming solver that is optimized for sports scheduling. (For the first 80 years of the league, the schedule was constructed essentially by hand.)

51.97 Example Major League Baseball. From 1982 through 2004, this large schedule (2,430 games in 26 weeks) was constructed on a personal computer by Holly and Henry Stevenson. In 2005, Major League Baseball awarded their scheduling contract to Sports Scheduling Group (a company consisting of 3 professors). They use advanced methods in combinatorial optimization to construct a schedule that not only satisfies the necessary conditions for the schedule (number of games, number of home games, number of games versus a particular opponent) but optimizes numerous other constraints such as travel distance, field availability, and TV network scheduling. One particular problem with the Stevenson's schedule was the existence of *semirepeaters*, blocks of games where two teams play nearly back-to-back series (for example, in 2004 the Cubs and Cardinals played 19 times in the first half of the season and no times in the second half). The new system reduces the number of such instances.

51.98 Example Czech National Hockey League and Czech National Soccer League. Typically, schedules with perfect or low carry-over effect do not have good home-away patterns. Often they force three or more away (or home) games in a row for some teams. There are soccer leagues in Europe that have good carry-over effects while not the best possible HAPs (Italy, for instance). It is known that a schedule for $2n$ teams with the best possible HAP with $2n-2$ breaks cannot have perfect carry-over effect. The CNHL and CNSL use schedules for 14 and 16 teams with 12 and 14 breaks, respectively, in which no team receives the carry-over effect from any other team more than three times.

51.99 Example Jai-alai. In the game of jai-alai, several players compete in each match but only two can compete at any one time. At any time there is an ordered list of competitors. The first two in the list play; the winner stays at the top of the list and the loser goes to the bottom. Thus the tournament structure is related to a pop-up stack. The winner scores one or more points (there are different methods for different types of events, and in different countries), and the first to amass a certain number of points wins. See [701] for a discussion of the advantages of different starting positions.

See Also

§VI.3	Balanced tournament designs are tournament designs with an additional balance on the courts.
§VI.50	Room squares give an arrangement for a round robin tournament.
§VI.29	Howell designs give incomplete tournaments played in rounds.
§VI.55	Starters are useful in constructing round robin tournaments
[977, 1580]	Contain many schedules for bridge tournaments.
[1933]	Contains a number of interesting schedules for duplicate bridge.
[1798]	A reference for ranking the teams in a tournament after the results of the games are known.
[1983]	Studies schedules of league play where there is more than one conference and the number of meetings between a pair of teams in the same conference may be different than the number of meetings between teams from different conferences.
[159, 701]	Discusses tournaments where there is an advantage to certain starting positions in each heat of a race. The schedules constructed in these papers balance for the starting positions.
[2074]	Web site containing many links related to sports scheduling.

References Cited: [95, 159, 369, 455, 572, 663, 701, 725, 727, 779, 815, 824, 835, 836, 877, 977, 1157, 1160, 1358, 1392, 1393, 1580, 1585, 1717, 1742, 1798, 1814, 1825, 1830, 1834, 1917, 1933, 1983, 2074, 2106, 2107, 2109]

52 Secrecy and Authentication Codes

K. Gopalakrishnan
Douglas R. Stinson

52.1 Secrecy Codes

52.1 **Remark** One fundamental goal of cryptography is to allow two people, Alice and Bob, to communicate over an insecure channel in such a way that an observer, Oscar, cannot understand what is being said. Alice encrypts the plaintext message, using a predetermined key, and sends the resulting ciphertext. Even if Oscar intercepts the ciphertext, he cannot determine the plaintext; but Bob, who knows the key, can decrypt the ciphertext and obtain the plaintext.

52.2 A *cryptosystem* or *secrecy code* is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where:

1. $\mathcal{P}$ is a finite set of possible *plaintexts*.
2. $\mathcal{C}$ is a finite set of possible *ciphertexts*
3. $\mathcal{K}$, the *keyspace*, is a finite set of possible *keys*.
4. For each $K \in \mathcal{K}$, there is an injective *encryption rule* $e_K \in \mathcal{E}$ and a corresponding *decryption rule* $d_K \in \mathcal{D}$. Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are such that $d_K(e_K(x)) = x$ for every plaintext $x \in \mathcal{P}$.

52.3 **Remark** Alice and Bob jointly choose a secret random key $K \in \mathcal{K}$. At a later time, when Alice wants to send $x \in \mathcal{P}$ to Bob, she encrypts x using the encryption rule e_K. That is, she computes $y = e_K(x)$ and sends y to Bob over the channel. When Bob receives y, he decrypts it using the decryption function d_K, obtaining x.

52.4 Suppose there is a probability distribution $p_{\mathcal{P}}$ on $\mathcal{P}$. A cryptosystem provides *perfect secrecy* provided that $p_{\mathcal{P}}(x|y) = p_{\mathcal{P}}(x)$ for every $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

52.5 **Remark** Informally, perfect secrecy means that observation of a ciphertext gives no information about the corresponding plaintext.

52.6 The *encryption matrix* of a cryptosystem is the $|\mathcal{K}| \times |\mathcal{P}|$ matrix in which the entry in row K ($K \in \mathcal{K}$) and column x ($x \in \mathcal{P}$) is $e_K(x)$.

52.7 **Theorem** In any cryptosystem that provides perfect secrecy, $|\mathcal{K}| \geq |\mathcal{P}|$. Further, equality occurs if and only if the encryption matrix is a latin square of order $|\mathcal{P}|$ and the encryption rules are used with equal probability.

52.8 **Remark** Shannon [1892] proved Theorem 52.7 in 1949; it is a fundamental result and it is probably the first theorem linking design theory and cryptography.

52.9 **Example** *Vernam one-time pad.* $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$ for some integer $n \geq 1$. For any $x = (x_1, \ldots, x_n) \in (\mathbb{Z}_2)^n$ and $K = (K_1, \ldots, K_n) \in (\mathbb{Z}_2)^n$, define

$$e_K(x) = (x_1 + K_1 \pmod 2, \ldots, x_n + K_n \pmod 2).$$

The encryption matrix is a latin square of order 2^n, and thus perfect secrecy is achieved.

52.10 **Remark** Example 52.9 assumes that each key is used for only one encryption. The theory can be extended in a natural way, assuming that each key is used to encrypt up to t plaintexts, where $t \geq 1$ is an integer.

52.11 For any $s \leq t$, suppose there is a probability distribution $p_{\binom{\mathcal{P}}{s}}$ on the set of s-subsets of $\mathcal{P}$. Let $P(s)$ denote the property:

$p_{\binom{\mathcal{P}}{s}}(X|Y) = p_{\binom{\mathcal{P}}{s}}(X)$ for every $X \subseteq \mathcal{P}$ and $Y \subseteq \mathcal{C}$ such that $|X| = |Y| = s$.

A cryptosystem provides *perfect t-fold secrecy* whenever $P(s)$ is satisfied for $1 \leq s \leq t$.

52.12 **Remark** Perfect t-fold secrecy means that observation of a set of at most t ciphertexts gives no information about the corresponding set of t plaintexts.

52.13 **Theorem** Suppose a perpendicular array $PA_\lambda(t, k, v)$ with $k \geq 2t - 1$ exists (§VI.38). Then there exists a cryptosystem (with k plaintexts, v ciphertexts, and $\lambda\binom{v}{t}$ encryption rules) that provides perfect t-fold secrecy.

52.14 **Remark** An outline of the proof of Theorem 52.13. If the transpose of a $PA_\lambda(t, k, v)$ is used as the encryption matrix of a cryptosystem and each of the $\lambda\binom{v}{t}$ encryption rules is chosen with equal probability, then it follows that property $P(t)$ is satisfied. However, property $P(s)$ must be satisfied for all $1 \leq s \leq t$. In other words, the $PA_\lambda(t, k, v)$ must also be a $PA_{\lambda(s)}(s, k, v)$ for $1 \leq s \leq t$. Such a perpendicular array is *inductive*. It is not hard to prove that any $PA_\lambda(t, k, v)$ is inductive provided $k \geq 2t - 1$.

52.15 **Remark** Theorem 52.16 gives a partial converse to Theorem 52.13.

52.16 **Theorem** Suppose a cryptosystem provides perfect t-fold secrecy and $|\mathcal{P}| \geq 2t - 1$. Then $|\mathcal{K}| \geq \binom{|\mathcal{P}|}{t}$, with equality if and only if the encryption matrix is the transpose of a perpendicular array $PA(t, |\mathcal{P}|, |\mathcal{P}|)$ and the encryption rules are used with equal probability.

52.2 Authentication Codes

52.17 Remark Authentication codes were invented in 1974 by Gilbert, MacWilliams, and Sloane and have been extensively studied in recent years. The general theory of unconditional authentication was developed by Simmons. Research in authentication codes has involved considerable use of various combinatorial designs. This section presents four different types of authentication codes (viz., authentication codes without secrecy, general authentication codes, authentication codes with secrecy, and authentication-codes with arbitration) and discusses their relation to combinatorial designs.

▷ Authentication without Secrecy

52.18 Remark The three participants are again designated Alice, Bob, and Oscar. Suppose that Oscar has the ability to introduce his own messages into the channel and/or to modify existing messages. The purpose of an authentication code is to protect the *integrity* of the message. That is, when Bob receives a message from Alice, he wants to be sure that it was really sent by Alice and was not tampered with by Oscar.

52.19 An *authentication code without secrecy* is a four-tuple $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$, where:

1. $\mathcal{S}$ is a finite set of plaintexts, *source states*.
2. $\mathcal{A}$ is a finite set of *authenticators*.
3. $\mathcal{K}$ is a finite set of *keys*.
4. For each $K \in \mathcal{K}$, there is an *authentication rule* $e_K \in \mathcal{E}$. Each $e_K : \mathcal{S} \to \mathcal{A}$.

An authentication code is represented by the $|\mathcal{E}| \times |\mathcal{S}|$ *authentication matrix*, in which the rows are indexed by authentication rules, the columns are indexed by source states, and the entry in row e and column s is $e(s)$.

52.20 Remark As before, Alice and Bob jointly choose a secret key $K \in \mathcal{K}$. At a later time, when Alice wants to communicate a source state $s \in \mathcal{S}$ to Bob, she uses the authentication rule e_K to produce the authenticator $a = e_K(s)$. The *message* $m = (s, a)$ is then sent over the channel. When Bob receives m, he verifies that $a = e_K(s)$ to authenticate the source state s. Two types of attacks are considered. When Oscar places a (new) message m' into the channel, this is *impersonation*. When Oscar sees a message m and changes it to a message $m' \neq m$, this is *substitution*. When Oscar performs impersonation or substitution, his goal is to have his bogus message $m' = (s', a')$ accepted as authentic by Bob, thus misleading Bob as to the source. That is, if e is the authentication rule being used (which is not known to Oscar), then he is hoping that $a' = e(s')$.

52.21 Given a probability distribution on $\mathcal{S}$, known to all the participants, Alice and Bob choose a probability distribution for $\mathcal{E}$, an *authentication strategy*. Once Alice and Bob have chosen their authentication strategy, it is possible to compute, for $i = 0, 1$, a *deception probability* denoted by P_{d_i}, which is the probability that Oscar can deceive Bob by impersonation and substitution, respectively. In computing the deception probabilities, Oscar is using an optimal strategy.

52.22 Theorem In any authentication code without secrecy, $P_{d_0} \geq 1/|\mathcal{A}|$ and $P_{d_1} \geq 1/|\mathcal{A}|$.

52.23 Remark It is of interest not only to minimize the deception probabilities, but also to minimize the number of authentication rules in the code. This is because the key, K, must be exchanged secretly between Alice and Bob, and thus the amount of information that must be kept secret is minimized. Theorem 52.24 gives the connection

between authentication codes and orthogonal arrays.

52.24 Theorem Suppose there exists an authentication code without secrecy for k source states and having l authenticators, in which $P_{d_0} = P_{d_1} = 1/l$. Then

1. $|\mathcal{E}| \geq l^2$, and equality occurs if and only if the authentication matrix is the transpose of an orthogonal array $OA(2, k, l)$ (with $\lambda = 1$) and the authentication rules are used with equal probability;
2. $|\mathcal{E}| \geq k(l-1)+1$, and equality occurs if and only if the authentication matrix is the transpose of an orthogonal array $OA_\lambda(2, k, l)$ where $\lambda = (k(l-1)+1)/l^2$, and the authentication rules are used with equal probability.

52.25 Suppose the same encoding rule is used for the transmission of i messages, which Oscar observes in the channel. Then, suppose that Oscar inserts a new message of his own choosing, hoping to have it accepted by Bob as authentic. This is *spoofing* of *order* i. The deception probability P_{d_i} is the probability that Oscar succeeds in deceiving Bob with an order i spoofing attack. An authentication code is *t-fold secure against spoofing* if $P_{d_i} = 1/l$ for $0 \leq i \leq t$.

52.26 Theorem Given an authentication code without secrecy that is $(t-1)$-fold secure against spoofing. Then $|\mathcal{E}| \geq |\mathcal{A}|^t$, and equality occurs if and only if the authentication matrix is the transpose of an orthogonal array $OA(t, |\mathcal{S}|, |\mathcal{E}|)$ and the authentication rules are used with equal probability.

52.27 Remark This is a natural generalization of the first part of Theorem 52.24. The generalization of the second part to t-fold secure authentication codes remains open.

▷ General Authentication Codes

52.28 Remark In the case of general authentication codes, one has an arbitrary message space $\mathcal{M}$; that is, a message does not consist of a source state with an appended authenticator. It is not a requirement that the message reveals the source state.

52.29 Theorem In a general authentication code,

$$P_{d_0} \geq \frac{|\mathcal{S}|}{|\mathcal{M}|} \quad \text{and} \quad P_{d_1} \geq \frac{|\mathcal{S}|-1}{|\mathcal{M}|-1}.$$

52.30 Remark Codes satisfying these bounds with equality and having the minimum number of authentication rules have been characterized in terms of Steiner 2-designs $S(2, k, v)$.

52.31 Theorem Suppose $P_{d_0} = |\mathcal{S}|/|\mathcal{M}|$ and $P_{d_1} = (|\mathcal{S}|-1)/(|\mathcal{M}|-1)$. Then

1. $|\mathcal{E}| \geq |\mathcal{M}|(|\mathcal{M}|-1)/(|\mathcal{S}|(|\mathcal{S}|-1))$, and equality occurs if and only if the authentication matrix is an $S(2, |\mathcal{S}|, |\mathcal{M}|)$, the authentication rules are used equiprobably, and the source states occur equiprobably.
2. $|\mathcal{E}| \geq |\mathcal{M}|$, and equality occurs if there is an $S(2, |\mathcal{S}|, |\mathcal{M}|)$ (this design is a symmetric BIBD). Further, equality occurs if and only if the authentication rules are used equiprobably, and the messages occur equiprobably.

52.32 Remark In part 2 of Theorem 52.31, it is not necessary that the authentication matrix of a code in which $|\mathcal{E}| = |\mathcal{M}|$ be a symmetric BIBD. In fact, there are examples of codes with $|\mathcal{E}| = |\mathcal{M}|$ for nonuniform source distributions where the authentication matrix is not a symmetric BIBD; see [1795].

52.33 Theorem (Massey) The deception probabilities of any general authentication code are bounded below by $P_{d_i} \geq \frac{|\mathcal{S}|-i}{|\mathcal{M}|-i}$.

52.34 A general authentication code is *t-fold secure against spoofing* if for $0 \le i \le t$,
$$P_{d_i} = \tfrac{|\mathcal{S}|-i}{|\mathcal{M}|-i}.$$

52.35 Theorem Suppose a general authentication code is t-fold secure against spoofing. Then
$$|\mathcal{E}| \ge \tfrac{\binom{|\mathcal{M}|}{t+1}}{\binom{|\mathcal{S}|}{t+1}},$$
and equality occurs only if the authentication matrix is an $S(t+1, |\mathcal{S}|, |\mathcal{M}|)$. Conversely, if there exists an $S(t+1, k, v)$, then there exists an authentication code for k equiprobable source states, having v possible messages and $\binom{v}{t+1}/\binom{k}{t+1}$ equiprobable authentication rules, that is t-fold secure against spoofing.

▷ Authentication with Secrecy

52.36 A (t, t')-code is an authentication code that is t-fold secure against spoofing and simultaneously provides perfect t'-fold secrecy.

52.37 Theorem Suppose there is an $S(2, k, v)$, where $v-1 \equiv 0 \pmod{k(k-1)}$. Then there is a $(1, 1)$-code for k equiprobable source states, having v messages and $v(v-1)/(k(k-1))$ equiprobable encoding rules.

52.38 Remark The authentication capability of the code is analogous to the situation of general authentication codes. To provide for perfect secrecy, every block of the $S(2, k, v)$ must be ordered in such a way that every point occurs in each possible position in exactly $(v-1)/(k(k-1))$ blocks. A necessary condition for this to be possible is $v - 1 \equiv 0 \pmod{k(k-1)}$, since every point occurs in exactly $(v-1)/(k-1)$ blocks. That this condition is also sufficient can be demonstrated by finding suitable systems of distinct representatives.

52.39 An *authentication perpendicular array* $\mathrm{APA}_\lambda(t, k, v)$ is a $\mathrm{PA}_\lambda(t, k, v)$ such that, for any $s \le t-1$ and for any $s+1$ distinct symbols x_i $(1 \le i \le s+1)$, it holds that among the columns of the PA that contain all the symbols x_i $(1 \le i \le s+1)$, the s symbols x_i $(1 \le i \le s)$ occur in all possible subsets of s columns equally often.

52.40 Remark Authentication perpendicular arrays are discussed in §VI.38.

52.41 Theorem If there exists an $\mathrm{APA}_\lambda(t, k, v)$, then there exists an authentication code that is $(t-1)$-fold secure against spoofing and provides t-fold secrecy for k equiprobable source states, having v messages and $\lambda\binom{v}{t}$ encoding rules. The code is optimal if and only if $\lambda = 1$.

52.42 Remark It was pointed out in Theorem 52.13 that (inductive) perpendicular arrays $\mathrm{PA}_\lambda(t, k, v)$ yield codes having t-fold secrecy. If one employs an $\mathrm{APA}_\lambda(t, k, v)$, then a $(t-1, t)$-code is obtained.

52.43 Example An $\mathrm{APA}(2, 3, 11)$. Construct a 3×55 array A by developing these five columns modulo 11:

0	0	0	0	0
1	9	3	4	5
2	7	6	8	10

Any unordered pair $\{x, y\}$ occurs in three columns of A. Within these three columns, x occurs once in each of the three rows, as does y.

▷ Authentication with Arbitration

52.44 Remark Authentication with arbitration deals with the situation where Alice and Bob do not trust each other. Motivated by this scenario, Simmons described a variation of authentication codes that protect against certain "insider attacks." A trusted *arbiter* is an essential feature of these schemes, which are sometimes termed A^2 *codes*. The arbiter chooses an *encoding rule* e_K that is given only to Alice and a *verification rule* f_K that is given only to Bob. Later, the arbiter resolves any disputes that occur. As well as impersonation or substitution by an outsider, authentication with arbitration protects against three kinds of insider attacks:

1. *Impersonation by the transmitter* occurs when Alice may claim not to have sent a message to Bob when, in fact, she did. The attack succeeds if Bob accepts the message as authentic, and the arbiter confirms that the message was not generated using Alice's encoding rule.
2. *Impersonation by the receiver* refers to the situation when Bob claims to receive a message from Alice when he did not. The attack succeeds if the arbiter confirms that Alice could have generated the message using her encoding rule.
3. *Substitution by the receiver* occurs when Bob receives a message m from Alice, and then claims to have received a different message, m'. The attack succeeds if the arbiter confirms that Alice could have constructed m' using her encoding rule.

52.45 Construction [1201] An A^2 code. Fix a line L in the projective geometry $\mathrm{PG}(3, q)$. The $q + 1$ points on L are source states. Alice's encoding rule e_K is a line that does not intersect L. Bob's verification rule f_K is a point on e_K. In order to transmit source state s to Bob, Alice sends Bob the plane M generated by s and the line e_K. Bob reconstructs s by intersecting M and L, and he accepts the message if $f_K \in M$.

52.46 Theorem In the code described, there are $q + 1$ source states, $q^3 + q^2$ possible messages, $q^3 + q^2$ possible verification rules, and q^4 encoding rules. Moreover, the success probability for any insider or outsider attack is bounded above by $1/q$.

See Also

§III.1	Secrecy codes are characterized using latin squares.
§III.3	Orthogonal arrays of strength 2.
§III.7	Orthogonal arrays of strength $t > 2$.
§VI.38	Perpendicular arrays and authentication perpendicular arrays.
[1892]	Shannon's classic paper on secrecy systems.
[1916]	A survey on authentication codes.
[906]	The paper that introduced authentication codes.
[1795, 1968, 1969]	Gives connections between authentication codes and designs.
[1201, 1202, 1914]	Information about authentication with arbitration.
[1972]	Chapter 9 discusses authentication.
[1725]	A monograph on the role of combinatorial designs in authentication codes.

References Cited: [906, 1201, 1202, 1725, 1795, 1892, 1914, 1916, 1968, 1969, 1972]

53 Skolem and Langford Sequences

Nabil Shalaby

53.1 Definitions and Examples

53.1 A *Skolem sequence* of order n is a sequence $S = (s_1, s_2, \ldots, s_{2n})$ of $2n$ integers satisfying the conditions

1. for every $k \in \{1, 2, \ldots, n\}$ there exist exactly two elements $s_i, s_j \in S$ such that $s_i = s_j = k$, and
2. if $s_i = s_j = k$ with $i < j$, then $j - i = k$.

Skolem sequences are also written as collections of ordered pairs $\{(a_i, b_i) : 1 \leq i \leq n, b_i - a_i = i\}$ with $\bigcup_{i=1}^{n}\{a_i, b_i\} = \{1, 2, \ldots, 2n\}$.

53.2 **Example** A Skolem sequence of order 5: $S = (1, 1, 3, 4, 5, 3, 2, 4, 2, 5)$ or, equivalently, the collection $\{(1, 2), (7, 9), (3, 6), (4, 8), (5, 10)\}$.

53.3 An *extended Skolem sequence* of order n is a sequence ES $= (s_1, s_2, \ldots s_{2n+1})$ of $2n + 1$ integers satisfying conditions 1 and 2 of the definition and

3. there is exactly one $s_i \in ES$ such that $s_i = 0$.

The element $s_i = 0$ is the *hook* or *zero* of the sequence.

53.4 A *hooked Skolem sequence* HS of order n is an extended Skolem sequence of order n with $s_{2n} = 0$.

53.5 **Example** A hooked Skolem sequence of order 6 that is also an extended Skolem sequence of order 6: $(1, 1, 2, 5, 2, 4, 6, 3, 5, 4, 3, 0, 6)$.

53.6 A *Langford sequence* of order n and defect $d, n > d$, is a sequence $L = (l_1, l_2, \ldots, l_{2n})$ of $2n$ integers satisfying the conditions

1. for every $k \in \{d, d+1, \ldots, d+n-1\}$ there exist exactly two elements $l_i, l_j \in L$ such that $l_i = l_j = k$, and
2. if $l_i = l_j = k$ with $i < j$, then $j - i = k$.

53.7 A *near-Skolem sequence* of order n and defect $m, n \geq m$, is a sequence NS $= (s_1, s_2, \ldots, s_{2n-2})$ of $2n - 2$ integers satisfying the conditions

1. for every $k \in \{1, 2, \ldots, m-1, m+1, \ldots n\}$, there exist exactly two elements $s_i, s_j \in$NS, such that $s_i = s_j = k$, and
2. if $s_i = s_j = k$ with $i < j$, then $j - i = k$.

53.8 **Remark** The *(extended) hooked Langford* and *(extended) hooked near-Skolem* sequences are defined in a manner similar to that of the (extended) hooked Skolem sequence. When the hook of an extended Skolem sequence is in the middle position ($n + 1$ position), then the sequence is known as *Rosa* or a *split Skolem* sequence of order n.

53.9 **Examples** A Langford sequence of order 5 and defect 3, a near-Skolem sequence of order 7 and defect 4, a hooked Langford sequence of order 4 and defect 2, and a hooked near-Skolem sequence of order 7 and defect 3, respectively.

$$\text{L} = (7, 5, 3, 6, 4, 3, 5, 7, 4, 6) \qquad \text{NS} = (1, 1, 6, 3, 7, 5, 3, 2, 6, 2, 5, 7)$$
$$\text{HL} = (4, 5, 6, 2, 4, 2, 5, 0, 6) \qquad \text{HNS} = (2, 5, 2, 4, 6, 7, 5, 4, 1, 1, 6, 0, 7)$$

53.2 Existence

53.10 Theorems (see [51, 138])

1. (Skolem) A Skolem sequence of order n exists if and only if $n \equiv 0, 1 \pmod 4$. When $n = 1$, take (1,1). When $n = 4$, take (1,1,3,4,2,3,2,4). When $n = 5$, take (2,4,2,3,5,4,3,1,1,5). When $n > 5$, use the construction (as ordered pairs):

$$n = 4s: \begin{cases} (4s + r - 1, 8s - r + 1) & r = 1, \ldots, 2s \\ (r, 4s - r - 1) & r = 1, \ldots, s - 2 \\ (s + r + 1, 3s - r) & r = 1, \ldots, s - 2 \\ (s - 1, 3s),\ (s, s + 1),\ (2s, 4s - 1),\ (2s + 1, 6s) \end{cases}$$

$$n = 4s + 1: \begin{cases} (4s + r + 1, 8s - r + 3) & r = 1, \ldots, 2s \\ (r, 4s - r + 1) & r = 1, \ldots, s \\ (s + r + 2, 3s - r + 1) & r = 1, \ldots, s - 2 \\ (s + 1, s + 2),\ (2s + 1, 6s + 2),\ (2s + 2, 4s + 1) \end{cases}$$

2. (O'Keefe) A hooked Skolem sequence of order n exists if and only if $n \equiv 2, 3 \pmod 4$. When $n = 2$, take (1,1,2,0,2). When $n = 3$, take (3,1,1,3,2,0,2). For $n \geq 6$, use the construction (as ordered pairs):

$$n = 4s + 2: \begin{cases} (r, 4s - r + 2) & r = 1, \ldots, 2s \\ (4s + r + 3, 8s - r + 4) & r = 1, \ldots, s - 1 \\ (5s + r + 2, 7s - r + 3) & r = 1, \ldots, s - 1 \\ (2s + 1, 6s + 2),\ (4s + 2, 6s + 3), & \\ (4s + 3, 8s + 5),\ (7s + 3, 7s + 4) & \end{cases}$$

$$n = 4s - 1: \begin{cases} (4s + r, 8s - r - 2) & r = 1, \ldots, 2s - 2 \\ (r, 4s - r - 1) & r = 1, \ldots, s - 2 \\ (s + r + 1, 3s - r) & r = 1, \ldots, s - 2 \\ (s - 1, 3s), (s, s + 1), (2s, 4s - 1), (2s + 1, 6s - 1), (4s, 8s - 1) & \end{cases}$$

3a. (Abrham and Kotzig) An extended Skolem sequence of order n exists for all n.

3b. (Baker) An extended Skolem sequence of order n exists for all positions i of the zero if and only if i is odd and $n \equiv 0, 1 \pmod 4$ or i is even and $n \equiv 2, 3 \pmod 4$.

53.11 Theorems [1918] A Langford sequence of order n and defect d exists if and only if

1. $n \geq 2d - 1$, and
2. $n \equiv 0, 1 \pmod 4$ and d is odd, or $n \equiv 0, 3 \pmod 4$ and d is even.

A hooked Langford sequence of order n and defect d exists if and only if

1. $n(n - 2d + 1) + 2 \geq 0$, and
2. $n \equiv 2, 3 \pmod 4$ and d is odd, or $n \equiv 1, 2 \pmod 4$ and d is even.

53.12 Theorem [1467] If $n \geq 2d - 1$ and $n \notin [2d + 2, 8d - 5]$, then there exists a k-extended Langford sequence of order n, defect d, and all positions k of the zero whenever $(n, k) \equiv (0, 1), (1, d), (2, 0), (3, d + 1) \pmod{(4, 2)}$.

53.13 Theorem [138, 1466, 1467] The necessary conditions for the existence of a k-extended Langford sequence of order n and defect d, $1 \leq d \leq 4$, are sufficient.

53.14 Theorem [1888] A near-Skolem sequence of order n and defect m exists if and only if $n \equiv 0, 1 \pmod 4$ and m is odd, or $n \equiv 2, 3 \pmod 4$ and m is even. A hooked near-Skolem sequence of order n and defect m exists if and only if $n \equiv 0, 1 \pmod 4$ and m is even, or $n \equiv 2, 3 \pmod 4$ and m is odd.

53.15 Theorem [1889] The necessary conditions for the existence of near-Rosa and hooked near-Rosa sequences are sufficient.

53.16 Remark There are numerous open problems of the existence of related generalizations of Skolem–Langford sequences (see [1888, 1685]).

53.3 Connections with Other Designs

53.17 Construction A cyclic Steiner triple system STS($6n+1$). Suppose that $\{1,\dots,3n\}$ can be partitioned into m triples $\{a,b,c\}$ such that $a+b=c$ or $a+b+c\equiv 0 \pmod{6n+1}$. (This is the *first Heffter difference problem*.) Then the set of all triples $\{0,a,a+b\}$ is a $(6n+1,3,1)$ cyclic difference family, the base blocks for an STS($6n+1$). From a Skolem sequence or hooked Skolem sequence of order n (Theorem 53.10), construct the pairs (b_r,a_r) such that $b_r-a_r=r$, for $1\le r\le n$. The set of all triples (r,a_r+n,b_r+n), for $1\le r\le n$, is a solution to the first Heffter difference problem.

53.18 Example The Skolem sequence of order 4, $S=(1,1,4,2,3,2,4,3)$ yields the pairs $\{(2,1),(6,4),(8,5),(7,3)\}$. These pairs in turn give the triples $\{(1,5,6),\ (2,8,10),\ (3,9,12),(4,7,11)\}$ forming a solution of the first Heffter problem. These triples yield base blocks for an STS(25): $\{0,1,6\},\{0,2,10\},\{0,3,12\},\{0,4,11\}$.

53.19 Construction A cyclic Steiner triple system STS($6n+3$) [1820]. Suppose $\{1,\dots,3n+1\}\backslash\{2n+1\}$ can be partitioned into m triples $\{a,b,c\}$ such that $a+b=c$ or $a+b+c\equiv 0 \pmod{6n+3}$. (This is the *second Heffter difference problem*). Then the set of all triples $\{0,a,a+b\}$, together with the "short block" $\{0,2n+1,4n+2\}$, is a $(6n+3,3,1)$ cyclic partial difference family, the base blocks for an STS($6n+3$). Heffter's second difference problem is solved using extended Skolem sequences of order n with a hook in the nth position; from such a sequence, construct the pairs (b_r,a_r) such that $b_r-a_r=r$, for $1\le r\le n$. Then take the set of all triples (r,a_r+n,b_r+n), for $1\le r\le n$.

An explicit construction for the required extended Skolem sequences (as ordered pairs):

$$
\begin{array}{ll}
n=4s: & \left\{\begin{array}{ll}
(r,4s-r+1) & r=1,\dots,s-1\\
(s+r-1,3s-r) & r=1,\dots,s-1\\
(4s+r+1,8s-r+1) & r=1,\dots,s-1\\
(5s+r+1,7s-r+1) & r=1,\dots,s-1\\
(2s-1,2s),\ (3s,5s+1),\ (3s+1,7s+1),\ (6s+1,8s+1)
\end{array}\right.\\[2ex]
n=4s+1: & \left\{\begin{array}{ll}
(r,4s-r+2) & r=1,\dots,2s\\
(5s+r,7s-r+3) & r=1,\dots,s\\
(4s+r+2,8s-r+3) & r=1,\dots,s-2\\
(2s+1,6s+2),\ (6s+1,8s+4),\ (7s+3,7s+4)
\end{array}\right.\\
(n>5) & \\[2ex]
n=4s+2: & \left\{\begin{array}{ll}
(r,4s-r+3) & r=1,\dots,2s\\
(4s+r+4,8s-r+4) & r=1,\dots,s-1\\
(5s+r+3,7s-r+3) & r=1,\dots,s-2\\
(2s+1,6s+3),\ (2s+2,6s+2),\ (4s+4,6s+4),\\
(7s+3,7s+4),\ (8s+4,8s+6)
\end{array}\right.\\
(n>2) & \\[2ex]
n=4s-1: & \left\{\begin{array}{ll}
(r,4s-r) & r=1,\dots,2s-1\\
(4s+r+1,8s-r) & r=1,\dots,s-2\\
(5s+r,7s-r-1) & r=1,\dots,s-2\\
(2s,6s-1),\ (5s,7s+1),\ (4s+1,6s),\ (7s-1,7s)
\end{array}\right.
\end{array}
$$

When $n=2$, take the sequence $\{(1,2),(4,6\}$; when $n=5$, take

$$\{(1,5),(2,7),(3,4),(8,10),(9,12)\}.$$

When $n=1$, the sequence does not exist; indeed, there is no cyclic STS(9).

53.20 Remark A Skolem sequence of order n is equivalent to a starter (coming from Skolem) in $\mathbb{Z}_{2n+1}$ by taking the set of pairs of subscripts of the numbers $1, \ldots, n$. Thus special types of Skolem and extended Skolem sequences produce special types of starters.

53.21 Example $S = (5, 6, 7, 8, 2, 5, 2, 6, 4, 7, 3, 8, 4, 3, 1, 1)$ is a Skolem sequence of order 8. It gives a strong starter in $\mathbb{Z}_{17}$: $\{\{15, 16\}, \{5, 7\}, \{11, 14\}, \{9, 13\}, \{1, 6\}, \{3, 10\}, \{4, 12\}\}$

53.22 Theorem [51] The existence of an extended Skolem sequence implies the existence of a unique additive permutation.

53.23 Example $S = (3, 1, 1, 3, 4, 2, 0, 2, 4)$ produces a unique additive permutation $y = (3, 1, -1, -3, 4, 2, 0, -2, -4)$ of $f = (-4, -3, -2, -1, 0, 1, 2, 3, 4)$, such that $y + f = z = (-1, -2, -3, -4, 4, 3, 2, 1, 0)$ is another permutation of f.

53.24 Remark A recursive theorem of Rosa (1975) uses the existence of Skolem sequences: If there is a large set of Steiner triple systems on v points, then there is a large set of Steiner triple systems on $2v + 1$ points.

53.4 Enumeration of Sequences

53.25 Theorems [50] Lower bounds on Skolem and Langford sequences.

1. The number of distinct Skolem sequences of order $n, \sigma_n \geq 2^{\lfloor n/3 \rfloor}$.
2. The number of distinct extended Skolem sequences of order $n, \epsilon_n \geq 2^{\lfloor n/3 \rfloor}$.
3. The number of extremal Langford sequences with defect d, $l_n \geq 4^{\lfloor (d-1)/3 \rfloor}$ (the Langford sequences with the smallest order n that satisfy the necessary conditions for Theorem 53.11).

53.26 Remark Bennett, Grannell, and Griggs [213] have extended the lower bound of $2^{\lfloor n/3 \rfloor}$ to the number of hooked Skolem, Rosa, and hooked Rosa sequences.

53.27 Table The number N_S of distinct Skolem sequences of order $n \leq 21$.

n	1	4	5	8	9	12	13	16
N_S	1	6	10	504	2656	455936	3040560	1400156768

n	17	20	21
N_S	12248982496	11435578798976	123564928167168

53.28 Table The number N_H of distinct hooked Skolem sequences of order $n \leq 15$.

n	2	3	6	7	10	11	14	15
N_H	1	2	38	124	12808	72648	21878816	168870048

53.29 Table [1745] The number N_E of distinct extended Skolem sequences of order $n \leq 16$.

n	1	2	3	4	5	6	7	8	9	10	11
N_E	2	2	6	22	48	160	636	3556	19488	95872	594320

n	12	13	14	15	16
N_E	4459888	32131648	227072544	1875064880	17851780784

53.30 Table (see [1604]) The number N_L of distinct Langford sequences ($d = 2$) of order $n \leq 23$.

n	3	4	7	8	11	12	15	16
N_L	2	2	52	300	35584	216288	79619280	653443600

n	19	20	23
N_L	513629782560	5272675722400	7598911885030976

53.31 Remarks

1. In all of the tables, the sequence and its reverse are considered distinct.
2. Many computer scientists are using the number of distinct Langford sequences of order n and defect $d = 2$ as a benchmark for testing new algorithms [1001, 1181].
3. The website [1604] has a nice discussion of the enumeration of Langford sequences.

53.32 Table The number N_{HL} of distinct hooked Langford sequences (d =2) of order $n \leq 14$.

n	2	5	6	9	10	13	14
N_{HL}	1	6	18	1348	6824	1534048	10938744

53.33 Table The number N_{EL} of distinct extended Langford sequences ($d = 2$) of order $n \leq 14$.

n	1	2	3	4	5	6	7	8	9
N_{EL}	1	2	6	10	22	76	364	1876	8316

n	10	11	12	13	14
N_{EL}	467668	320208	2127544	13974760	107492000

See Also

§II.2	Skolem sequences generate cyclic Steiner triple systems.
§VI.2	Generalizations of Skolem sequences generate balanced ternary designs.
§VI.16	Skolem sequences generate difference families.
§VI.55	Starters are generalizations of Skolem sequences.
[139]	Disjoint Skolem sequences generate disjoint cyclic Steiner and Mendelsohn systems and 1-covering designs.
[388]	Hooked Skolem and Hooked Rosa sequences were used to construct cyclic k-cycle systems for the complete graph.
[575]	Langford sequences are used to construct 2-factorizations of $2K_n$.
[770]	An application of Heffter's difference problem to the construction of codes resistant to random interference.
[936]	An application of Langford sequences to the construction of binary sequences with controllable complexity.
[1181]	Use parallel processing algorithms to find the number of distinct Langford sequences.
[1199]	Skolem sequences are used to construct k-rotational Steiner triple systems.
[1791]	Constucts simple indecomposable twofold cyclic triple systems from a generalizations of Skolem and Rosa sequences.
[1888]	Contains generalizations of Skolem sequences and their relations to designs and graph labelings. Also contains a detailed bibliography.
[2200]	Langford sequences are used to construct cyclic balanced sampling plans that avoid the selection of adjacent units.

References Cited: [50, 51, 138, 139, 213, 388, 575, 770, 936, 1001, 1181, 1199, 1466, 1467, 1604, 1685, 1745, 1791, 1820, 1888, 1889, 1918, 2200]

54 Spherical Designs

Akihiro Munemasa

54.1 Definitions and Examples

54.1 Let d be a positive integer greater than 1. Let$(a)_0 = 1$, and $(a)_n = a(a+1)\cdots(a+n-1)$, $(a \in \mathbb{R},\ n \in \mathbb{N})$. Let ε denote 0 or 1. The *Gegenbauer polynomials* $Q_k(x)$, $Q_k^\varepsilon(x)$, of degree $k = 0, 1, 2, \ldots$ are given by $Q_{2k+\varepsilon}(x) = x^\varepsilon Q_k^\varepsilon(x^2)$ and $Q_k^\varepsilon(x) = \sum_{r=0}^{k}(-1)^{k-r}\binom{k}{r}(\frac{d}{2}+2k+\varepsilon-1)\{(\frac{d}{2})_{k+r+\varepsilon-1}/(\frac{1}{2})_{r+\varepsilon}k!\}x^r$.

54.2 Let $\Omega_d = \{x \in \mathbb{R}^d : |x| = 1\}$ be the unit sphere in $\mathbb{R}^d$. A *spherical t-design* is a finite nonempty subset X of Ω_d satisfying

$$\sum_{x,y\in X} Q_k(\langle x, y\rangle) = 0,\ \forall k = 1, 2, \ldots, t,$$

where $\langle x, y\rangle$ denotes the standard euclidean inner product.

54.3 Remark The most natural definition of a spherical t-design is that X is a spherical t-design if and only if one is able to determine *exactly* the average value on Ω_d of any polynomial f of total degree at most t by sampling f at the points of X:

$$\frac{1}{\text{volume}(\Omega_d)}\int_{\Omega_d} f(\xi)d\xi = \frac{1}{|X|}\sum_{x\in X} f(x).$$

54.4 Examples

1. A nonempty subset $X \subseteq \Omega_d$ is a spherical 1-design if and only if its center of mass is the origin. X is a spherical 2-design if and only if it is a 1-design and is the image of v orthogonal vectors of the same length in $\mathbb{R}^v$ under the orthogonal projection onto (a copy of) $\mathbb{R}^d$. A spherical 2-design is known as a *eutactic star*.
2. A regular $(t+1)$-gon in Ω_2 is a spherical t-design and, conversely, for a spherical t-design $X \subseteq \Omega_2$, $t+1 \le |X| \le 2t+1$ implies that X is a regular polygon; if $|X| = 2t+2$, X is the union of two regular $(t+1)$-gons.
3. In Ω_3, the tetrahedron is a spherical 2-design. The octahedron and the cube are spherical 3-designs. The icosahedron and the dodecahedron are spherical 5-designs.

54.2 Constructions of Spherical Designs

54.5 Examples

1. The set of $d+1$ vertices of the regular simplex is a spherical 2-design in Ω_d.
2. The set of $2d$ vertices of the cross polytope, $(1, 0, \ldots, 0)^{PS}$, where v^{PS} denotes the orbit of a vector v whose coordinates are subject to permutations and sign changes, is a spherical 3-design in Ω_d.
3. The set of 2^d vertices of the d-cube is a spherical 3-design in Ω_d.
4. The (scaled) root system E_8 is a spherical 7-design of 240 points in Ω_8 consisting of vectors $\frac{1}{\sqrt{2}}(1, 1, 0, \ldots, 0)^{PS}$, $\frac{1}{2\sqrt{2}}(\pm 1, \ldots, \pm 1)$ (even numbers of -1s).
5. The set of 196560 shortest vectors of the Leech lattice Λ_{24}, scaled to lie in Ω_{24}, is a spherical 11-design.

54.6 The *angle set* of X is $A = \{\langle x, y\rangle \mid x, y \in X, x \neq y\}$. The *subconstituent* of X with respect to $\alpha \in A$ and $x \in X$ is $X_\alpha(x) = \{z \in X \mid \langle x, z\rangle = \alpha\}$.

54.7 Theorem For a spherical t-design X in Ω_{d+1}, write $A^* = A\backslash\{-1\}$, $s^* = |A^*|$. The *derived design* $D_\alpha(X)$ of X with respect to $\alpha \in A^*$ and $n \in X$ is the orthogonal projection of the subconstituent $X_\alpha(n)$ onto the hyperplane $\langle x, n\rangle = 0$, scaled to lie in Ω_d. It is a $(t+1-s^*)$-design with angle set contained in $\{(\beta-\alpha^2)/(1-\alpha^2) \mid \beta \in A^*\}$.

54.8 Theorem Let G be a finite subgroup of the real orthogonal group $O(d, \mathbb{R})$, and let $\mathrm{Harm}^G(k)$ denote the space of G-invariant harmonic homogeneous polynomials of degree k in d variables. If $\mathrm{Harm}^G(k) = 0$ for $1 \leq k \leq t$, then every orbit of G of a point on Ω_d forms a spherical t-design.

If, moreover, $\dim \mathrm{Harm}^G(t+1) = 1$ and $\mathrm{Harm}^G(k) = 0$ for $t+1 < k \leq t'$, then some orbit of G of a point on Ω_d forms a spherical t'-design.

54.9 Table Examples of finite groups $G \subset O(d, \mathbb{R})$ satisfying the hypotheses of Theorem 54.8.

G	d	t	t'	G	d	t	t'
$W(H_3)$	3	5	9	$W(E_7)$	7	5	7
$W(F_4)$	4	5	7	$W(E_8)$	8	7	11
$W(H_4)$	4	11	19	$Co.0$	24	11	15

54.10 Theorem Let L be a d-dimensional even unimodular lattice with minimum squared norm $2[\frac{d}{24}]+2$. Then every layer of L, when suitably scaled to lie on Ω_d, is a spherical 11-design if $d \equiv 0 \pmod{24}$, a spherical 7-design if $d \equiv 8 \pmod{24}$, and a spherical 3-design if $d \equiv 16 \pmod{24}$.

54.11 Examples Every layer of the E_8-lattice is a spherical 7-design, and every layer of the Leech lattice is a spherical 11-design. There are three 48-dimensional even unimodular lattices with minimum squared norm 6 known, and every layer of any of these lattices is a spherical 11-design.

54.12 Examples A lattice is *strongly perfect* if its shortest vectors form a spherical 5-design when suitably scaled. Strongly perfect lattices have been classified up to dimension 12. The Barnes–Wall lattices give an infinite family of 7-designs in Ω_{2^n}. Every extremal 32-dimensional even unimodular lattice is strongly perfect, giving a spherical 7-design with 146880 points. In Table 54.15, those spherical designs coming from strongly perfect lattices are marked as "SPL". See Tables 19.1 and 19.2 of [1527] for other lattices.

54.13 Construction From strongly regular graphs (§VII.11) or association schemes (§VI.1), one obtains spherical designs. If $A_0 = I, A_1, \ldots, A_s$ are the adjacency matrices of a symmetric s-class association scheme on v points and $E = \frac{1}{v}\sum_{i=0}^{s} \theta_i^* A_i$ is a nontrivial primitive idempotent, then the row vectors of E, suitably scaled to lie in Ω_d, form a spherical t-design with angle set $\{\theta_i^*/\theta_0^* : i = 1, \ldots, s\}$, where $t \geq 2$. The Krein parameter q_{11}^1 corresponding to $E_1 := E$ is zero if and only if $t \geq 3$.

54.14 Examples Every strongly regular graph on v points can be represented by v points on the sphere by Construction 54.13. Together with their antipodes, these form a spherical t-design of $2v$ points with $t \geq 3$. For designs obtained by this method, the parameters of the strongly regular graphs are given as $\supset$SRG(v,k,λ,μ) in Table 54.15.

54.15 Table Example of spherical designs obtained from lattices or association schemes.

	d	v	A	t	Description	Comments
1	24	196560	$A_{24} = \{-1, 0, \pm\frac{1}{4}, \pm\frac{1}{2}\}$	11*	Λ_{24}	SPL, Q
2	23	4600	$\{-1, 0, \pm\frac{1}{3}\}$	7*	$D_{1/2}$ of **1**	SPL, Q →SRG(2300,891,378,324)
3	22	891	$\{-\frac{1}{2}, -\frac{1}{8}, \frac{1}{4}\}$	5	$D_{1/3}$ of **2**	Q
4	22	2816	$\{-1, 0, \pm\frac{1}{3}\}$	5	D_0 of **2**	SPL, Q →SRG(1408,567,246,216)
5	23	47104	$\{-\frac{3}{5}, -\frac{1}{3}, -\frac{1}{15}, \frac{1}{5}, \frac{7}{15}\}$	7	$D_{1/4}$ of **1**	Q
6	22	2025	$\{-\frac{4}{11}, -\frac{1}{44}, \frac{7}{22}\}$	4	$D_{7/15}$ of **5**	Q
7	22	15400	$\{-\frac{2}{3}, -\frac{7}{18}, -\frac{1}{9}, \frac{1}{6}, \frac{4}{9}\}$	4	$D_{1/5}$ of **5**	
8	22	22275	$\{-\frac{17}{28}, -\frac{19}{56}, -\frac{1}{14}, \frac{11}{56}, \frac{13}{28}\}$	4	$D_{-1/15}$ of **5**	
9	22	7128	$\{-\frac{1}{2}, -\frac{1}{5}, \frac{1}{10}, \frac{2}{5}\}$	5	$D_{-1/3}$ of **5**	Q
10	22	275	$\{-\frac{1}{4}, \frac{1}{6}\}$	4*	$D_{-3/5}$ of **5** $D_{1/5}$ of **15**	SRG(275,112,30,56)
11	21	162	$\{-\frac{2}{7}, \frac{1}{7}\}$	3	$D_{1/6}$ of **10**	SRG(162,56,10,24)
12	21	112	$\{-\frac{1}{3}, \frac{1}{9}\}$	3	$D_{-1/4}$ of **10**	SRG(112,30,2,10)
13	23	93150	A_{24}	7	D_0 of **1**	
14	22	43164	A_{24}	5	D_0 of **13**	
15	23	552	$\{-1, \pm\frac{1}{5}\}$	5*	$Co.3$	SPL, Q
16	23	2048	$\{-\frac{9}{23}, -\frac{1}{23}, \frac{7}{23}\}$	3	Golay	Q
17	22	1782	$\{-1, \pm\frac{1}{8}, \pm\frac{1}{4}, \pm\frac{1}{2}\}$	5	**3**∪−**3**	SPL, Q
18	22	550	$\{-1, \pm\frac{1}{4}, \pm\frac{1}{6}\}$	5	**10**∪−**10**	SPL, Q, →SRG of **10**
19	22	100	$\{-\frac{4}{11}, \frac{1}{11}\}$	3	HS	SRG(100,22,0,6)
20	16	512	$\{-1, 0, \pm\frac{1}{3}\}$	5	O_{16}	SPL, Q →SRG(256,120,56,56)
21	8	240	$\{-1, 0, \pm\frac{1}{2}\}$	7*	E_8	SPL, Q, →SRG(120,56,28,24)
22	7	56	$\{-1, \pm\frac{1}{3}\}$	5*	$D_{1/2}$ of **21**	SPL, Q, ⊃SRG(28,12,6,4)
23	6	27	$\{-\frac{1}{2}, \frac{1}{4}\}$	4*	$D_{1/3}$ of **22**	SRG(27,10,1,5)
24	5	16	$\{-\frac{3}{5}, \frac{1}{5}\}$	3	$D_{1/4}$ of **23**	SRG(16,5,0,2)
25	4	10	$\{-\frac{2}{3}, \frac{1}{6}\}$	2	$D_{1/5}$ of **24**	SRG(10,3,0,1)
26	7	126	$\{-1, 0, \pm\frac{1}{2}\}$	5	D_0 of **21**	E_7 =SPL, Q →SRG(63,30,13,15)
27	6	32	$\{-1, \pm\frac{1}{3}\}$	3	$D_{1/2}$ of **26**	Q
28	6	72	$\{-1, 0, \pm\frac{1}{2}\}$	5	E_6	SPL, Q →SRG(36,15,6,6)
29	4	24	$\{-1, 0, \pm\frac{1}{2}\}$	5	D_4	SPL, Q, → $3K_4$
30	12	756	A_{24}	7	K_{12}	SPL

54.3 Bounds and Tight Designs

54.16 Theorem Suppose that a spherical design X has angle set A of size s and let $|X|\prod_{\alpha\in A}(x-\alpha)/(1-\alpha) = \sum_{i=0}^{s} a_i Q_i(x)$. If $a_i \geq 0$ for $0 \leq i \leq s$, then $a_i \leq 1$

for $0 \le i \le s$. Assume $a_i > 0$ for $0 \le i \le s$. Then X is an $(s+i)$-design if and only if $a_0 = a_1 = \cdots = a_i = 1$.

54.17 Remark In Theorem 54.16, each a_i is proportional to $|X|$. Thus, the inequality $a_i \le 1$ gives an upper bound on $|X|$, a *special bound*. The name comes from the fact that the bound depends on the set A. On the other hand, Theorem 54.19 gives a bound that depends only on $|A|$, the *absolute bound*.

54.18 Let $R_e(x) = \sum_{i=0}^{e} Q_i(x)$, and $C_e(x) = \sum_{i=0}^{\lfloor k/2 \rfloor} Q_{e-2i}(x)$.

54.19 Theorem Every spherical $2e$-design X satisfies $|X| \le R_e(1)$. Every spherical $(2e+1)$-design X satisfies $|X| \le 2C_e(1)$.

54.20 A spherical $2e$-design X is *tight* if any of the (equivalent) following holds:
(1) $|X| = R_e(1)$, or (2) $t = 2s$. The elements of A are then the roots of $R_e(x)$.
A spherical $(2e+1)$-design X is *tight* if any of the (equivalent) following holds:
(1) $|X| = 2C_e(1)$, or (2) $t = 2s-1$. The elements of A are the roots of $(x+1)C_e(x)$.

54.21 Theorem Every tight 4-design in Ω_d is a derived design of a tight 5-design. The converse also holds.

54.22 Examples A regular $(t+1)$-gon in Ω_2 is a tight t-design. A regular pentagon is a tight 4-design in Ω_2 that is a derived design of the icosahedron, a tight 5-design in Ω_3. All other known tight designs are given in Table 54.15 with an asterisk (*). Other tight t-designs could possibly exist only for $t = 4, 5$ or 7. The dimensions are $d = (2e+1)^2 - 3$ for $t = 4$, $d = (2e+1)^2 - 2$ for $t = 5$, and $d = 3e^2 - 4$ for $t = 7$, where e is a positive integer. Some of them were ruled out in [157].

54.4 Regularity and Association Schemes

54.23 A spherical design X is *regular* if each *subdegree* $d_\alpha(x) = |\{y \in X : \langle x, y\rangle = \alpha\}|$ is a constant, d_α.

54.24 A spherical design X *carries an association scheme* if the set of relations $R_\alpha = \{(x, y) \in X \times X : \langle x, y\rangle = \alpha\}$ $(\alpha \in A \cup \{1\})$ defines an association scheme (§VI.1).

54.25 Theorems If $t \ge s-1$, then X is regular. If $t \ge 2s-2$, then X carries a Q-polynomial association scheme.

54.26 Examples Every tight design carries a Q-polynomial association scheme. In Table 54.15, "Q" indicates that the design carries a Q-polynomial association scheme. If $s = 2$, then the association scheme can be regarded as a strongly regular graph, and in this case, the parameters are given, writing SRG(v,k,λ,μ) in the "Comments" column. If $-1 \in A$ and $s = 4$ or 5, then the quotient scheme has class 2, hence it is also a strongly regular graph. In this case, the parameters are given, writing $\rightarrow$SRG(v,k,λ,μ) or $\rightarrow mK_k$, the latter meaning the disjoint union of m copies of the complete graph on k vertices.

54.5 Existence of Spherical Designs

54.27 Theorem Spherical t-designs exist for all t and d.

54.28 Remark The proof of Theorem 54.27 in [1885] is nonconstructive, but [1325] gives a construction with $C(d)t^{d^2/2+d/2}$ points.

54.29 Theorem A spherical 2-design on n points on Ω_d exists unless both n and d are odd or $n \le d$.

54.30 Theorem Spherical 3-designs on Ω_d with v points exists if and only if $v \geq 2d$ except v odd and $v < 5d/2$, or $(d, v) = (3, 9)$ or $(5, 13)$.

54.31 Theorem A spherical 4-design on Ω_3 with v points exists if and only if $v = 12, 14$ or $v \geq 16$. A spherical 5-design on Ω_3 with v points exists if $v = 12, 16, 18, 20$ or $v \geq 22$.

54.32 Examples For existence of spherical t-designs of given size in Ω_3 and Ω_4, see `http://www.research.att.com/~njas/sphdesigns/`.

54.6 Designs in Projective Spaces

54.33 Let $\mathbb{F}$ denote the real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, quaternions $\mathbb{H}$, or octonions (Cayley numbers) $\mathbb{O}$. The *projective space* $\mathbb{F}\mathbf{P}^{d-1}$, or just $\mathbf{P}$, is the set of idempotents x of trace 1 in the $\mathbb{R}$-linear space of d by d hermitean matrices over $\mathbb{F}$ ($d = 2, 3$ if $\mathbb{F} = \mathbb{O}$), with inner product $\langle x, y\rangle =$ real part of trace(xy).

54.34 Let $m = \frac{1}{2}, 1, 2$, or 4 according as $\mathbb{F} = \mathbb{R}, \mathbb{C}, \mathbb{H}$, or $\mathbb{O}$; let $N = md$. The *special polynomials* $Q_k(x)$ of degree $k = 0, 1, 2, \ldots$ associated with $\mathbf{P}$ are given by

$$Q_k(x) = \textstyle\sum_{r=0}^{k} (-1)^{k-r} \binom{k}{r} (N + 2k - 1)\{(N)_{k+r-1}/(m)_r k!\} x^r.$$

A *t-design* in $\mathbf{P}$ is a finite nonempty subset X satisfying

$$\textstyle\sum_{x,y \in X} Q_k(\langle x, y\rangle) = 0, \ \forall k = 1, 2, \ldots, t.$$

54.35 Remark The angle set of a t-design X in $\mathbf{P}$ is defined in the same manner as in Definition 54.6. Analogues of Theorem 54.7, Theorem 54.19, Theorem 54.25, Theorem 54.27 also hold for designs in projective spaces. See [1121] for details.

54.36 Examples

1. A subset $X \subset \Omega_d$ is antipodal if $x \in X$ implies $-x \in X$. A t-design in $\mathbb{R}\mathbf{P}^{d-1}$ of size v with $A = \{\alpha^2, \beta^2, \ldots\}$ is equivalent to an antipodal spherical $(2t+1)$-design of size $2v$ with $A = \{-1, \pm\alpha, \pm\beta, \ldots\}$ in Ω_d.
2. A 2-design in $\mathbb{C}\mathbf{P}^{d-1}$ with $A = \{0, \frac{1}{d}\}$ is equivalent to $d + 1$ mutually unbiased bases [1309]. Such bases exist when d is a prime power, and the existence is an open problem when d is not a prime power.

54.37 Table Some t-designs in projective spaces. In this table, $A_1 = \{0, \frac{1}{4}, \frac{1}{2}, (3 \pm \sqrt{5})/8\}$, "refl.gp" means either complex or quaternionic reflection groups, "GH(2,8)" means a generalized hexagon of order $(2, 8)$. If $|A| = 2$ and $t \geq 2$, then there is a strongly regular graph associated to the design. Such a graph is either described by its parameters SRG(k,λ,μ), or by its structure as a disjoint union of complete graphs.

$\mathbb{F}$	d	v	A	t	Description	Comments
	3	9	$\{\frac{1}{4}\}$	2	$\mathbb{C}$-form of **23**	
	3	21	$\{0, \frac{1}{4}, \frac{1}{2}\}$	3	refl.gp. No.24	
	3	45	A_1	2	refl.gp. No.27	
	4	40	$\{0, \frac{1}{3}\}$	3	refl.gp. No.32	SRG(12,4,2)
$\mathbb{C}$	4	60	$\{0, \frac{1}{4}, \frac{1}{2}\}$	3	refl.gp. No.31	
	5	45	$\{0, \frac{1}{4}\}$	2	refl.gp. No.33	SRG(12,3,3)
	6	126	$\{0, \frac{1}{4}\}$	3	refl.gp. No.34	SRG(45,18,12)
	8	64	$\{\frac{1}{9}\}$	2	$\mathbb{H}$-refl.gp. $W(\mathbf{S}_1)$	
	12	32760	$\{0, \frac{1}{3}, \frac{1}{4}, \frac{1}{12}\}$	5	Leech	
	28	4060	$\{0, \frac{1}{16}\}$	2	Rudvalis	SRG(1755,780,730)

$\mathbb{F}$	d	v	A	t	Description	Comments
	2	10	$\{0, \frac{1}{2}\}$	3	[1121]	$5K_2$
	3	63	$\{0, \frac{1}{4}, \frac{1}{2}\}$	3	refl.gp. $W(Q)$	
	3	316	A_1	5	refl.gp. $W(R)$	
$\mathbb{H}$	4	36	$\{0, \frac{1}{4}\}$	2	refl.gp. $W(\mathbf{S}_1)$	$9K_4$
	4	64	$\{\frac{1}{9}, \frac{1}{3}\}$	2	refl.gp. $W(\mathbf{S}_1)$	
	4	180	$\{0, \frac{1}{4}, \frac{1}{2}\}$	3	refl.gp. $W(\mathbf{S}_3)$	
	5	165	$\{0, \frac{1}{4}\}$	3	refl.gp. $W(U)$	SRG(36,9,3)
$\mathbb{O}$	2	18	$\{0, \frac{1}{2}\}$	3*	[1121]	$9K_2$
	3	819	$\{0, \frac{1}{4}, \frac{1}{2}\}$	5*	GH(2,8)	

See Also

§VI.1	Association schemes.
§VII.11	Strongly regular graphs.
[603, 1527]	Information about lattices yielding spherical designs.
[633]	Cubature, orbits, harmonics, polytopes, root systems.
[677]	The foundational paper for spherical designs.
[789]	Codes on spheres.
[1121]	Spherical designs in projective spaces.
[912, 1438]	General formulation in terms of polynomial metric spaces.

References Cited: [157, 603, 633, 677, 789, 912, 1121, 1309, 1325, 1438, 1527, 1885]

55 Starters

Jeffrey H. Dinitz

55.1 Definitions and Examples

55.1 A *starter* in the odd order abelian group G (written additively), where $|G| = g$ is a set of unordered pairs $S = \{\{s_i, t_i\} : 1 \le i \le (g-1)/2\}$ that satisfies:

1. $\{s_i : 1 \le i \le (g-1)/2\} \cup \{t_i : 1 \le i \le (g-1)/2\} = G \backslash \{0\}$, and
2. $\{\pm(s_i - t_i) : 1 \le i \le (g-1)/2\} = G \backslash \{0\}$.

55.2 A *strong starter* is a starter $S = \{\{s_i, t_i\}\}$ in the abelian group G with the additional property that $s_i + t_i = s_j + t_j$ implies $i = j$, and for any i, $s_i + t_i \neq 0$.

55.3 A *skew starter* is a starter $S = \{\{s_i, t_i\}\}$ in the abelian group G with the additional property that $s_i + t_i = \pm(s_j + t_j)$ implies $i = j$, and for any i, $s_i + t_i \neq 0$.

55.4 Remarks

1. These definitions extend to nonabelian groups.
2. A skew starter is a strong starter.
3. Much of the material of this chapter is covered in the survey paper [725].

55.5 Example A strong starter in $\mathbb{Z}_{17}$.

$$\{9, 10\}, \{3, 5\}, \{13, 16\}, \{11, 15\}, \{1, 6\}, \{2, 8\}, \{7, 14\}, \{4, 12\}$$

55.6 Let $S = \{\{s_i, t_i\} : 1 \le i \le (g-1)/2\}$ and $T = \{\{u_i, v_i\} : 1 \le i \le (g-1)/2\}$ be two starters in G. Without loss of generality, assume that $s_i - t_i = u_i - v_i$, for all i. Then S and T are *orthogonal* starters if $u_i - s_i = u_j - s_j$ implies $i = j$, and if $u_i \neq s_i$ for all i.

55.7 Construction In any abelian group G of odd order, the set of pairs $P = \{\{x, -x\} : x \in G\}$ is a starter, the *patterned* starter. See Example VII.5.46.

55.8 Example Two orthogonal starters in $\mathbb{Z}_7$ (P is the patterned starter).

$$S = \{\{2,3\},\{4,6\},\{1,5\}\}, \qquad P = \{\{3,4\},\{6,1\},\{5,2\}\}$$

55.9 An *adder* for the starter $S = \{\{s_i, t_i\} : 1 \le i \le (g-1)/2\}$ is an ordered set $A_S = \{a_1, a_2, \ldots, a_{(g-1)/2}\}$ of $(g-1)/2$ distinct nonzero elements from G such that the set $T = \{\{s_i + a_i, t_i + a_i\} : 1 \le i \le (g-1)/2\}$ is also a starter in the group G.

55.10 Remarks The starters S and T (in the definition) are orthogonal starters. Conversely, given any two orthogonal starters, S and T, the adder A_S is found as the "differences" between the pairs in the two starters. In Example 55.8 the adder is $A_S = \{1, 2, 4\}$.

55.2 The Connection Between Starters and Other Designs

55.11 Theorem Let G be a finite group of order $2n-1$. A starter in G implies the existence of a 1-factorization of K_{2n} with an automorphism group containing G. When $G = \mathbb{Z}_{2n-1}$, the resulting 1-factorization is 1-rotational. Construction VII.5.45 shows how to construct a 1-factorization from a starter.

55.12 Theorem The existence of d pairwise orthogonal starters in an abelian group of order n implies the existence of a Room d-cube of side n. (See §VI.50.)

55.13 Construction Let $S = \{\{s_i, t_i\} : 1 \le i \le (n-1)/2\}$ and $T = \{\{u_i, v_i\} : 1 \le i \le (n-1)/2\}$ be two orthogonal starters in G (usually $\mathbb{Z}_n$), (n odd) with $A_S = \{a_i : 1 \le i \le (n-1)/2\}$ the associated adder. Let R be an $n \times n$ array indexed by the elements of G. Each $\{s_i, t_i\} \in S$ is placed in the first row in cell $R(0, -a_i)$. This is now cycled so that the pair $\{s_i + x, t_i + x\}$ is in the cell $R(x, -a_i + x)$, where all arithmetic is performed in G. Finally, for each $x \in G$, place the pair $\{\infty, x\}$ in cell $R(x, x)$. Then R is a Room square of side n.

55.14 Example The Room square of side 7 in Example VI.50.5 was constructed from the orthogonal starters given in Example 55.8 using Construction 55.13.

55.15 Remark If $S = \{\{s_i, t_i\} : 1 \le i \le (g-1)/2\}$ is a starter, then $-S = \{\{-s_i, -t_i\} : 1 \le i \le (g-1)/2\}$ is also a starter.

55.16 Theorem If there exists a strong starter S in an abelian group of odd order n, then the starters S, $-S$, and P are pairwise orthogonal.

55.17 Theorem If there exists a starter in an abelian group of odd order $2n+1$, then there exists an odd balanced tournament design OBTD(n) (see §VI.3 and §VI.51.3).

55.18 Remark The connection between starters and Skolem sequences is given in Remark VI.53.20. The construction of a round robin tournament from a starter is given in Remark VI.51.9.

55.19 Remark Starters can be used to construct cyclic packings, which in turn can be used to construct optimal optical orthogonal codes. (See §VI.40.7 and §V.9 and [476].)

55.3 Constructions for Strong Starters

55.20 Let q be a prime power that can be written in the form $q = 2^k t + 1$, where $t > 1$ is odd and let ω be a primitive element in the field $\mathbb{F}_q$. Then define

1. C_0 to be the multiplicative subgroup of $\mathbb{F}_q \backslash \{0\}$ of order t,
2. $C_i = \omega^i C_0$, $0 \le i \le 2^k - 1$ to be the cosets of C_0 (*cyclotomic classes*), and
3. $\Delta = 2^{k-1}$, $H = \cup_{i=0}^{\Delta-1} C_i$ and $C_i^a = (1/(a-1))C_i$.

55.21 Theorem Let $T = \{\{x, \omega^\Delta x\} : x \in H\}$. Then T is a skew starter in the additive subgroup of $\mathbb{F}_q$. T is the *Mullin–Nemeth starter* in $\mathbb{F}_q$.

55.22 Theorem For each $a \in C_\Delta$, let $S_a = \{\{x, ax\} : x \in \cup_{i=0}^{\Delta-1} C_i^a\}$. Then for any $a \in C_\Delta$, S_a is a strong starter in the additive group of $\mathbb{F}_q$. Further, S_a and S_b are orthogonal if $a, b \in C_\Delta$ with $a \ne b$. Hence, the set $\{S_a | a \in C_\Delta\}$ is a set of t pairwise orthogonal starters of order q. The starters S_a are the *Dinitz starters* in $\mathbb{F}_q$.

55.23 Theorem Let $p > 5$ be a Fermat prime. There exists a strong starter in the additive group of $\mathbb{F}_p$.

55.24 Remark No strong starter in the additive group of $\mathbb{F}_3$, $\mathbb{F}_5$, or $\mathbb{F}_9$ exists.

55.25 Remark A very effective method for constructing strong starters uses a hill-climbing algorithm. A description of hill-climbing (for Steiner triple systems) is given in §VII.6.5. Hill-climbing for strong starters is described in [725].

55.26 Remark The following are multiplication-type constructions. These can be used to construct examples for strong starters in groups not of prime power order.

55.27 Theorem (Horton) Let G be an abelian group of order relatively prime to 6, and suppose there is a strong starter in G. Then there is a strong starter in the direct sum $G \oplus \mathbf{Z}_5$.

55.28 Theorem (Gross) Let G and H be abelian groups of odd order, where also H has order relatively prime to 3. Suppose there exist strong starters in G and in H. Then there is a strong starter in the direct sum $G \oplus H$.

55.29 Theorem (Gross and Leonard) Let G be an abelian group of odd order, and let H be a subgroup of G. Suppose there exist strong starters in H and in G/H. Suppose also that there is a permutation π of H such that $\pi + I$ and $\pi - I$ are also permutation s of H, where I is the identity permutation. Then there is a strong starter in G.

55.4 Existence and Enumeration of Starters

55.30 Table [1134, 1745] The number, DS(n), of distinct starters in $\mathbb{Z}_n$, for $n \le 33$.

n	3	5	7	9	11	13	15	17	19	21	23	25
DS(n)	1	1	3	9	25	133	631	3857	25905	188181	1515283	13376125

n	27	29	31	33
DS(n)	128102625	1317606101	14534145947	170922533545

55.31 Remark It remains a conjecture that there exists a strong starter in $\mathbb{Z}_n$ for all $n > 9$. It has been shown by computer to hold when $7 \le n \le 999$, $n \ne 9$. More generally, Horton [1134] conjectured that any abelian group of odd order has a strong starter, with the exceptions of the groups $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_9$, and $\mathbb{Z}_3 \times \mathbb{Z}_3$. The strongest general existence result for strong starters is Theorem 55.32.

55.32 Theorem Let G be an abelian group of order n where $n > 5$ and n is relatively prime to 6. Then there is a strong starter in G.

55.33 Theorem [476] There exists a skew starter in $\mathbb{Z}_n$ for all n such that $\gcd(n, 6) = 1$, n is not divisible by 5, or n is divisible by 25.

55.34 Remark Liaw [1447] gives constructions for skew starters in $\mathbb{Z}_n$ when n is divisible by 5.

55.35 Two strong starters S_1 and S_2 in an abelian group G are *equivalent* if there exists $\theta \in Aut(G)$ such that for some $f \in Aut(G)$, $\theta(\{x, y\}) = \{f(x), f(y)\} \in S_2$ for all $\{x, y\} \in S_1$.

55.36 Table The number of distinct and inequivalent strong starters in $\mathbb{Z}_n$, for $n \leq 27$ [1318].

n	3	5	7	9	11	13	15	17	19	21	23	25	27
Distinct	0	0	1	0	4	4	32	224	800	6600	27554	158680	1249650
Inequivalent	0	0	1	0	2	2	4	14	52	555	1257	7934	69425

55.37 Table [1318] The inequivalent strong starters in $\mathbb{Z}_n$, for $n \leq 19$.

$n = 7$

1.	2,3	4,6	1,5	

$n = 11$

1.	1,2	7,9	3,6	4,8	5,10
2.	2,3	5,7	6,9	8,1	10,4

$n = 13$

1.	1,2	8,10	3,6	5,9	7,12	11,4
2.	3,4	5,7	9,12	10,1	6,11	2,8

$n = 15$

1.	2,3	6,8	7,10	9,13	11,1	14,5	12,4
2.	2,3	8,10	4,7	12,1	9,14	5,11	6,13
3.	2,3	12,14	8,11	6,10	4,9	1,7	13,5
4.	3,4	7,9	11,14	2,6	8,13	10,1	5,12

$n = 17$

1.	1,2	3,5	10,13	11,15	4,9	6,12	7,14	8,16
2.	1,2	3,5	12,15	7,11	9,14	4,10	6,13	8,16
3.	1,2	4,6	8,11	12,16	10,15	3,9	7,14	5,13
4.	1,2	5,7	8,11	12,16	9,14	4,10	13,3	15,6
5.	1,2	6,8	12,15	7,11	4,9	10,16	13,3	14,5
6.	1,2	7,9	3,6	12,16	10,15	8,14	4,11	5,13
7.	1,2	8,10	4,7	11,15	9,14	16,5	6,13	12,3
8.	1,2	12,14	4,7	6,10	11,16	3,9	8,15	5,13
9.	2,3	4,6	9,12	7,11	13,1	10,16	8,15	14,5
10.	2,3	7,9	12,15	1,5	8,13	10,16	4,11	6,14
11.	2,3	11,13	9,12	6,10	16,4	1,7	8,15	14,5
12.	3,4	5,7	12,15	6,10	13,1	8,14	9,16	11,2
13.	3,4	7,9	12,15	2,6	8,13	10,16	11,1	14,5
14.	4,5	10,12	15,1	7,11	3,8	13,2	9,16	6,14

$n = 19$

1.	1,2	3,5	7,10	11,15	8,13	12,18	9,16	17,6	14,4
2.	1,2	3,5	7,10	12,16	8,13	9,15	11,18	17,6	14,4
3.	1,2	3,5	7,10	12,16	13,18	9,15	4,11	6,14	8,17
4.	1,2	3,5	9,12	13,17	6,11	10,16	8,15	18,7	14,4
5.	1,2	3,5	13,16	11,15	4,9	6,12	7,14	10,18	8,17
6.	1,2	3,5	15,18	10,14	8,13	6,12	4,11	9,17	7,16
7.	1,2	4,6	5,8	13,17	11,16	9,15	7,14	10,18	3,12
8.	1,2	4,6	14,17	5,9	11,16	7,13	8,15	10,18	3,12

9.	1,2	5,7	9,12	13,17	11,16	4,10	15,3	6,14	18,8
10.	1,2	5,7	10,13	14,18	3,8	11,17	9,16	4,12	6,15
11.	1,2	5,7	11,14	12,16	8,13	4,10	15,3	17,6	9,18
12.	1,2	6,8	7,10	14,18	12,17	9,15	4,11	16,5	13,3
13.	1,2	6,8	12,15	18,3	9,14	10,16	4,11	5,13	17,7
14.	1,2	6,8	13,16	7,11	4,9	12,18	10,17	14,3	15,5
15.	1,2	7,9	5,8	10,14	11,16	12,18	15,3	17,6	4,13
16.	1,2	7,9	12,15	13,17	6,11	18,5	3,10	8,13	14,4
17.	1,2	7,9	14,17	12,16	3,8	4,10	11,18	5,13	6,15
18.	1,2	8,10	4,7	14,18	11,16	9,15	5,12	17,6	13.3
19.	1,2	8,10	12,15	13,17	4,9	5,11	18,6	14,3	7,16
20.	1,2	8,10	14,17	11,15	4,9	7,13	18,6	16,5	3,12
21.	1,2	11,13	3,6	5,9	12,17	10,16	8,15	18,7	14,4
22.	1,2	11,13	7,10	12,16	4,9	18,5	15,3	6,14	8,17
23.	1,2	11,13	12,15	3,7	5,10	17,4	9,16	6,14	18,8
24.	1,2	11,13	15,8	3,7	4,9	10,16	15,12	6,14	8,17
25.	1,2	12,14	6,9	7,11	13,18	17,4	3,10	8,16	15,5
26.	1,2	12,14	6,9	18,3	11,16	4,10	8,15	5,13	17,7
27.	1,2	12,14	10,13	5,9	3,8	11,17	16,4	18,7	6,15
28.	1,2	14,16	6,9	11,15	8,13	18,5	3,10	4,12	17,7
29.	1,2	15,17	13,16	4,8	5,10	6,12	7,14	3,11	9,18
30.	1,2	16,18	5,8	6,10	12,17	9,15	7,14	3,11	4,13
31.	2,3	5,7	12,15	9,13	6,11	14,1	16,4	10,18	8,17
32.	2,3	5,7	15,18	6,10	8,13	11,17	9,16	12,1	14,4
33.	2,3	6,8	9,12	16,1	13,18	5,11	10,17	7,15	14,4
34.	2,3	7,9	5,8	12,16	10,15	14,1	11,18	17,6	4,13
35.	2,3	7,9	12,15	1,5	8,13	10,16	11,18	17,6	14,4
36.	2,3	8,10	14,17	12,16	4,9	5,11	13,1	18,7	6,15
37.	2,3	9,11	4,7	14,18	12,17	10,16	1,8	5,13	6,15
38.	2,3	10,12	5,8	7,11	13,18	14,1	16,4	9,17	6,15
39.	2,3	12,14	6,9	13,17	11,16	4,10	1,8	18,7	15,5
40.	3,4	5,7	15,18	10,14	8,13	11,17	2,9	12,1	16,6
41.	3,4	8,10	12,15	1,5	13,18	11,17	2,9	6,14	7,16
42.	3,4	8,10	12,15	16,1	13,18	5,11	2,9	6,14	17,7
43.	3,4	9,11	5,8	10,14	12,17	15,2	13,1	18,7	16,6
44.	3,4	10,12	15,18	1,5	8,13	11,17	2,9	6,14	7,16
45.	3,4	10,12	15,18	16,1	8,13	5,11	2,9	6,14	17,7
46.	3,4	11,13	7,10	12,16	15,1	18,5	2,9	6,14	8,17
47.	3,4	14,16	7,10	1,5	8,13	9,15	11,18	17,6	12,2
48.	4,5	8,10	11,14	9,13	17,3	15,2	18,6	12,1	7,16
49.	4,5	12,14	17,1	6,10	3,8	9,15	11,18	13,2	7,16
50.	7,8	3,5	14,17	6,10	16,2	9,15	11,18	12,1	4,13
51.	7,8	3,5	14,17	9,13	16,2	4,10	11,18	12,1	6,15
52.	8,9	1,3	11,14	13,17	2,7	10,16	18,6	4,12	15,5

55.38 Table A strong starter in $\mathbb{Z}_n$ for $21 \leq n \leq 51$.

n	Starter
21	{4,5}, {13,15}, {8,11}, {20,3}, {18,2}, {6,12}, {9,16}, {14,1}, {10,19}, {7,17}
23	{7,8}, {1,3}, {17,20}, {10,14}, {6,11}, {15,21}, {18,2}, {4,12}, {13,22}, {9,19}, {5,16}
25	{3,4}, {11,13}, {18,21}, {2,6}, {7,12}, {17,23}, {15,22}, {1,9}, {10,19}, {14,24}, {5,16}, {8,20}
27	{15,16}, {20,22}, {2,5}, {4,8}, {14,19}, {6,12}, {23,3}, {18,26}, {1,10}, {7,17}, {13,24}, {9,21}, {25,11}
29	{25,26}, {14,16}, {2,5}, {17,21}, {15,20}, {6,12}, {4,11}, {22,1}, {23,3}, {9,19}, {7,18}, {27,10}, {24,8}, {28,13}

n	Starter
31	{17,18}, {24,26}, {11,14}, {2,6}, {5,10}, {21,27}, {28,4}, {22,30}, {7,16}, {13,23}, {29,9}, {8,20}, {12,25}, {1,15}, {19,3}
33	{20,21}, {27,29}, {4,7}, {32,3}, {6,11}, {10,16}, {24,31}, {5,13}, {17,26}, {9,19}, {14,25}, {18,30}, {22,2}, {1,15}, {8,23}, {12,28}
35	{23,24}, {9,11}, {4,7}, {16,20}, {27,32}, {22,28}, {1,8}, {13,21}, {5,14}, {19,29}, {26,2}, {3,15}, {18,31}, {33,12}, {30,10}, {25,6}, {17,34}
37	{1,2}, {24,26}, {14,17}, {16,20}, {6,11}, {30,36}, {21,28}, {25,33}, {3,12}, {5,15}, {18,29}, {34,9}, {19,32}, {8,22}, {35,13}, {31,10}, {27,7}, {23,4}
39	{9,10}, {27,29}, {4,7}, {36,1}, {20,25}, {17,23}, {35,3}, {33,2}, {12,21}, {6,16}, {26,37}, {18,30}, {15,28}, {38,13}, {19,34}, {8,24}, {5,22}, {14,32}, {31,11}
41	{12,13}, {14,16}, {21,24}, {4,8}, {26,31}, {11,17}, {29,36}, {1,9}, {38,6}, {18,28}, {32,2}, {22,34}, {33,5}, {30,3}, {20,35}, {23,39}, {10,27}, {7,25}, {37,15}, {40,19}
43	{16,17}, {25,27}, {29,32}, {10,14}, {4,9}, {39,2}, {15,22}, {28,36}, {42,8}, {40,7}, {20,31}, {23,35}, {13,26}, {41,12}, {34,6}, {3,19}, {21,38}, {30,5}, {18,37}, {24,1}, {33,11}
45	{31,32}, {41,43}, {39,42}, {18,22}, {4,9}, {30,36}, {13,20}, {6,14}, {8,17}, {38,3}, {33,44}, {25,37}, {11,24}, {15,29}, {19,34}, {5,21}, {40,12}, {10,28}, {16,35}, {7,27}, {26,2}, {1,23}
47	{25,26}, {27,29}, {40,43}, {14,18}, {8,13}, {45,4}, {37,44}, {20,28}, {23,32}, {2,12}, {6,17}, {30,42}, {22,35}, {1,15}, {31,46}, {3,19}, {41,11}, {21,39}, {5,24}, {34,7}, {36,10}, {16,38}, {33,9}
49	{13,14}, {16,18}, {4,7}, {30,34}, {21,26}, {40,46}, {32,39}, {35,43}, {29,38}, {23,33}, {48,10}, {8,20}, {2,15}, {17,31}, {37,3}, {45,12}, {24,41}, {42,11}, {6,25}, {27,47}, {1,22}, {36,9}, {5,28}, {44,19}
51	{42,43}, {30,32}, {2,5}, {3,7}, {44,49}, {23,29}, {41,48}, {6,14}, {15,24}, {8,18}, {16,27}, {40,1}, {25,38}, {36,50}, {11,26}, {19,35}, {4,21}, {28,46}, {20,39}, {13,33}, {47,17}, {9,31}, {22,45}, {10,34}, {12,37}

55.39 Example [1134] A strong starter in $\mathbb{Z}_3 \times \mathbb{Z}_9$ ((a,b) denoted ab). {18,04}, {05,03}, {15,27}, {28,17}, {07,21}, {12,22}, {10,06}, {01,23}, {08,02}, {14,13}, {11,26}, {20,24}, {16,25}.

55.40 Remark There are few general nonexistence results on starters. Probably the most interesting is Theorem 55.41, due to Mullin and Wallis.

55.41 Theorem Suppose G is an abelian group of order $n \equiv 3 \pmod 6$ in which the 3-Sylow subgroup is cyclic. Then there is no skew starter in G. In particular, there does not exist a skew starter in $\mathbb{Z}_n$ if $n \equiv 0 \pmod 3$.

55.5 Other Types of Starters

55.42 Let G be an abelian group of order $2n$ written *multiplicatively* with identity element e and a unique element g^* of order 2. An *even starter* in G is a set of $n-1$ unordered pairs $E = \{\{x_i, y_i\} : 1 \le i \le n-1\}$ which satisfies:

1. $\{x_i : 1 \le i \le n-1\} \cup \{y_i : 1 \le i \le n-1\}$ are all the nonidentity elements of G except one, denoted m_E, and
2. $\{x_i^{-1}y_i, y_i^{-1}x_i : 1 \le i \le n-1\} = G \setminus \{e, g^*\}$.

Even starters can be defined analogously in abelian groups written additively.

55.43 Example An even starter in $\mathbb{F}_{11}^*$: {{6,10}, {3,9}, {4,8}, {5,7}}. Note that $m_E = 2$ and $g^* = -1$.

55.44 Remark Construction VII.5.47 shows how an even starter in a group of order $2n$ induces a 1-factorization of K_{2n+2}. Construction VII.5.64 gives two infinite classes

of even starters that induce nonisomorphic (perfect) 1-factorizations of K_{p+1} for all primes $p \geq 11$.

55.45 Table [1745] The number, ES($2n$), of distinct even starters in $\mathbb{Z}_{2n}$, for $n \leq 16$.

$2n$	4	6	8	10	12	14	16	18	20	22	24
ES($2n$)	2	4	12	56	224	960	5760	42816	320512	2366080	20857088

$2n$	26	28	30	32
ES($2n$)	216731392	2229359616	23000005632	270569758720

55.46 Let G be an additive abelian group of order g, and let H be a subgroup of order h of G, where $g - h$ is even. A *frame starter* in $G\backslash H$ is a set of unordered pairs $S = \{\{s_i, t_i\} : 1 \leq i \leq (g-h)/2\}$ such that

1. $\{s_i : 1 \leq i \leq (g-h)/2\} \cup \{t_i : 1 \leq i \leq (g-h)/2\} = G\backslash H$, and
2. $\{\pm(s_i - t_i) : 1 \leq i \leq (g-h)/2\} = G\backslash H$

55.47 Remark A starter is the special case of a frame starter when $H = \{0\}$. The concepts of strong, skew, and orthogonal for frame starters are as for starters (§55.1), replacing $\{0\}$ by H and $(g-1)/2$ by $(g-h)/2$.

55.48 Example A skew frame starter in $\mathbb{Z}_{10}\backslash\{0,5\}$: $S = \{\{3,4\},\{7,9\},\{1,8\},\{2,6\}\}$.

55.49 Theorem Suppose a pair of orthogonal frame starters in $G\backslash H$ exist, where $|G| = g$ and $|H| = h$. Then there exists a Room frame of type $h^{g/h}$ (see §VI.50.6).

55.50 Remark The construction for a Room frame from a pair of orthogonal frame starters is a generalization of Construction 55.13.

55.51 Theorem Let $q \equiv 1 \pmod 4$ be a prime power such that $q = 2^k t + 1$, where $t > 1$ is odd. Then there exist t orthogonal frame starters in $(\mathbb{F}_q \times (\mathbb{Z}_2)^n)\backslash(\{0\} \times (\mathbb{Z}_2)^n)$ for all $n \geq 1$.

55.52 Remark It is sometimes useful to consider the pairs of elements in a starter as *ordered pairs*. When certain additional conditions are satisfied these are *balanced starters* or *symmetric skew balanced starters*. These starters are useful in constructing balanced Room squares and Howell movements for bridge tournaments. See [725, §10] for a description of the construction of these starters. See §VI.51.10 for more on the existence of balanced Room squares and the connection to Howell movements.

55.53 Remark Howell starters are discussed in §VI.29.2.

See Also

§VI.3	The connection to tournament designs is given in Theorem 55.17.
§VI.50	Starters are used to construct Room squares.
§VI.51	Starters are particularly useful in the construction of round robin tournaments.
§VI.53	Starters are related to Skolem sequences.
§VI.64	Starters are related to $\mathbb{Z}$-cyclic Whist tournaments.
§VII.5.5	The existence of a starter in the cyclic group implies the existence of a 1-rotational 1-factorization of the complete graph.
[725]	A comprehensive survey on Room squares including starters; contains much of the information given in this chapter. References not given in this chapter can be found in this survey.
[2110]	A textbook dealing with Room squares and starters.
[476, 1491]	Constructs optimal optical orthogonal codes from starters.

References Cited: [476, 725, 1134, 1318, 1447, 1491, 1745, 2110]

56 Superimposed Codes and Combinatorial Group Testing

Charles J. Colbourn
Frank K. Hwang

56.1 Definitions and Examples

56.1 Let $x = [x_0 x_1 \dots x_{n-1}]^T$ and $y = [y_0 y_1 \dots y_{n-1}]^T$ be two binary n-dimensional vectors. The bit-by-bit boolean sum is the *superposition sum*, denoted by $x \vee y = [x_0 \vee y_0 \quad x_1 \vee y_1 \dots x_{n-1} \vee y_{n-1}]^T$. A vector x is *contained* in y, if $x \vee y = y$.

56.2 A $v \times b$ binary matrix M with columns indexed by $\{1, \dots, b\}$ is a
- d-***disjunct matrix*** if the superposition sum of any d columns of M does not contain any other column of M;
- d-***separable matrix*** if for every $D_1, D_2 \subseteq \{1, \dots, b\}$ with $|D_1| = |D_2| = d$, the superposition sum of the columns indexed by D_1 and the superposition sum of the columns indexed by D_2 are equal only if $D_1 = D_2$;
- $\overline{d}$-***separable matrix*** if for every $D_1, D_2 \subseteq \{1, \dots, b\}$ with $|D_1| \leq d$ and $|D_2| \leq d$, the superposition sum of the columns indexed by D_1 and the superposition sum of the columns indexed by D_2 are equal only if $D_1 = D_2$.

56.3 A family of v subsets $C_1, \dots, C_v$ of a b-set X is *d-disjunct* if for every $D \subset X$ with $|D| \leq d$, every $x \in X \setminus D$, at least one of the $\{C_i\}$ contains x but contains no member of D.

56.4 A family of b subsets $B_1, \dots, B_b$ of a v-set V is
- d-***cover-free*** if for every $D \subseteq \{1, \dots, b\}$ with $|D| = d$ and $i \notin D$, $B_i \not\subset \bigcup_{j \in D} B_j$;
- d-***weakly union-free*** if for every $D_1, D_2 \subseteq \{1, \dots, m\}$ with $|D_1| = |D_2| = d$, $\bigcup_{j \in D_1} B_j = \bigcup_{j \in D_2} B_j$ implies $D_1 = D_2$;
- d-***(strongly) union-free*** if for every $D_1, D_2 \subseteq \{1, \dots, m\}$ with $|D_1| \leq d$ and $|D_2| \leq d$, $\bigcup_{j \in D_1} B_j = \bigcup_{j \in D_2} B_j$ implies $D_1 = D_2$.

56.5 A *d-superimposed code* of *size* b and *length* v is a collection of b binary vectors (*codewords*) of length v, with the property that the superposition sum of a set D of d or fewer codewords uniquely determines D.

56.6 Examples A 9×12 matrix that is 2-disjunct, a 2-superimposed code with length 9, and a 2-cover-free family on 9 points (also an STS(9)).

```
100100100100
100010010010
100001001001
010100001010
010010100001
010001010100
001100010001
001010001100
001001100010
```

```
[111000000] [000111000]
[000000111] [100100100]
[010010010] [001001001]
[100010001] [010001100]
[001100010] [100001010]
[010100001] [001010100]
```

{1,2,3}, {4,5,6}, {7,8,9},
{1,4,7}, {2,5,8}, {3,6,9},
{1,5,9}, {2,6,7}, {3,4,8},
{1,6,8}, {2,4,9}, {3,5,7}

56.7 Theorem d-Superimposed codes of length v and size b, $\overline{d}$-separable $v \times b$ matrices, and

d-(strongly)-union-free families of b subsets of a ground set of size v are all equivalent.

56.8 Theorem Every d-disjunct matrix is $\overline{d}$-separable. Every $\overline{(d+1)}$-separable matrix is d-disjunct.

56.9 Remark In applications to digital communications with d-superimposed codes [2162], d contemporaneous communications can be successfully decoded given the *a priori* guarantee that no more than d codewords are transmitted concurrently. Determining *which* selection of at most d codewords is in general not easy; however, when the superimposed code corresponds to a d-cover-free family, the codewords transmitted are precisely those codewords contained in the superposition sum, and hence decoding is easy.

56.10 Theorems

1. The removal of any row from a d-disjunct matrix yields a d-separable matrix.
2. [471] By adding at most one row, a $2d$-separable matrix becomes a d-disjunct matrix.

56.11 Theorem A $v \times b$ matrix with $d < b$ is d-separable if and only if it is k-separable for every $1 \le k \le d$. (Hence, an analogous definition for $\overline{d}$-separable matrices would correspond to d-separable matrices.)

56.2 Bounds

56.12 $t(d, b)$ is the minimum number of rows in a d-disjunct matrix with b columns.

56.13 Theorem $t(d, b) \ge \min(b, \binom{d+1}{2})$. Indeed, for $\binom{d+2}{2} \ge b$, $t(d, b) = b$.

56.14 Theorem [765, 766] For d fixed and $b \to \infty$, $K_d(1 + \mathrm{o}(1)) \log b \le t(d, b) \le \frac{d}{A_d}(1 + \mathrm{o}(1)) \log b$. As $d \to \infty$, $K_d = \frac{d^2}{\log d}(1 + \mathrm{o}(1))$ and $A_d = \frac{1}{d \log e}(1 + \mathrm{o}(1))$.

56.3 Constant Weight Superimposed Codes

56.15 A superimposed code has *constant weight* w if every codeword contains exactly w ones. Equivalently, the corresponding set system is *w-uniform*.

56.16 Theorem Uniform packings yield superimposed codes: A t-$(v, k, 1)$ packing with b blocks yields a $\lfloor \frac{k-1}{t-1} \rfloor$-superimposed code of size b and length v. In particular,

1. An $OA_1(t, k, v)$ produces a $\lfloor \frac{k-1}{t-1} \rfloor$-superimposed code of length k having v^t codewords.
2. A Steiner system $S(t, k, v)$ produces an $\lfloor \frac{k-1}{t-1} \rfloor$-superimposed code of length v having $\binom{v}{t}/\binom{k}{t}$ codewords.

56.17 Theorem (Erdős, Frankl, and Füredi, see [758]) For a d-superimposed code of constant weight k, with v rows, the largest number b of columns satisfies $b \ge \frac{\binom{v}{t}}{\binom{k}{t}^2}$. Indeed, suppose that d, k, and t satisfy $k = d(t-1) + 1 + x$ with $0 \le x < d$. Then for v sufficiently large, $(1 - \mathrm{o}(1)) \frac{\binom{v-x}{t}}{\binom{k-x}{t}} \le b \le \frac{\binom{v-x}{t}}{\binom{k-x}{t}}$ whenever $x \in \{0, 1\}$ or $x < \frac{d}{2t^2}$, or $t = 2$ and $x < \lceil \frac{2d}{3} \rceil$. When a Steiner system $S(t, k-x, v-x)$ exists, the upper bound is exact.

56.18 Remark Requiring all weights to be "small" can arise in testing problems in which an item (column) can be tested in only a small number of tests (rows).

56.19 Theorem [2083] The maximum number of columns in a 2-separable matrix with v rows, no two columns of which agree in two positions both containing a "1", is $\lfloor \frac{v(v+1)}{6} \rfloor$. An optimal solution in which every column has weight at most three can be produced using 3-GDDs.

56.4 Nonadaptive Group Testing

56.20 Remarks A population $\mathcal{P}$ of b items contains a number d of *defective* items, and the remaining $b-d$ items are *good*. Items can be pooled together for testing: for a subset $X \subseteq \mathcal{P}$, the *group test* reports "yes" if X contains one or more defective elements, and reports "no" otherwise. The objective is to determine, using a number of group tests performed in parallel, precisely which items are defective.

56.21 Theorem Let $\mathcal{P}$ be a set of b items, and let $\mathbf{X}$ be a collection of subsets of $\mathcal{P}$ corresponding to the group tests performed. Then $(\mathcal{P}, \mathbf{X})$ is a solution to the nonadaptive group testing problem if and only if, for any possible sets D_1 and D_2 of defective items, $\{X : D_1 \cap X \neq \emptyset,\ X \in \mathbf{X}\} = \{X : D_2 \cap X \neq \emptyset,\ X \in \mathbf{X}\}$ only if $D_1 = D_2$.

56.22 Remarks Often one knows with high probability that the number of defectives η does not exceed some threshold value d. Consider the dual $(V, \mathcal{B})$ of $(\mathcal{P}, \mathbf{X})$. In the *hypergeometric* problem, the number of defectives never exceeds d; then $(V, \mathcal{B})$ has the unions of any two distinct sets, each containing at most d blocks, themselves distinct. Then the dual $(V, \mathcal{B})$ of $(\mathcal{P}, \mathbf{X})$ is a d-union-free family. In the *strict* problem, one is required to correctly identify the set of defective items when $\eta \leq d$ and is also required to report when $\eta > d$. In the latter case, the specific set of defective items need not be determined, however.

In the *error detection/correction* version of the problem, some group tests are permitted to report "false positives"; an *a priori* bound q on the number of such false positives is assumed.

56.23 Theorem [147, 764] $(V, \mathcal{B})$ is a solution to the strict group testing problem with threshold p and error detection (correction) for q false positives if and only if, for every union of p or fewer blocks, every other block contains at least $q+1$ ($2q+1$, respectively) points not in this union. Hence, any packing $(V, \mathcal{B})$ of t-sets into k-sets having $k \geq p(t-1)+q+1$ ($k \geq p(t-1)+2q+1$, respectively) is a solution to the strict group testing problem with threshold p and error detection (correction, respectively) for q false positives.

56.5 Topology Transparent Networks

56.24 Remarks Access to a shared communications channel can be managed using a *scheduled* scheme in which time is divided into *frames*, each consisting of a fixed number v of *slots*. Then b nodes are each assigned a *frame schedule* which is a binary vector of length v; a "1" in the ith position indicates that the node is permitted to transmit in the ith slot. A receiver node successfully receives a transmission when there is precisely one transmitting node within radio range (a distance known in advance) of the receiver; when two transmissions arrive in the same slot, a *collision* occurs and no data can be recovered. See [583].

56.25 A set of b binary vectors of length v is a *topology-transparent schedule* supporting d active neighbors if for every node x and every set D of d nodes not containing x, the schedule for node x contains a "1" in a slot for which no other node in D also contains a "1".

56.26 Remarks Stated informally, there is a slot in which x can transmit and $y \in D$ can receive, without collision, even if node y has d neighbors that are active in transmission during this frame. Orthogonal arrays were first proposed as a means to construct topology-transparent schedules [495, 1218].

56.27 Theorem [564] A d-cover-free family of size b on a ground set of size v is equivalent to a topology-transparent schedule supporting d active neighbors.

56.28 Theorem [508] Frame synchonization in topology-transparent scheduling can be replaced by (the weaker) slot synchonization by using *cyclic* d-superimposed codes and assigning each node a cyclic orbit of codewords.

56.6 Frameproof Codes

56.29 Remarks In order to identify copies of a software package that are legally distributed, vendors can *fingerprint* the executable image by placing marks in a subset of v locations that do not impact execution. Users can then compare their versions to determine the location of some or all of the marks and then change them. In the process, the users may collude to select an invalid fingerprint; but they may also succeed in producing a valid fingerprint that is not assigned to any of the colluding users (see Boneh and Shaw [294]).

56.30 Given a set D of d binary vectors of length v, the *feasible set* $F(D)$ contains all binary vectors in which every entry agrees with the corresponding entry of at least one vector in D. A *d-frameproof code* of length v and size b is a set of b binary vectors of length v for which, for every set D of at most d of the b vectors in the code, $C \in F(D)$ only if $C \in D$.

56.31 Remark Using a d-frameproof code, if a valid codeword is produced by altering known marks, no user not in a coalition of d users altering the marks can be implicated.

56.32 Theorem [1974] A d-frameproof code is equivalent to a d-cover-free family.

56.7 Key Distribution Patterns

56.33 A family of sets $\mathcal{B}$ is (w, d)-*cover-free* if whenever $\mathcal{B}_1, \mathcal{B}_2 \subset \mathcal{B}$, $|\mathcal{B}_1| = w$, $|\mathcal{B}_2| = d$, and $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$, it holds that $\bigcap_{B \in \mathcal{B}_1} B \not\subseteq \bigcup_{B \in \mathcal{B}_2} B$. A d-cover-free family is $(1, d)$-cover-free. (See [767, 1979].)

56.34 Remark Suppose that among n network users $P_1, P_2, \ldots, P_n$, every w-set is to communicate in a secure way (usually $w = 2$). A conventional (symmetric or private key) cryptosystem is being used. A trusted authority can generate and distribute a secret key for each w-set of users, but this involves $\binom{n}{w}$ keys and requires each user to store $\binom{n-1}{w-1}$ keys. The number of keys to be stored can be considerably reduced under weaker security conditions. See [1617].

56.35 A *key distribution pattern* (KDP) with parameters (n, v, m) is a pair $(X, \mathcal{B})$, where X is a set of v keys, say, $\{K_1, K_2, \ldots, K_v\}$, and $\mathcal{B}$ is a set of n m-subsets of X, say, $\{B_1, B_2, \ldots, B_n\}$.

56.36 Remark KDPs are used as follows. User P_i is given the m keys in B_i. When w users $\{u_1, \ldots, u_w\}$ wish to communicate, they apply a special function (such as a one-way function or a resilient function) to the set of common keys held by the users, $\bigcap_{i=1}^{w} B_{u_i}$.

56.37 A KDP with $w = 2$ is *d-collusion resistant* if for every pair of users P_i, P_j and every set of d users C such that $C \cap \{P_i, P_j\} = \emptyset$, it holds that $(B_i \bigcap B_j) \setminus \left(\bigcup_{P_\ell \in C} B_\ell\right) \neq \emptyset$.

56.38 Theorem Suppose a 3-(n, k, λ_3) design exists such that $\lambda_2 > d\lambda_3$. Then, there exists a (n, b, λ_1) d-collusion resistant key distribution pattern with $w = 2$.

See Also

§II.5	Existence results on Steiner systems.
§III.7	Existence results for orthogonal arrays.
§VI.46	Pooling designs are group testing schemes for genomic applications.
[758]	A comprehensive book on the combinatorics of group testing.
[402, 1158]	Contains related results on nonadaptive group testing.
[2083]	Discusses testing with two defectives.
[583, 2162]	Applications of group testing in communications.
[1974]	A general treatment of frameproof codes and key distribution patterns.
[1972]	Chapter 10 concerns key distribution patterns.

References Cited: [147, 294, 402, 471, 495, 508, 564, 583, 758, 764, 765, 766, 767, 1158, 1218, 1617, 1972, 1974, 1979, 2083, 2162]

57 Supersimple Designs

Hans-Dietrich O. F. Gronau

57.1 Definitions and Examples

57.1 A (v, k, λ)-design $(V, \mathcal{B})$ is *supersimple* if $|B_1 \cap B_2| \leq 2$ for all blocks $B_1, B_2 \in \mathcal{B}$, $B_1 \neq B_2$. Moreover, any design (PBD, TD, GDD, or the like) is *supersimple* if any two of its blocks intersect in at most two points.

57.2 Theorem Necessary conditions for the existence of a supersimple (v, k, λ)-design are

1. $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$;
2. $v \geq \lambda(k-2) + 2$; and
3. $v \geq (k-1)^2 - (k-1)(k-2)/\lambda + 1$.

57.3 Remarks Any simple $(v, 3, \lambda)$-design and any $(v, k, 1)$-design is supersimple.

57.4 Examples

1. Any symmetric $(v, k, 2)$-design (biplane) is supersimple, for example, (7,4,2) and (11,5,2).
2. No symmetric (v, k, λ)-design, $\lambda \geq 3$, is supersimple.
3. A supersimple $(v, k, \frac{v-2}{k-2})$-design is exactly a 3-$(v, k, 1)$-design; for example, a 3-$(8, 4, 1)$-design implies a supersimple $(8, 4, 3)$-design.
4. The residual of a 3-$(v, k, 1)$-design is a supersimple $(v-1, k, \frac{v-k}{k-2})$-design; for example, a 3-$(8, 4, 1)$-design implies a supersimple $(7, 4, 2)$-design.

5. Just one $(9, 4, 3)$-design is supersimple, (No. 11 in Table II.1.24).
6. All $(10, 4, 2)$-designs are supersimple; see Table II.1.25

57.2 Existence when $k = 4$ or 5

57.5 Theorem ([475] and references therein) There exists a supersimple $(v, 4, \lambda)$-design with $2 \le \lambda \le 6$ if and only if

$\lambda = 2$, $v \equiv 1 \pmod 3$ and $v \ge 7$;
$\lambda = 3$, $v \equiv 0, 1 \pmod 4$ and $v \ge 8$;
$\lambda = 4$, $v \equiv 1 \pmod 3$ and $v \ge 10$;
$\lambda = 5$, $v \equiv 1 \pmod{12}$, $v \ge 13$ or $v \equiv 4, 16, 40 \pmod{48}$, $v \ge 16$ or possibly $v \equiv 28 \pmod{48}$, $v \ge 28$ (in the latter case, there are partial results by Chen and Wei);
$\lambda = 6$ and $v \ge 14$.

57.6 Theorem [477] There exists a supersimple cyclic $(v, 4, \lambda)$-design (with full orbits) for $7 \le v \le 41$ and all admissible λ with two exceptions $(v, \lambda) \in \{(9, 3), (13, 5)\}$.

57.7 Theorem (Chen and Wei) Suppose $k \in \{4, 5\}$ and $\lambda \in \{2, 3, 4\}$. There exists a supersimple cyclic (v, k, λ)-design (with full orbits) for each integer v having all prime factors congruent to 1 modulo $k(k-1)$.

57.8 Theorem (see [2202]) There exists a supersimple resolvable $(v, 4, 2)$-design if and only if $v \equiv 4 \pmod{12}$ and $v \ge 16$. There exists a supersimple resolvable $(v, 4, 3)$-design if and only if $v \equiv 0 \pmod 4$ and $v \ge 8$ except for $v = 12$.

57.9 Two cyclic block designs with block sets $\mathcal{B}_1, \mathcal{B}_2$ are *(multiplier-)equivalent* if there exist $w, i \in \mathbb{Z}_v$ such that for each base block $B_1 \in \mathcal{B}_1$, there is some base block $B_2 \in \mathcal{B}_2$ with $w \cdot B_1 + i = B_2$. They are *inequivalent* if they are not equivalent.

57.10 Table (Grüttmüller) The number of inequivalent supersimple cyclic $(v, 4, \lambda)$-designs with full orbits. A dash (–) indicates that the necessary conditions of Theorem 57.2 are not satisfied.

v/λ	1	2	3	4	5	6	7	8	9	10	11
7	–	2	–	–	–	–	–	–	–	–	–
9	–	–	0	–	–	–	–	–	–	–	–
10	–	–	–	1	–	–	–	–	–	–	–
13	1	2	5	6	0	–	–	–	–	–	–
15	–	–	–	–	–	2	–	–	–	–	–
16	–	–	–	94	–	–	–	–	–	–	–
17	–	–	47	–	–	94	–	–	–	–	–
19	–	17	–	4874	–	10746	–	17	–	–	–
21	–	–	4899	–	–	2012010	–	–	146	–	–
22	–	–	–	507085	–	–	–	≥ 1	–	–	–
23	–	–	–	–	–	≥ 1	–	–	–	–	–
25	0	493	237118	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1

57.11 Theorem (see [478]) A supersimple $(v, 5, \lambda)$-design with $2 \le \lambda \le 5$ exists if and only if

$\lambda = 2$, $v \equiv 1, 5 \pmod{10}$, $v \ne 5, 15$, except possibly when $v \in \{115, 135\}$;
$\lambda = 3$, $v \equiv 1 \pmod{20}$ and $v \ge 21$, and possibly when $v \equiv 5 \pmod{20}$, $v \ge 25$ (Chen and Wei);
$\lambda = 4$, $v \equiv 0, 1 \pmod 5$ and $v \ge 15$;
$\lambda = 5$, $v \equiv 1 \pmod 4$ and $v \ge 17$, except possibly when $v = 21$.

57.3 Existence for Arbitrary k

57.12 Table All admissible triples (k, λ, v) according to Theorem 57.2 with $\lambda \geq 2$ and $v \leq 32$. If $\boxed{\lambda}$ is boxed, nonexistence is known. If $\underline{\lambda}$ is underlined, the existence is not decided. In all other cases existence is known. (See also [290, 477]).

k	v	λ	k	v	λ	k	v	λ	k	v	λ
4	7	2	4	8	3	5	11	2	5	15	$\boxed{2}$ 4
4	9	3	4	10	2 4	5	16	4	5	17	5
4	12	3	4	13	2 3 4 5	5	20	4	5	21	2 3 4 $\underline{5}$ $\underline{6}$
4	14	6	4	15	6	5	25	2 $\underline{3}$ 4 5 $\underline{6}$ 7	5	26	4 8
4	16	2 3 4 5 6 7	4	17	3 6	5	29	5	5	30	4 $\underline{8}$
4	18	6	4	19	2 4 6 8	5	31	2 4 $\underline{6}$ $\underline{8}$			
4	20	3 6 9	4	21	3 6 9	6	16	2	6	21	$\boxed{2}$ $\underline{3}$ 4
4	22	2 4 6 8 10	4	23	6	6	22	5	6	24	$\underline{5}$
4	24	3 6 9	4	25	2 3 4 5 6 7 8 9 10 11	6	25	5	6	26	$\underline{3}$ 6
4	26	6 12	4	27	6 12	6	27	$\underline{5}$	6	28	$\underline{5}$
4	28	2 3 4 5 6 7 8 9 10 $\underline{11}$ 12 13	4	29	3 6 9 12	6	30	$\underline{5}$	6	31	2 $\underline{3}$ $\underline{4}$ $\underline{5}$ $\underline{6}$ $\underline{7}$
4	30	6 12	4	31	2 4 6 8 10 12 14	7	22	$\boxed{2}$	7	28	2
4	32	3 6 9 12 15				7	29	$\underline{3}$	8	29	$\boxed{2}$

57.13 Theorem [974] Let G be an abelian group and $\mathcal{D}$ be a set of base blocks generating a $(k, 1)$-GDD of type g^u with no short orbits. Then $\mathcal{D} \cup -\mathcal{D}$ generates a supersimple $(k, 2)$-GDD of type g^u.

57.14 Theorem (see [1064]) A supersimple $\mathrm{TD}(4, \lambda; v)$ exists if and only if $\lambda \leq v$ and (λ, v) is neither $(1, 2)$ nor $(1, 6)$.

57.15 Theorem [1064] Let $k \geq 4$ and λ be positive integers. There exists a constant $v_0(k, \lambda)$ such that a supersimple (v, k, λ) design exists for every $v \geq v_0$ satisfying the necessary condition $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.

See Also

[1298]	Applications to superimposed codes.
[1978]	Applications to perfect hash families.

References Cited: [290, 475, 477, 478, 974, 1064, 1298, 1978, 2202]

58 Threshold and Ramp Schemes

K. Gopalakrishnan
Douglas R. Stinson

58.1 Threshold Schemes

58.1 Example Suppose that a bank has a vault that must be opened every day. The bank employs three senior tellers, but they do not want to trust any individual with the combination. Hence, they would like a system whereby any two of the three senior tellers can gain access to the vault. This problem can be solved by means of threshold schemes.

58.2 Remark Threshold schemes, which are a special case of secret sharing schemes, were first described by Shamir and Blakley in 1979. Blakley's solution uses finite geometries, while Shamir's scheme is based on polynomial interpolation (actually, orthogonal arrays in disguise).

58.3 A *perfect* (t, w)*-threshold scheme* is a method of sharing a secret key K among a finite set $\mathcal{P}$ of w participants, in such a way that any t participants can compute the value of K, but no group of $t-1$ (or fewer) participants can compute any information about the value of K (in an information-theoretic sense) from the shares they hold.

58.4 Remark The value of K is chosen by a special participant, the *dealer*. The dealer is denoted by D and it is assumed that $D \notin \mathcal{P}$. When D wants to share the key K among the participants in $\mathcal{P}$, he gives each participant some partial information, a *share*. The shares should be distributed secretly, so no participant knows the share given to another participant.

At a later time, a subset of participants $B \subseteq \mathcal{P}$ pool their shares in an attempt to compute the secret key K. If $|B| \geq t$, then they should be able to compute the value of K as a function of the shares they collectively hold; if $|B| < t$, then they should not be able to compute K. In Example 58.1, a $(2, 3)$-threshold scheme is desired.

Each share is chosen from a specified *share set* $\mathcal{S}$. It is well known that, in any perfect threshold scheme, $|\mathcal{K}| \leq |\mathcal{S}|$. A scheme where equality is attained is an *ideal scheme*.

58.5 Theorem An ideal (t, w)-threshold scheme with $|\mathcal{K}| = v$ is equivalent to an orthogonal array $OA(t, w+1, v)$.

58.6 Construction To obtain a threshold scheme from an $OA(t, w+1, v)$, associate the first w rows of the array with the w participants, and the last row with the key. If the dealer wants to share key K, then he chooses a random column of the array such that K occurs in the last row and gives out the remaining w elements in that column as the shares. Now, any t shares uniquely determine a column of the array, and the key is revealed as the element in the last row. But $t-1$ shares leave the key completely undetermined, since for any hypothetical value of the key, say K', there is a unique column containing the $t-1$ given shares and having K' in the last row.

58.2 Ramp Schemes

58.7 Remark Sometimes it is not necessary to have a "sharp" threshold, t, in securing a secret. This motivates the idea of a ramp scheme [279].

58.8 Let t_0, t_1, and w be nonnegative integers such that $t_0 < t_1 \leq w$. A (t_0, t_1, w)*-ramp scheme* is a method of splitting a secret key K into w shares, in such a way that K can be uniquely reconstructed from any t_1 of the w shares, but no information about K is revealed by any t_0 (or fewer) shares.

58.9 Remarks

1. A (t, w) threshold scheme is the same as a $(t-1, t, w)$-ramp scheme.
2. As the number of shares in a ramp scheme is increased from t_0 to t_1, the amount of information about the secret gradually increases, as well.
3. In a $(0, t_1, w)$-ramp scheme, there is no security requirement. In this case, the resulting scheme is known as an *information dispersal algorithm*.

58.10 Theorem [1177] $|\mathcal{K}| \leq |\mathcal{S}|^{t_1 - t_0}$ in any (t_0, t_1, w)-ramp scheme.

58.11 Theorem [1177] If there exists an $OA(t_1, w+t_1-t_0, v)$, then there exists a (t_0, t_1, w)-ramp scheme in which $|\mathcal{S}| = v$ and $|\mathcal{K}| = v^{t_1-t_0}$.

58.12 Construction This is a generalization of Construction 58.6. Start with an $OA(t_1, w+t_1-t_0, v)$, associate the first w rows of the orthogonal array with the w participants, and associate the last t_1-t_0 rows with the key (thus, a key is a (t_1-t_0)-tuple). If the dealer wants to share key $K = (k_1, \ldots, k_{t_1-t_0})$, then he chooses a random column of the array such that the tuple K occurs in the last t_1-t_0 rows and gives out the remaining w elements in that column as the shares. Any t_1 shares uniquely determine a column of the array, and the key is revealed. But t_0 shares leave the key completely undetermined, since for any hypothetical value of the key, say K', there is a unique column containing the t_0 given shares and having the tuple K' in the last t_1-t_0 rows.

58.3 Anonymous Threshold Schemes

58.13 A perfect threshold scheme is *anonymous* if the following two properties are satisfied:

1. The w participants receive w distinct shares.
2. The key can be computed solely as a function of t shares, without the knowledge of which participant holds which share. Thus, the key computation can be performed by a black box that is given t shares and does not know the identities of the participants holding those shares.

58.14 Theorem [1977] In an anonymous (t, w)-threshold scheme, $|\mathcal{S}| \geq |\mathcal{K}|(w-t+1)+t-1$. Further, equality occurs if and only if there exists a Steiner system $S(t, w, v)$ that can be partitioned into $S(t-1, w, v)$.

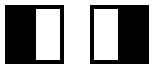
58.15 Example Using Theorem 58.14, a large set $\mathcal{L}$ of $S(2, 3, 9)$ can be used to construct an anonymous $(3, 3)$-threshold scheme with seven possible keys. $\mathcal{L}$ consists of seven disjoint $S(2, 3, 9)$. Denote them by $(X, \mathcal{B}_i)$ $(0 \leq i \leq 6)$. Now, the seven keys correspond to the seven designs in $\mathcal{L}$; the shares are the nine points in X. If the dealer's secret key is K, where $0 \leq K \leq 6$, then he chooses a random block B from $\mathcal{B}_K$ and gives the three points in B to the three participants as their shares. Now, three shares uniquely determine the block B, which occurs in exactly one of the seven designs (because $\mathcal{L}$ is a large set). Hence, three participants can compute K. But from two shares, say x and y, nothing can be determined, since for each possible secret K', there is a (unique) block in $\mathcal{B}_{K'}$ that contains x and y.

58.4 Visual Cryptography

58.16 Remark Naor and Shamir introduced *visual cryptography*, where the secret and each share consists of a collection of black and white (transparent) pixels on a transparency. In a (t, w)-visual threshold scheme, the secret is an image obtained by stacking t transparencies, so the "computation" is performed by the human visual system. Realizing a visual threshold scheme requires expanding each pixel into some number $m \geq 2$ of subpixels in each of the w shares. A reconstructed pixel is not necessarily totally black or white—there is a loss of contrast, which is measured by the difference in darkness between a reconstructed black and white pixel. The goal of a visual threshold scheme is to maximize the contrast while minimizing the pixel expansion.

58.17 Construction The following is Naor and Shamir's algorithm for encoding one pixel in a visual $(2, 2)$-threshold scheme. The algorithm is to be applied for every pixel P in the secret image in order to construct the two shares. A pixel P is split into $m = 2$

subpixels in each of the two shares. If the given pixel P is white, then a random choice of one of the first two rows in the following table is made. If the given pixel P is black, then a random choice of one of the last two rows of the table is made. Then the pixel P is encrypted as two subpixels in each of the two shares, as determined by the chosen row.

Pixel		s_1	s_2	$s_1 + s_2$
	$p = .5$			
	$p = .5$			
	$p = .5$			
	$p = .5$			

In this scheme, a reconstructed pixel (consisting of two subpixels) has a *grey level* equal to 1 if P is black and a grey level equal to 1/2 if P is white. Therefore, there is a 50% loss of contrast in the reconstructed image. The pixel expansion is equal to 2 because each pixel is split into two subpixels (in each of the shares).

58.18 In a (t, w)-visual threshold scheme, suppose that the grey level of a reconstructed white pixel is equal to g_0 and the grey level of a reconstructed black pixel is equal to g_1. Then the visual threshold scheme has *contrast* equal to $g_1 - g_0$. The contrast of the scheme is denoted by γ.

58.19 Theorem [288] In any $(2, w)$-visual threshold scheme, $\gamma \le \gamma^*(w)$, where

$$\gamma^*(w) = \begin{cases} \frac{w}{4w-4} & \text{if } w \text{ is even} \\ \frac{w+1}{4w} & \text{if } w \text{ is odd.} \end{cases}$$

58.20 Theorem [288] Suppose w is even. Then there exists a $(2, w)$-visual threshold scheme with pixel expansion m and optimal contrast $\gamma^*(w)$ if and only if there exists a $\mathrm{BIBD}\Big(w, \frac{w}{2}, \frac{m(w-2)}{4w-4}\Big)$.

58.21 Theorem [288] Suppose w is odd. Then there exists a $(2, w)$-visual threshold scheme with pixel expansion m and optimal contrast $\gamma^*(w)$ if and only if there exists a $\Big(w, \{\frac{w-1}{2}, \frac{w+1}{2}\}, r - \frac{m(w+1)}{4w}\Big)$-PBD such that every point occurs in exactly r blocks, where r is an integer such that $\frac{(w-1)m}{2w} \le r \le \frac{(w+1)m}{2w}$.

58.22 Theorem [288] Suppose that there exists a $(2, w)$-visual threshold scheme with pixel expansion m and optimal contrast $\gamma^*(w)$.

1. If w is even, then $m \ge 2w - 2$, and $m = 2w - 2$ if and only if there exists a $\mathrm{BIBD}\big(w, \frac{w}{2}, \frac{w}{2} - 1\big)$.
2. If $w \equiv 3 \bmod 4$, then $m \ge w$, and $m = w$ if and only if there exists a $\mathrm{BIBD}\big(w, \frac{w-1}{2}, \frac{w-3}{4}\big)$. (This BIBD is equivalent to a Hadamard matrix of order $w + 1$.)
3. If $w \equiv 1 \bmod 4$, then $m \ge 2w$, and $m = 2w$ if and only if there exists a $\mathrm{BIBD}\big(w, \frac{w-1}{2}, \frac{w-3}{2}\big)$ or a $\mathrm{BIBD}\big(w + 1, \frac{w+1}{2}, \frac{w-1}{2}\big)$.

See Also

§II.1	Balanced incomplete block designs.
§II.4.4	Large sets of t-designs.
§III.3	Orthogonal arrays of strength 2.
§III.7	Orthogonal arrays of strength $t > 2$.
§V.1	Hadamard matrices and designs.
[1915, 1970]	Surveys on secret sharing schemes.
[1972]	Chapter 13 concerns secret-sharing schemes.
[278, 1890]	The papers that introduced threshold schemes.
[279]	The paper that introduced ramp schemes.
[1177]	Provides numerous results on ramp schemes.
[1977]	Connects anonymous threshold schemes and designs.
[1666]	The paper that introduced visual cryptography.
[288, 773]	Connects visual threshold schemes and design theory.

References Cited: [278, 279, 288, 773, 1177, 1666, 1890, 1915, 1970, 1972, 1977]

59 (t,m,s)-Nets

William J. Martin

59.1 Definitions and Motivation

59.1 Let $[0,1)^s$ be the half-open unit cube of dimension s and suppose numerical computation is to be done in base $b \geq 2$. An *elementary interval in base b* in $[0,1)^s$ is a euclidean set of the form

$$E = \prod_{i=1}^{s} \left[\tfrac{a_i}{b^{d_i}}, \tfrac{a_i+1}{b^{d_i}}\right)$$

where each integer $d_i \geq 0$ and for each i, the integer a_i satisfies $0 \leq a_i < b^{d_i}$. Clearly, $\mathrm{Vol}(E) = b^{-\sum d_i}$.

59.2 **Example** The set $E = [0, 1/2) \times [9/16, 10/16) \times [0, 1)$, contained in the unit 3-cube, is an elementary interval in base two having volume 2^{-5}.

59.3 Let $s \geq 1$, $b \geq 2$, and $m \geq t \geq 0$ be integers. A (t, m, s)-*net in base b* is a multiset $\mathcal{N}$ of b^m points in $[0,1)^s$ with the property that every elementary interval in base b of volume b^{t-m} contains precisely b^t points from $\mathcal{N}$.

59.4 **Remark** For a collection $\mathcal{N}$ of N points in the unit s-cube, the expected number of points in an interval $E = \prod_i [a_i, b_i)$ of volume ϵ is ϵN.

59.5 The *local discrepancy* of a particular interval E is the absolute value of $|\mathcal{N} \cap E|/N - \mathrm{Vol}(E)$. The *star-discrepancy* of a set $\mathcal{N}$ is then $D_N^*(\mathcal{N}) = \sup_E \left| \frac{|\mathcal{N} \cap E|}{N} - \mathrm{Vol}(E) \right|$ where the supremum is over all intervals $E = \prod_i [0, a_i)$ contained in $[0,1)^s$.

59.6 **Theorem** (Koksma–Hlawka Inequality) If f is a function of s variables with bounded variation $V(f) < +\infty$, then $\left| \int_{[0,1]^s} f(u)\, du - \frac{1}{N} \sum_{x \in \mathcal{N}} f(x) \right| \leq V(f) D_N^*(\mathcal{N})$.

59.7 **Theorem** [1677, 1678] A (t, m, s)-net in base $b = 2$ satisfies $D_N^*(\mathcal{N}) \leq \frac{2^t}{N} \sum_{i=0}^{s-1} \binom{m-t}{i}$ and a (t, m, s)-net in base $b \geq 3$ satisfies $D_N^*(\mathcal{N}) \leq \frac{b^t}{N} \sum_{i=0}^{s-1} \binom{s-1}{i} \binom{m-t}{i} \lfloor \frac{b}{2} \rfloor^i$.

59.8 Remark From Theorems 59.6 and 59.7, (t, m, s)-nets yield Quasi-Monte Carlo methods for numerical integration (deterministic surrogates for Monte Carlo methods). These are important in contexts where random number generation becomes computationally expensive; also as the net gets larger, the error bound scales as $O(N^{-1})$ in comparison with $O(N^{-\frac{1}{2}})$ for Monte Carlo methods.

59.9 Remark In addition, (t, m, s)-nets are useful for simulations and pseudorandom number generation.

59.10 Remark For applications, it is important to have a nested sequence of (t_i, m_i, s)-nets (with m_i going to infinity) in the same dimension s and with all t_i bounded above by a constant t. This allows one to improve estimates on an integral without losing the benefit of preliminary computations. Such a sequence of nets can be constructed via (t, s)-sequences.

59.11 Let $s \geq 1$, $b \geq 2$, and $t \geq 0$ be integers. A (t, s)-*sequence in base* b is an infinite sequence $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots$ of points in $[0,1]^s$ with the property that, for every $m > t$ and every $k \geq 0$, the set

$$\mathcal{N} = \{[\mathbf{x}_i] : kb^m \leq i < (k+1)b^m\}$$

is a (t, m, s)-net in base b. Here, $[\mathbf{x}]$ represents the point obtained by truncating each coordinate of $\mathbf{x}$ to m digits of accuracy in a fixed prescribed b-adic expansion of it.

59.12 Example (van der Corput sequence) Fix a base $b \geq 2$ and, for an integer $n \geq 0$, write $n = \sum_{j=0}^{\infty} a_j b^j$ with $0 \leq a_j < b$ and take the rational number $x_n = \sum_{j=0}^{\infty} a_j b^{-j-1}$. Then $x_0, x_1, x_2, \ldots$ is a $(0, 1)$-sequence in base b.

59.13 Remarks [1678, Ch. 3] In Example 59.12, write $\phi_b(n) = \sum_{j=0}^{\infty} a_j b^{-j-1}$. The *Halton sequence* is then $\mathbf{x}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n))$, $n \geq 0$ where $b_1, b_2, \ldots, b_s$ are integers greater than one and the *Hammersley point set* is the set $\mathbf{x}_0, \ldots, \mathbf{x}_{N-1}$ given by $\mathbf{x}_n = (\frac{n}{N}, \phi_{b_1}(n), \ldots, \phi_{b_{s-1}}(n))$ where the bases $b_1, \ldots b_{s-1} \geq 2$ are arbitrary and discrepancy bounds are strongest when the b_i are relatively prime. These popular low-discrepancy point sets are not (t, s)-sequences.

If one orders the primitive polynomials over $\mathbb{F}_2$ by degree $p_1(x), p_2(x), \ldots$, then the *Sobol' sequence* yields a (t_s, s)-sequence in base $b = 2$ for each s where $t_s = \sum_{i=1}^{s-1}(\deg p_i - 1)$. Unrelated to this, the *Niederreiter sequence* in any prime power base q yields a $(T_q(s), s)$-sequence where $T_q(s) = \sum_{i=1}^{s}(\deg p_i - 1)$ for any collection of pairwise relatively prime polynomials $p_1(x), p_2(x), \ldots$ of positive degree over $\mathbb{F}_q$ [1678, Sec. 4.5] so that, in particular, $T_2(s) < t_s$ for $s \geq 8$ if polynomials of lowest possible degree are chosen for the construction of the Niederreiter sequence.

59.14 Theorem [1677, Lem. 5.15] If a (t, s)-sequence in base b exists, then there exist $(t, m, s+1)$-nets in base b for all $m \geq t$.

59.15 Remark The finite problem of deciding whether a (t, m, s)-net exists can yield not only nonexistence results for (t, s)-sequences but can also indicate what to aim for and how to find it.

59.16 Remark For nets, the goal is to construct (t, m, s)-nets for any dimension s and with any size b^m having *quality parameter* t as close to zero as possible. Among two nets with the same number of points, one prefers the one which evenly samples more elementary intervals. At the trivial end, when $t = m$, no structure is imposed and any multiset of b^m points in $[0,1)^s$ is an (m, m, s)-net. When $t = m - 1$, the requirement is simply that the projections of the points $x \in \mathcal{N}$ onto any coordinate are uniformly distributed among the intervals $[a/b, (a+1)/b)$ $(0 \leq a < b)$. Hence the cases of interest are when $m \geq t + 2$. At the other end of the spectrum, it is known that for $m > 1$, a $(0, m, s)$-net in base b can exist only in dimensions $s \leq b + 1$ since a $(0, 2, s)$-net in

base b is equivalent to $s-2$ MOLS of order b (see Theorem 59.18).

59.2 Constructions and Propagation Rules

59.17 Remark Theorem 59.18 gives a connection between orthogonal arrays and certain (t,m,s)-nets. See also Theorems 59.32 and 59.21 as well as Remark 59.28.

59.18 Theorem [1677] A $(0,2,s)$-net in base b exists if and only if there exist $s-2$ MOLS of order b. (More generally, a $(t,t+2,s)$-net in base b is equivalent to an $\mathrm{OA}_{b^t}(2,s,b)$.)

59.19 Construction Suppose there exist $s-2$ mutually orthogonal latin squares $L_h=[\ell_{ij}^{(h)}]$ $(1\le h\le s-2)$ defined over the digits $0,1,\ldots,b-1$ and with rows and columns indexed by $0,1,\ldots,b-1$. Let σ be any function from $\{1,\ldots,s-2\}$ to itself satisfying $\sigma i\ne i$ for all i. The b^2 points $\mathbf{x}_n$ $(0\le n<b^2)$ in $[0,1)^s$ are defined by $\mathbf{x}_{ib+j}=\frac{1}{b^2}\left(b\ell_{ij}^{(1)}+\ell_{ij}^{(\sigma 1)},\ldots,b\ell_{ij}^{(s-2)}+\ell_{ij}^{(\sigma(s-2))},bi+\ell_{ij}^{(1)},bj+\ell_{ij}^{(1)}\right)$.

59.20 Example To see how two MOLS(3) are used to construct the $(0,2,4)$-net in base 3 $\mathcal{N}=\{(0,0,0,0),(\frac{4}{9},\frac{4}{9},\frac{1}{9},\frac{4}{9}),(\frac{8}{9},\frac{8}{9},\frac{2}{9},\frac{8}{9}),(\frac{5}{9},\frac{7}{9},\frac{4}{9},\frac{1}{9}),(\frac{2}{3},\frac{2}{9},\frac{5}{9},\frac{5}{9}),(\frac{1}{9},\frac{1}{3},\frac{1}{3},\frac{2}{3}),(\frac{7}{9},\frac{5}{9},\frac{8}{9},\frac{2}{9}),(\frac{2}{9},\frac{2}{3},\frac{2}{3},\frac{1}{3}),(\frac{1}{3},\frac{1}{9},\frac{7}{9},\frac{7}{9})\}$, apply Construction 59.19 to the 2 MOLS(3) on the left, with rows and columns numbered 0,1,2 and with σ swapping 1 and 2. The resulting net $\mathcal{N}$ is presented on the right.

0	1	2
1	2	0
2	0	1

0	1	2
2	0	1
1	2	0

.00	.00	.00	.00
.11	.11	.01	.11
.22	.22	.02	.22
.12	.21	.11	.01
.20	.02	.12	.12
.01	.10	.10	.20
.21	.12	.22	.02
.02	.20	.20	.10
.10	.01	.21	.21

59.21 Theorem [262] If there is a linear q-ary $[s,s-m,k+1]$ code and $\mathrm{GR}(2k-2\ell,s-1,\ell,b)<b^{m-\ell+1}$ for all $2\le\ell<k$, then there exists a (t,m,s)-net in base b where $t=m-k$.

59.22 Remark The quantity $\mathrm{GR}(2r,s,\ell,b)$ is the size of a ball of radius r in so-called "NRT space" [262] and is the sum of the coefficients of $x^0,x^1,\ldots,x^r$ in the expansion of $[1+(b-1)x+(b^2-b)x^2+\cdots+(b^\ell-b^{\ell-1})x^\ell]^s$.

59.23 Remark The most powerful known constructions of (t,s)-sequences are those of Niederreiter and Xing (see [1680]), based on global function fields with many places. Rather than delve into algebraic geometry here, the flavor of these constructions is exhibited with an elementary (t,m,s)-net analog of Reed–Solomon codes.

59.24 Example (Rosenbloom,Tsfasman) Let q be a prime power, $S=\{a_1,\ldots,a_s\}\subseteq\mathbb{F}_q$ and $1\le m\le q$. Fix any bijection $\beta:\mathbb{F}_q\to\{0,\ldots,q-1\}$ and write $((c))=\beta(c)$ for $c\in\mathbb{F}_q$. The set $\mathcal{N}$ contains a point $\mathbf{x}_f$ for each polynomial $f(t)\in\mathbb{F}_q[t]$ of degree less than m, where the ith coordinate of $\mathbf{x}_f$ is $(\mathbf{x}_f)_i=\sum_{j=0}^{m-1}((f^{(j)}(a_i)))q^{-1-j}$, where $f^{(j)}(a_i)$ denotes the evaluation of the jth derivative of f at the point a_i. Since a nonzero polynomial of degree n has at most n roots, counting multiplicities, this is a $(0,m,s)$-net in base q. One may obtain $s=q+1$ by extending the coordinates to the projective line $PG(1,q)$. As in coding theory, one then replaces S with a set of points on some algebraic curve to obtain (t,m,s)-net analogs of Goppa codes and the like.

59.25 Theorem A representative sample of the dozens of propagation rules known. (See [1680] and references therein.)

1. **projection:** Every (t, m, s)-net in base b yields a (t', m, s')-net in base b for every $t \le t' \le m$ and every $1 \le s' \le s$.
2. **subnets:** Every (t, m, s)-net in base b yields a (t, m', s)-net in base b for each $t \le m' \le m$.
3. **base change:** Every (t, m, s)-net in base b^r with $r \ge 1$ yields a (t', rm, s)-net in base b with $t' = \min\{rt + (r-1)(s-1), rm\}$.
4. **product:** If a (t_1, m_1, s_1)-net exists in base b and a (t_2, m_2, s_2)-net exists in base b with $s_1 \le s_2$, then a $(t, m_1{+}m_2, s_1{+}s_2)$-net exists for $t = \max(m_1{+}t_2, m_2{+}t_1)$. (See also the $(u, u+v)$-construction in [262].)

59.3 Ordered Orthogonal Arrays

59.26 In an array with $s\ell$ columns, labeled $\{(i,j) : 1 \le i \le s, 1 \le j \le \ell\}$, a set T of columns is *left-justified* if $(i,j) \in T$ with $j > 1$ implies $(i, j-1) \in T$. An *ordered orthogonal array* $\mathrm{OOA}_\lambda(t, s, \ell, v)$ is a $\lambda v^t \times s\ell$ array $A = (a_{r,(i,j)})$ with columns indexed by ordered pairs (i,j) as above and with elements from an alphabet F of size v, with the property that every left-justified set T of t columns has the *OA property*: in the subarray obtained by restricting to columns lying in T, each t-tuple over F occurs exactly λ times as a row.

59.27 Example An $\mathrm{OOA}_2(3,3,3,2)$ and an $\mathrm{OOA}_1(2,3,2,4)$.

0	0	0	0	0	0	0	0	0
0	0	1	1	0	1	1	0	1
0	1	0	1	1	0	1	0	0
0	1	1	0	1	1	0	0	1
1	0	0	0	1	0	1	0	0
1	0	1	1	1	1	0	0	1
1	1	0	1	0	0	0	0	0
1	1	1	0	0	1	1	0	1
0	0	0	1	1	0	0	1	0
0	0	1	0	1	1	1	1	1
0	1	0	0	0	0	1	1	0
0	1	1	1	0	1	0	1	1
1	0	0	1	0	0	1	1	0
1	0	1	0	0	1	0	1	1
1	1	0	0	1	0	0	1	0
1	1	1	1	1	1	1	1	1

0	0	0	0	0	0
0	1	2	1	3	1
0	2	3	2	1	2
0	3	1	3	2	3
1	0	1	0	1	0
1	1	3	1	2	1
1	2	2	2	0	2
1	3	0	3	3	3
2	0	2	0	2	0
2	1	0	1	1	1
2	2	1	2	3	2
2	3	3	3	0	3
3	0	3	0	3	0
3	1	1	1	0	1
3	2	0	2	2	2
3	3	2	3	1	3

In the second example, with natural ordering of the columns the left-justified sets of two columns are $\{1,2\}$, $\{3,4\}$, $\{5,6\}$, $\{1,3\}$, $\{1,5\}$, $\{3,5\}$ labeled $\{(1,1),(1,2)\}$, $\{(2,1),(2,2)\}$, $\{(3,1),(3,2)\}$, $\{(1,1),(2,1)\}$, $\{(1,1),(3,1)\}$, $\{(2,1),(3,1)\}$, respectively.

59.28 Remark For any $1 \le \ell' < \ell$, one may delete columns (i,j) with $j > \ell'$ from any $\mathrm{OOA}_\lambda(t, s, \ell, v)$ to obtain an $\mathrm{OOA}_\lambda(t, s, \ell', v)$. In particular, with $\ell' = 1$, this yields an $\mathrm{OA}_\lambda(t, s, v)$.

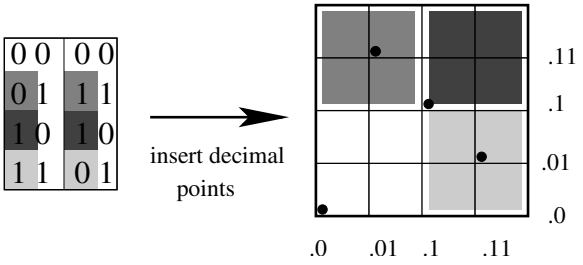
59.29 If the alphabet F is a field and the rows of the OOA form a subspace of $F^{s\ell}$, then the OOA is a *linear OOA*. These correspond to *digital* (t, m, s)*-nets*.

59.30 Remark All statements in Theorem 59.25 remain valid for digital nets.

59.31 Remark The connection to combinatorial designs is based on Theorem 59.32.

59.32 Theorem [1407, 1649] There exists a (t, m, s)-net in base b if and only if there exists an $\mathrm{OOA}_{b^t}(m-t, s, m-t, b)$.

59.33 Example An $\mathrm{OOA}_1(2,2,2,2)$ and the corresponding $(0,2,2)$-net $\mathcal{N} = \{(0,0), (\frac{1}{4}, \frac{3}{4}), (\frac{1}{2}, \frac{1}{2}), (\frac{3}{4}, \frac{1}{4})\}$ in base $b = 2$. The shading indicates the partition of the OOA determined by values in columns $(1,1)$ and $(2,1)$ and the corresponding partition of the cube into intervals of size $b^{-1} \times b^{-1}$.



59.4 Bounds on OOAs and Nets

59.34 Theorem (Orthogonal Array Bound, Clayman et al.) If a (t, m, s)-net exists in base b, then $s \le \min_{t+2 \le h \le m} f(b^h, b, h-t)$ where $f(N, b, \tau)$ is the maximum value of k for which an $\mathrm{OA}(\tau, k, b)$ exists with N columns.

59.35 Theorem (Generalized Rao Bound; Martin, Stinson) If there exists a (t, m, s)-net in base b, then $b^n \ge \mathrm{GR}(n-t, s, n-t, b)$ for all integers n such that $t+2 \le n \le m$ where

$$\mathrm{GR}(k, s, \ell, b) = \begin{cases} 1 + \sum_{h=1}^{k/2} \sum_{w=1}^{h} \binom{s}{w} N_{h,w,\ell} (b-1)^w b^{h-w} & (k \text{ even}); \\ \mathrm{GR}(k-1, s, \ell, b) + \sum_{w=1}^{(k+1)/2} \binom{s-1}{w-1} N_{\frac{k+1}{2},w,\ell} (b-1)^w b^{\frac{k+1}{2}-w} & (k \text{ odd}) \end{cases}$$

and $\quad N_{h,w,\ell} = \sum_{j=0}^{\lfloor \frac{h-w}{\ell} \rfloor} (-1)^j \binom{w}{j} \binom{h-\ell j-1}{w-1}$.

59.36 Theorem (Dual Plotkin Bound; Martin,Visentin) For a (t, m, s)-net in base b, let $\ell = 1 + \lfloor \frac{m-t}{s} \rfloor$, then $t \ge m + 1 - \frac{s}{1-b^{m-s\ell}} \left(\ell - \frac{1}{b} - \frac{1}{b^2} - \cdots - \frac{1}{b^\ell} \right)$.

59.37 Remark These bounds are special cases of the linear programming bound [1526].

See Also

§III.7	Orthogonal arrays of higher strength.
§VI.1	Association schemes.
§VII.1	Linear codes.
[1858]	`http://mint.sbg.ac.at/` Online tool giving tables with latest constructions and bounds.
[1679]	Applications of (t, m, s)-nets. `http://www.netlib.org/`: TOMS647, a library of FORTRAN90 routines, using single precision arithmetic, which implements the Faure, Halton, and Sobol' quasirandom sequences.
[1680]	Randomized (or "scrambled") nets which allow for error analysis.

References Cited: [262, 1407, 1526, 1649, 1677, 1678, 1679, 1680, 1858]

60 Trades

A. S. Hedayat
Gholamreza B. Khosrovshahi

60.1 Definitions and Examples

60.1 Let $v > k > t \geq 1$ be three integers and $P_l(X)$ be the set of all l-subsets based on a v-set X. A $\mathrm{T}(t,k,v)$ *trade* T based on the elements (blocks) of $P_k(X)$ is a pair of nonempty disjoint collections, T_1 and T_2, each consisting of m blocks from $P_k(X)$, such that the number of times that each element of $P_t(X)$ is covered by T_1 is the same as the number of times it is covered by T_2. Repetition of a block is permitted within T_i, and an element of $P_t(X)$ need not be covered at all. T_1 and T_2 are the two *legs* of the trade or the *trade mates.*

60.2 A trade is *simple* if there are no repeated blocks. A trade is *Steiner* if no element of $P_t(X)$ is repeated more than once in any leg of the trade.

60.3 The *foundation* of a trade is the set of s elements from X appearing in the trade.

60.4 Remark The four integers m, k, s, and t are the *basic parameters* of a trade and are the *volume, length, foundation size,* and the *strength* of the trade, respectively.

60.5 Remark A $\mathrm{T}(t,k,v)$ trade based on $P_k(X)$ is also a $\mathrm{T}(t,k,u)$ trade based on $P_k(Y)$ if $X \subset Y$ and $|Y| = u$. A trade of strength t is also a trade of strength t' for all $t' < t$.

60.6 Remark Depending on the context, the elements of $P_k(X)$ are denoted by x_1,x_2,$\cdots$,x_k or $x_1x_2\cdots x_k$ while the order among the k elements is immaterial.

60.7 Example Let $X = \{1, 2, \ldots, 6\}$. Then $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2\}$ is an example of a Steiner T(2,3,6) trade on $P_3(X)$, where $\mathrm{T}_1 = \{123, 156, 246, 345\}$ and $\mathrm{T}_2 = \{126, 135, 234, 456\}$. T has volume 4 and foundation size 6. T is also a $\mathrm{T}(2,3,u)$ trade for $u \geq 6$.

60.8 Example Let $X = \{1, 2, \ldots, 6\}$. Then $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2\}$ is an example of a simple (but not a Steiner) T(2,3,6) trade on $P_3(X)$, where $\mathrm{T}_1 = \{123, 124, 156, 256, 345, 346\}$ and $\mathrm{T}_2 = \{125, 126, 134, 234, 356, 456\}$.

60.2 Foundation Size and Volume

60.9 Theorem A $\mathrm{T}(t,k,v)$ trade has foundation size at least $k+t+1$ and volume at least 2^t.

60.10 A *basic trade* is a $\mathrm{T}(t,k,v)$ trade with volume 2^t. A *minimal trade* is a basic $\mathrm{T}(t,k,v)$ trade with foundation $k+t+1$.

60.11 Remark [1159] There exists a minimal $\mathrm{T}(t,k,v)$ trade. It is unique up to isomorphism.

60.12 Example Let $X = \{1, 2, \cdots, 8\}$, $\mathrm{T}_1 = \{1356, 1478, 2378, 2456\}$, and $\mathrm{T}_2 = \{1378, 1456, 2356, 2478\}$. Then $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2\}$ is a basic trade that is not a minimal trade.

60.13 Example The Steiner $\mathrm{T}(2,3,6)$ trade in Example 60.7 is a minimal $\mathrm{T}(2,3,6)$ trade.

60.14 Theorem [954] A $\mathrm{T}(2,k,v)$ trade with volumes $2^{t+1} - 2^{t-i}$ exists for all i, $0 \leq i \leq t$.

60.15 Theorem [1129] A $\mathrm{T}(t,k,v)$ trade with volume m exists if $m \geq (t-2)2^t + 2^{t-1} + 2$.

60.16 Theorem [1290] No T(t,k,v) trade exists with volume m for $2^t \le m \le 2^t + 2^{t-1}$.

60.17 Theorem [1130] There are no Steiner T(t,k,v) trades with volume m when:
(i) $2^t + 2^{t-1} < m < 2^t + 2^{t-1} + 2^{t-2}$,
(ii) $m = 29$ and $t = 4$, or
(iii) $m < (t-1)2^t + 2$ when $k > t+1$.

60.18 Conjecture (Khosrovshahi–Malek) For every α with $1 \le \alpha \le t-1$, there is no trade with volume m for $\sum_{i=\alpha+1}^{t} 2^i < m < \sum_{i=\alpha}^{t} 2^i$.

60.3 Building Minimal Trades by Polynomials

60.19 Theorem [940, 952] Let $2 \le t < k,\ v \ge k+t+1$, and let $X = \{1, 2, \cdots, v\}$. Further, let $B = (b_1, b_2, \cdots, b_k)$ and $C = (c_1, c_2, \cdots, c_{t+1})$ be two disjoint and arbitrarily ordered subsets of sizes k and $t+1$ of X, respectively. Use B and C to form the polynomial:

$$\phi(x_1, \cdots, x_v) = (x_{b_1} - x_{c_1}) \cdots (x_{b_{t+1}} - x_{c_{t+1}}) x_{b_{t+2}} \cdots x_{b_k}.$$

Upon multiplication, there are 2^t terms with "+" sign and 2^t terms with "−" sign. Let T_1 be the 2^t blocks of size k formed by taking the k subscripts in 2^t terms with "+" signs. Similarly form T_2 by taking the k subscripts in 2^t terms with "−" signs. Then $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2\}$ is a minimal T(t,k,v) trade.

60.20 Example Let $v = 6,\ k = 3$, and $t = 2$. Choose $B = (1,2,3)$ and $C = (4,5,6)$. Then

$$\phi(x_1, \cdots, x_6) = (x_1 - x_4)(x_2 - x_5)(x_3 - x_6)$$

upon multiplication produces $\mathrm{T}_1 = \{123, 156, 426, 453\}$ and $\mathrm{T}_2 = \{126, 153, 423, 456\}$. $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2\}$ is a minimal T(2,3,6) trade as in Example 60.7.

60.21 Example Let $v = 8,\ k = 4$, and $t = 2$. Choose $B = (1,2,3,4)$ and $C = (5,6,7)$. Then

$$\phi(x_1, \cdots, x_8) = (x_1 - x_5)(x_2 - x_6)(x_3 - x_7)x_4$$

produces a minimal trade: T(2,4,8) $= \{\mathrm{T}_1, \mathrm{T}_2\}$ where $\mathrm{T}_1 = \{1234, 3456, 1467, 2457\}$ and $\mathrm{T}_2 = \{1247, 4567, 1346, 2345\}$.

60.4 A Linear Algebraic Representation of Trades

60.22 Let $1 < t < k \le v - t$, and let X be a v-element set. Order $P_t(X)$ and $P_k(X)$ lexicographically (or with any other ordering). Let $W_{tk}(v)$ be the $\binom{v}{t} \times \binom{v}{k}$ inclusion matrix where rows are indexed by the elements of $P_t(X)$ and the columns are indexed by the elements of $P_k(X)$. The (i,j)th entry of $W_{tk}(v)$ is one if the jth element of $P_k(X)$ contains the ith element of $P_t(X)$ and zero otherwise. If v can be deduced from the context, then $W_{tk}(v)$ is simply presented by W_{tk}. (See §VII.7.6)

60.23 Remark Given a collection of elements of $P_k(X)$, a $\binom{v}{k}$ column vector F' can be associated with it: $F' = (f_1, \cdots, f_{\binom{v}{k}})$ where f_i is the frequency of ith element of $P_k(X)$ in this collection. Conversely, for a given column vector, F' of size $\binom{v}{k}$ with nonnegative integers, a collection of the elements of $P_k(X)$ can be associated with it by taking f_i copies of the ith element of $P_k(X)$. Also for a given $S = \{S_1, S_2\}$, where S_1 and S_2 are two disjoint collections of m elements each from $P_k(X)$, an integral $\binom{v}{k}$ column vector F can be associated with it whose ith entry is f_i if the ith block of $P_k(X)$ appears f_i times in S_1 or $-f_i$ if the ith block of $P_k(X)$ appears f_i times in S_2. F represents a t-design if $W_{tk}(v)F = \lambda J$ where λ is a positive integer and J is the all 1 vector.

60.24 Theorem A $\binom{v}{k}$ integral vector F is a $\mathrm{T}(t,k,v)$ trade if and only if $W_{tk}F = 0$. The positive components of F identify the frequencies of the blocks in T_1, and the negative components (sign ignored) identify the frequencies of the blocks in T_2.

60.25 Remark If F_1 and F_2 represent two trades based on $W_{tk}(v)$, then $F_1 + F_2$ as well as $nF_1 (n \in \mathbb{Z})$ are also trades based on $W_{tk}(v)$. Therefore, the set of all $\mathrm{T}(t,k,v)$ trades forms a $\mathbb{Z}$-module. (It is well known that the rank of $W_{tk}(v)$ is $\binom{v}{t}$, therefore, the null space of $W_{tk}(v)$ that generates all $\mathrm{T}(t,k,v)$ trades has dimension $\binom{v}{k}-\binom{v}{t}$.) Indeed, a basis for this null space can be constructed consisting solely of minimal trades [1288].

60.26 Construction In [1290], an explicit method of constructing a triangular basis for $\mathrm{T}(t,k,v)$ trades is given. Construct $\binom{v}{k}-\binom{v}{t}$ subsets, $B_1, \cdots, B_{\binom{v}{k}-\binom{v}{t}}$, so that for each such subset $B = j_1 j_2 \cdots j_k$ (using the notation from Remark 60.6) the following conditions are satisfied:

- $j_1 < j_2 < \cdots < j_k$;
- $j_h \le v - k - t + 2h - 2,\ 1 \le h \le t+1$; and
- $j_h \le v - k + 1,\ t+2 \le h \le k$.

Now construct $\binom{v}{k}$–$\binom{v}{t}$ corresponding companion sets $C_1, C_2, \ldots, C_{\binom{v}{k}-\binom{v}{t}}$ as follows: If $B_s = b_1 b_2 \cdots b_k$ is a block, then its companion set C_s is defined to be $C_s = c_1 c_2 \cdots c_{t+1}$ where $c_i = min(\{b_i + 1, \ldots v\} - \{c_{i+1}, \cdots, c_{t+1}, b_{i+1}, \ldots, b_{t+1}\})$ for $i = 1, 2, \cdots, t+1$. Use Theorem 60.19 to build the required $\binom{v}{k} - \binom{v}{t}$ minimal trades for the basis of $W_{tk}(v)$. In particular, this basis is in a triangular form with regard to $\bar{W}_{tk}(v)$, where $\bar{W}_{tk}(v)$ is obtained from $W_{tk}(v)$ by allowing its first $\binom{v}{k} - \binom{v}{t}$ columns to be $B_1, \ldots, B_{\binom{v}{k}-\binom{v}{t}}$ in lexicographical ordering and its last $\binom{v}{t}$ columns to be the remaining elements of $P_k(X)$ in lexicographical ordering as well.

60.27 Remark In [1290] a more general method for constructing a triangular basis for the trades based on the concept of *starting blocks* is given.

60.28 Example If $v = 6,\ k = 3$, and $t = 2$, then $B_1 = 123,\ B_2 = 124,\ B_3 = 125,\ B_4 = 134,\ B_5 = 135,\ C_1 = 654,\ C_2 = 635,\ C_3 = 436,\ C_4 = 265$, and $C_5 = 246$. Then the 5 minimal trades that form the triangular basis for T(2,3,6) trades are given on the left below. In vector notation, these 5 trades have the triangular representation with respect to $\bar{W}_{23}(7)$ given on the right ("+" stands for +1,"−" stands for −1, and "blank" stands for 0).

Trades

$\{123, 145, 246, 356\},\ \{124, 135, 236, 456\}$
$\{124, 135, 256, 346\},\ \{125, 134, 246, 356\}$
$\{125, 136, 246, 345\},\ \{126, 135, 245, 346\}$
$\{134, 156, 235, 246\},\ \{135, 146, 234, 256\}$
$\{135, 146, 236, 245\},\ \{136, 145, 235, 246\}$

Blocks	Basis for Trades					
123	+					
124	−	+				
125		−	+			
134		−		+		
135	−	+	−	−	+	
126			−			
136			+			−
145	+					−
146				−	+	
156				+		
234				−		
235				+	−	
236	−				+	
245			−		+	
246	+	−	+	+	−	
256		+		−		
345			+			
346		+	−			
356	+	−				
456	−					

60.5 Applications of Trades

60.29 The *support* of a block design is the set of all distinct blocks of the design. The cardinality of the support is referred to as the *support size* of the design.

60.30 Remark Trades can be used to add or increase the frequencies of desirable blocks or to eliminate or decrease the frequencies of undesirable blocks from the support of a block design in general and t-designs in particular. Indeed, the concept and the theory of trade off evolved in this context for statistical applications of judiciously arranged block designs [825]. Among many possibilities two scenarios are considered here.

60.31 Remark Suppose the support of a t-design contains n undesirable blocks and the intention is to remove them completely or to reduce their frequencies in the design. If there is a trade $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2\}$ such that the blocks in T_1 are in the support and T_1 contains the undesirable blocks, then T_1 can be removed and be replaced by T_2. Often, additional blocks from the support are needed to form a leg T_1 of a trade.

60.32 Example Suppose that the blocks 124, 235, and 156 are undesirable blocks in the 2-design $D = \{124, 235, 346, 457, 156, 267, 137\}$. Based on Theorem 60.9, there is no trade with volume 3. So, by adding the block 235 to these 3 blocks, a trade $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2\}$ can be formed with $\mathrm{T}_1 = \{124, 235, 346, 156\}$ and $\mathrm{T}_2 = \{125, 356, 234, 146\}$. Now remove the blocks in T_1 from the support of the design D and add the blocks in T_2 to the support to obtain a new 2-design without the 3 undesirable blocks. In this case, the total number of blocks remains 7. This cannot be guaranteed in all cases.

60.33 Example Suppose it is desired to build a 2-design based on $v = 8$ and $k = 3$ without blocks 123 and 247. Based on $v = 8$ and $k = 3$, the minimum number of blocks needed to form a 2-design is 56. One possibility is to take the unreduced 2-design. At least 112 blocks are needed to form a 2-design without these two blocks. One way to do this is to take two copies of the unreduced design and do the following trade off. Remove T_1 and replace it by T_2 where $\{\mathrm{T}_1, \mathrm{T}_2\}$ is the following trade: $\mathrm{T}_1 = \{123, 123, 247, 247, 145, 146, 357, 367\}$, $\mathrm{T}_2 = \{124, 124, 237, 237, 135, 136, 457, 467\}$. The final design has 112 blocks with 54 distinct blocks in its support.

60.34 Theorem Let F be a frequency vector of a t-design based on v and k, and let T be a $\mathrm{T}(t, k, v)$ trade. Then for all positive integers m and n, $mF + n\mathrm{T}$ is a t-design if and only if $mF + n\mathrm{T} > 0$.

60.35 Remark If F is a t-design, then any t-design with the same set of parameters with F can be written in the form $F + \mathrm{T}$ for some trade T. Therefore, in order to search for all t-designs with the same parameters as F, it suffices to investigate the trade.

60.36 Theorem If F_1 and F_2 are two different t-designs based on the same set of parameters, then $F_2 - F_1 = \mathrm{T}$ is a trade. Consequently, all nonisomorphic t-designs with all possible supports and support sizes can be constructed by trades via $F + \mathrm{T}$ for a given t-design F and the set of trades.

60.37 Example If $v = 8$, $k = 3$, and $k = 2$, then there is no reduced 2-design. However, trades are used [825] to show that 2-designs with support size b^* can be constructed if and only if $22 \leq b^* \leq 56$.

60.38 A *signed t-design* based on $P_k(X)$ is a $\binom{v}{k}$ column vector S of integers (negative integers are allowed) such that $W_{tk}S = \lambda J$ for some positive integer λ.

60.39 Theorem There is at least one signed design for given t, k, v, with $0 < t \leq k \leq v$ and feasible λ. Some of these signed designs can be converted to t-designs by adding trades.

60.40 Remark There exists a very simple algorithm to produce signed designs [1290]. Since some of these signed designs can be converted to t-designs by augmentation of trades, trades form a powerful tool for constructing t-designs.

60.41 Table A signed design S and a trade T that produce a 2-design $S + \mathrm{T}$ for $v = 6$ and $k = 3$ is given on the right.

Block	S	T	S+T
123	0	+1	1
124	0	0	0
125	0	+1	1
134	0	0	0
135	0	0	0
126	+2	−2	0
136	+2	−1	1
145	+3	−2	1
146	−1	2	1
156	−1	+1	0
234	+2	−1	1
235	+2	−2	0
236	−2	+2	0
245	−1	+1	0
246	+1	0	1
256	+1	0	1
345	−1	+2	1
346	+1	−1	0
356	+1	0	1
456	+1	−1	0

60.6 A Generalization: N-Legged Trades

60.42 An *N-legged* trade, denoted by $\mathrm{T}[N](t, k, v)$ trade is a set $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2, \cdots, \mathrm{T}_N\}$ such that for $i \neq j$, $\{\mathrm{T}_i, \mathrm{T}_j\}$ is a $\mathrm{T}(t, k, v)$ trade.

60.43 Example A T[3](2,3,7). $\mathrm{T}_1 = \{123, 167, 247, 256, 346, 357\}$, $\mathrm{T}_2 = \{127, 136, 235, 246, 347, 567\}$, and $\mathrm{T}_3 = \{126, 137, 234, 257, 356, 467\}$.

60.44 Example A T[4](2,3,8).
$\mathrm{T}_1 = \{123, 145, 167, 248, 257, 346, 378, 568\}$, $\mathrm{T}_2 = \{124, 136, 157, 237, 258, 348, 456, 678\}$,
$\mathrm{T}_3 = \{125, 137, 146, 234, 278, 368, 458, 567\}$, $\mathrm{T}_4 = \{127, 134, 156, 238, 245, 367, 468, 578\}$.

60.45 Theorem Let G be a $\mathrm{T}[N](t_1, k_1, v_1)$ on $X_1 = \{a_1, a_2, \cdots, a_{v_1}\}$ and H be a $\mathrm{T}[N](t_2, k_2, v_2)$ on $X_2 = \{b_1, b_2, \cdots, b_{v_2}\}$ with $X_1 \cap X_2 = \phi$. By compounding G and H, a $\mathrm{T}[N](t, k, v)$ trade with $t = t_1 + t_2 + 1$, $k = k_1 + k_2$, $v = v_1 + v_2$ can be produced.

60.46 Remark If G_i is a leg in G and H_j is a leg in H, then $G_i|H_j$ represents a collection of blocks by enlarging each block in G_i with each and all blocks in H_j. Form an $N \times N$ array in the form of a latin square with entries $H_1, H_2, \cdots, H_N$ as given on the left. The N legs of the trade are given on the right.

$$\begin{array}{ll} H_1\ H_2 \cdots H_N & \{G_1|H_1,\ G_2|H_2,\ \cdots,\ G_N|H_N\} \\ H_2\ H_3 \cdots N_1 & \{G_1|H_2,\ G_2|H_3,\ \cdots,\ G_N|H_1\ \} \\ \quad\vdots & \quad\vdots \\ H_N\ H_1 \cdots H_{N-1} & \{G_1|H_N,\ G_2|H_1,\ \cdots,\ G_N|H_{N-1}\}. \end{array}$$

60.47 Example $G = \{\{45, 67\}, \{46, 57\}, \{47, 56\}$ is a $\mathrm{T}[3](1, 2, 4)$ trade on $X_1 = \{4, 5, 6, 7\}$ and $H = \{\{1\}, \{2\}, \{3\}\}$ is a T[3](0,1,3) trade on $X_2 = \{1, 2, 3\}$. Then $\{\mathrm{T}_1, \mathrm{T}_2, \mathrm{T}_3\}$ is a $\mathrm{T}[3](2, 3, 7)$ trade constructed by compounding G and H where $\mathrm{T}_1 = \{451, 671, 462, 572, 473, 563\}$, $\mathrm{T}_2 = \{452, 672, 463, 573, 471, 471\}$, $\mathrm{T}_3 = \{453, 673, 461, 571, 472, 562\}$.

See Also

§II.4	t-designs and large sets.
[273]	Combinatorial trades: a survey of recent results.
[1071]	The theory of trade-off for t-designs.
[1290]	On trades: an update.

References Cited: [273, 825, 940, 952, 954, 1071, 1129, 1130, 1159, 1288, 1290]

61 Turán Systems

Miklós Ruszinkó

61.1 Definitions and Equivalent Formulations

61.1 A *Turán* (n,k,r)*-system* $(n \geq k \geq r)$ is a collection of r-element blocks of an n element set X_n such that every k element subset of X_n contains at least one of the blocks.

61.2 The *Turán number* $T(n,k,r)$ is the minimum number of blocks in a Turán (n,k,r)-system [2077].

61.3 Example The complements of the lines of the Fano plane form a Turán $(7,5,4)$-system, $T(7,5,4) = 7$.

61.4 Remarks If $\mathrm{ex}_r(n, K_r(k))$ [845] is the maximum size of a collection of r-blocks in X_n that does not contain all $\binom{k}{r}$ blocks of some k element subset of X_n and $C(n,m,p)$ is the covering number, then

1. $T(n,k,r) = \binom{n}{r} - \mathrm{ex}_r(n, K_r(k))$;
2. $C(n,m,p) = T(n, n-p, n-m)$; and
3. $T(n,k,r) \geq \binom{n}{r}\binom{k}{r}^{-1}$. Equality holds if and only if there exists a Steiner system $S(n-k, n-r, n)$.

61.2 Recursive Bounds

61.5 Proposition (Schönheim; Katona, Nemetz, Simonovits) $T(n,k,r) \geq \left\lceil \frac{n}{n-r} T(n-1,k,r) \right\rceil$

61.6 Define $t(k,r) = \lim_{n\to\infty} T(n,k,r)\binom{n}{r}^{-1}$.

61.7 Proposition $t(k,r)$ always exists and $T(n,k,r) \leq \binom{n}{r} t(k,r)$.

61.8 Remark The values $t(k,r)$ for $k > r \geq 3$ are not known.

61.9 Proposition $T(n,k,r) \leq T(n-1,k,r) + T(n-1,k-1,r-1)$.

61.10 Corollary $t(k,r) \leq t(k-1,r-1)$.

61.11 Proposition $T\left(\sum_{i=1}^{\ell} n_i, \sum_{i=1}^{\ell} k_i + 1, r\right) \leq \sum_{i=1}^{\ell} T(n_i, k_i+1, r)$.

61.3 General Bounds

61.12 Theorem (de Caen) $T(n,k,r) \geq \frac{(n-k+1)}{(n-r+1)}\binom{n}{r}\binom{k-1}{r-1}^{-1}$.

61.13 Remark If $n = k^c$, c and r are fixed constants, then the magnitude of $T(k^c,k,r)$ is known. With $\ell = \left\lfloor \frac{k-1}{r-1} \right\rfloor$, $k_i = r-1$, $\forall i$, Proposition 61.11 yields $T(k^c,k,r) \leq \ell(r!)^{-1}\left(k^c \ell^{-1}\right)^r$ and by Theorem 61.12, $T(k^c,k,r) \geq (1+o(1))kr^{-1}(k^{c-1})^r$, that is, $T(k^c,k,r) = \Theta\left(k^{(c-1)r+1}\right)$. Theorem 61.12 also yields the following corollary.

61.14 Corollary $t(k,r) \geq \binom{k-1}{r-1}^{-1}$, in particular $t(r+1,r) \geq r^{-1}$.

61.15 Theorem (Kim, Roush; Frankl, Rödl; Sidorenko) $t(r+1,r) \leq (1/2 + o(1))r^{-1}\log r$.

61.16 Conjecture (de Caen) $\lim_{r\to\infty} r \cdot t(r+1,r) = \infty$.

61.4 The Case $r = 2$

61.17 Construction To get a Turán $(n, k+1, 2)$-system, divide X_n into into k nearly equal (of size m and $m+1$, resp.) groups and a pair of elements is a block if they belong to the same group.

61.18 Theorem (Turán) Construction 61.17 is optimal; that is, $T(n, k+1, 2) = nm - \binom{m}{2}k$ if $m \leq \frac{n}{k} \leq m+1$, and it is unique.

61.5 The Case $r = 3$

61.19 Construction To get a Turán $(n, 4, 3)$-system, divide X_n into 3 almost equal parts A_0, A_1, A_2 and take all triples $\{x, y, z\}$ with $x, y \in A_i$, $z \in A_i \cup A_{i+1 \pmod 3}$. This gives

$$T(n,4,3) \leq \begin{cases} m(m-1)(2m-1) & \text{if} \quad n = 3m \\ m^2(2m-1) & \text{if} \quad n = 3m+1 \\ m^2(2m+1) & \text{if} \quad n = 3m+1 \end{cases} \tag{61.1}$$

61.20 Conjecture (Turán) Equality holds in Equation (61.1).

61.21 Remarks Equality has been shown to hold in Equation (61.1) for $n \leq 13$. However, even if Conjecture 61.20 is true, Construction 61.19 is not unique in reaching this optimum.

61.22 Construction (Turán) To get a Turán $(n, 5, 3)$-system, divide X_n into 2 almost equal parts and take all triples within each group. This gives

$$T(n,5,3) \leq \binom{\lceil n/2 \rceil}{3} + \binom{\lfloor n/2 \rfloor}{3}.$$

61.23 Construction (Turán) For $k \geq 6$ the best known Turán $(n, k, 3)$-systems can be constructed as unions of $(u, 5, 3)$-, $(v, 4, 3)$-, and $(w, 3, 3)$-systems where the sums of the us, vs, and ws (with multiplicities) is n. In particular,

$$T(n, k+1, 3) \leq \frac{1}{2}\sum_{i=0}^{k-1} \binom{\lfloor (2n+i)/k \rfloor}{3}.$$

61.24 Remarks It has been shown that Construction 61.22 is not optimal for $n \geq 9$ odd and that Construction 61.23 is not optimal for those n where $2n/k$ is not integral. However, Constructions 61.22 and 61.23 seem to capture the magnitude correctly (if the following conjectures are true).

61.25 Conjecture (Turán) If $m = 2n/k$ is an integer then $T(km/2, k+1, 3) = \frac{k}{2}\binom{m}{3}$.

61.26 Conjecture (Turán) Asymptotically Conjecture 61.25 yields $t(k+1, 3) = (2k^{-1})^2$.

61.27 Theorem (Chung, Lu) The best known lower bound is $t(4,3) \geq (9 - \sqrt{17})/12 \approx 0.406$.

61.28 Table [1910] The values of $T(n, 5, 3)$, for $6 \le n \le 13$.

n	6	7	8	9	10	11	12	13
$T(n,5,3)$	2	5	8	12	20	29	40	52

61.6 The Case $r = 4$

61.29 Construction (Giraud; de Caen, Kreher, Wiseman) To get a Turán $(n, 2r+1, 2r)$-system, take an $(\lfloor n/2 \rfloor \times \lceil n/2 \rceil)$ matrix whose $x_{i,j} = 0, 1$ entries are chosen independently with $\mathbf{Prob}(x_{i,j} = 0) = \mathbf{Prob}(x_{i,j} = 1) = 1/2$. The n elements are the lines (rows and columns) of the matrix. $2r$ lines form a block if all of them are rows, or all of them are columns, or in the induced submatrix, the number of rows and the number of columns and the sum of the entries is even. The expected number of blocks is

$$\binom{\lfloor n/2 \rfloor}{2r} + \binom{\lceil n/2 \rceil}{2r} + \frac{1}{2}\sum_{i=1}^{r-1} \binom{\lfloor n/2 \rfloor}{2i}\binom{\lceil n/2 \rceil}{2(r-i)}.$$

61.30 Corollary $T(n, 2r+1, 2r) \le \left(\frac{1}{2^{2r}} + \frac{1}{4} + O\left(\frac{1}{n}\right)\right)\binom{n}{2r}$.

61.31 Remarks

1. Construction 61.29 gives the best known bounds for $t(5, 4)$ and $t(7, 6)$.
2. Construction 61.29 can be improved for $r \ge 4$.

61.32 Conjecture For $r = 2$ Construction 61.29 is asymptotically optimal; that is, $t(5, 4) = 5/16$.

61.33 Table [1910] The values of $T(n, 7, 4)$, for $8 \le n \le 16$.

n	8	9	10	11	12	13	13	15	16
$T(n,7,4)$	2	4	10	≤ 17	≤ 26	≤ 40	≤ 58	≤ 81	≤ 108

61.34 Remark Several generalizations of Turán systems have been extensively investigated. For example, a Turán $(n, k, r, \ge s)$-system is a collection of r-element blocks of X_n such that every k element subset of X_n contains at least s of the blocks.

See Also

§II.5	The connection to Steiner systems is given in Remark 61.4(3).
§VI.10	Turán systems are used to construct covering arrays.
§VI.11	The connection to coverings is given in Remark 61.4(2).
§VI.32	Turán systems are related to lotto designs.
§VI.56	Turán systems are related to superimposed codes.
[1910]	A comprehensive survey on Turán systems, contains much of the information given in this chapter.
[845]	A comprehensive survey on Turán type problems.

References Cited: [845, 1910, 2077]

62 Tuscan Squares

Wensong Chu
Solomon W. Golomb
Hong-Yeop Song

62.1 Definitions and Examples

62.1 An $r \times n$ *tuscan-k rectangle* has r rows and n columns such that

1. each row is a permutation of the n symbols and
2. for any two distinct symbols a and b and for each m from 1 to k, there is at most one row in which b is m steps to the right of a.

An $r \times n$ *circular* tuscan-k rectangle is a tuscan-k rectangle with r circular rows containing n symbols.

A tuscan-1 rectangle is a *tuscan* rectangle and an $r \times n$ tuscan-$(n-1)$ rectangle is a *florentine* rectangle. When $r = n$, they are *tuscan squares* and *florentine squares.*

62.2 A tuscan square is in *standard form* when the top row and the left-most column contain the symbols in natural order.

A *roman square* is both tuscan and latin and is also known as a *row complete latin square.*

A *vatican square* is a florentine square that is also latin.

62.3 **Remark** If there exists an $r \times n$ tuscan rectangle, then $r \le n$. If there exists an $r \times n$ circular tuscan rectangle, then $r \le n - 1$.

62.4 **Examples** Vatican squares of orders 2, 4, and 6. A tuscan square of order 7 that is not tuscan-2. A tuscan-2 of order 8 that is not tuscan-3.

1 2	1 2 4 3	6 2 1 4 5 3	6 1 5 2 4 3 7	1 2 3 4 5 6 7 8
2 1	2 3 1 4	1 3 2 5 6 4	2 6 3 5 4 7 1	2 1 6 8 7 3 5 4
	3 4 2 1	2 4 3 6 1 5	5 7 2 3 1 4 6	3 2 7 1 8 4 6 5
	4 1 3 2	3 5 4 1 2 6	4 2 5 1 6 7 3	4 1 7 5 3 8 6 2
		4 6 5 2 3 1	3 6 2 1 7 4 5	5 8 1 4 7 2 6 3
		5 1 6 3 4 2	1 3 2 7 5 6 4	6 1 5 2 4 8 3 7
			7 6 5 3 4 1 2	7 4 2 8 5 1 3 6
				8 2 5 7 6 4 3 1

62.5 **Examples** [509, 1936, 1937] A 4×8 circular florentine rectangle, a 6×7 circular tuscan-3 rectangle, and a 4×27 circular florentine array.

0	3	4	6	7	1	5	2
1	0	5	7	4	2	6	3
2	1	6	4	5	3	7	0
3	2	7	5	6	0	4	1

0	1	2	3	4	5	6	7
0	3	6	1	4	7	2	5
0	2	7	5	4	6	3	1
0	6	5	7	4	2	1	3
0	7	1	6	4	3	5	2
0	5	3	2	4	1	7	6

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	4	10	1	19	21	11	14	2	22	20	12	3	9	18	24	15	7	5	25	13	16	6	8	26	17	23
0	15	1	13	2	16	3	19	4	18	5	17	20	6	21	7	10	22	9	23	8	24	11	25	14	26	12
0	20	16	4	14	25	8	12	26	24	21	5	9	17	10	18	22	6	3	1	15	19	2	13	23	11	7

62.6 Remark Adjoining a column of asterisks to the left of an $n \times n$ tuscan square makes it an $n \times (n+1)$ circular tuscan rectangle. Rotating the rows so that another symbol fills the left-most column and then deleting it, gives a new $n \times n$ tuscan square. This is the *add-asterisk transformation*.

62.7 Two tuscan-k rectangles are *isomorphic* if their standard forms differ by

1. a substitution of symbols,
2. permuting the rows, and
3. taking the reverse order of symbols in every row.

62.8 Examples Two nonisomorphic 6×7 florentine rectangles and two nonisomorphic 8×9 florentine rectangles [1935].

1	2	3	4	5	6	7
2	5	7	4	3	1	6
3	7	1	4	6	5	2
5	3	6	4	7	2	1
6	1	5	4	2	7	3
7	6	2	4	1	3	5

1	2	3	4	5	6	7
2	6	1	4	7	5	3
3	1	7	4	6	2	5
5	7	6	4	1	3	2
6	5	2	4	3	7	1
7	3	5	4	2	1	6

1	2	3	4	5	6	7	8	9
2	1	7	9	5	8	3	6	4
3	7	2	8	5	4	1	9	6
4	9	8	1	5	7	6	3	2
6	8	4	7	5	2	9	1	3
7	3	1	6	5	9	2	4	8
8	6	9	3	5	1	4	2	7
9	4	6	2	5	3	8	7	1

1	2	3	4	5	6	7	8	9
2	9	6	1	5	8	3	7	4
3	6	9	7	5	4	2	1	8
4	1	7	9	5	3	8	6	2
6	8	4	3	5	1	9	2	7
7	3	2	8	5	9	1	4	6
8	7	1	6	5	2	4	9	3
9	4	8	2	5	7	6	3	1

62.2 Constructions and Related Combinatorial Objects

▷ Polygonal Path Constructions

62.9 A *tuscan-k polygonal path* of order n is a permutation $(X_1, X_2, \cdots, X_n)$ of $\mathbb{Z}_n$ such that $X_{s+d} - X_s \not\equiv X_{t+d} - X_t \pmod{n}$ for every s and t with $1 \le s < t < t+d \le n$ and for every d with $1 \le d \le k$. A tuscan-k polygonal path is *symmetric* if for $1 \le i \le n$, $\frac{n}{2} + X_i \equiv X_{n+1-i} \pmod{n}$.

62.10 A *circular tuscan-k polygonal path* of order n is a permutation $(X_1, X_2, \cdots, X_n, \infty)$ over $\mathbb{Z}_n \cup \{\infty\}$ such that $X_{s+d} - X_s \not\equiv X_{t+d} - X_t \pmod{n}$ for every $s \ne t$ and for every d with $1 \le d \le k$, where the subscripts are taken modulo $n+1$.

62.11 Theorems

1. Let $(X_1, X_2, \cdots, X_n)$ be a tuscan-k polygonal path of order n and let the ith row of square S be $(X_1+i-1, X_2+i-1, \cdots, X_n+i-1) \pmod{n}$ for $1 \le i \le n$. Then S is a tuscan-k square of order n.
2. Let $(X_1, X_2, \cdots, X_n, \infty)$ be a circular tuscan-k polygonal path of order n and let the ith row of square S be $(X_1 + i - 1, X_2 + i - 1, \cdots, X_n + i - 1, \infty) \pmod{n}$ for $1 \le i \le n$. Then S is an $n \times (n+1)$ circular tuscan-k square of order n.
3. If $(X_1, X_2, \cdots, X_n)$ is a symmetric tuscan-2 polygonal path of order n, then $(X_1, X_2, \cdots, X_n, \infty)$ is a circular tuscan-2 polygonal path of order n [927].

62.12 Example The vatican square of order 6 in Example 62.4 is constructed from a symmetric tuscan-5 polygonal path $(6, 2, 1, 4, 5, 3)$. The permutation $(6, 2, 1, 4, 5, 3, \infty)$ is a circular tuscan-5 polygonal path of order 5.

62.13 Construction Let $X = (X_1, X_2, \cdots, X_n)$ be a sequence over $\mathbb{Z}_n$.

1. For every even n, define $X_i = \frac{i}{2} \pmod{n}$ for even i and $X_i \equiv -\frac{i-1}{2} \pmod{n}$ for odd i. Then X is a tuscan-1 polygonal path of order n. It is the well-known "zig-zag" construction.

2. For $n = 2^N$, define $X_i = 1 + \frac{i(i-1)}{2} \pmod{n}$. Then X is a tuscan-1 polygonal path of order n.
3. For a prime $p = n + 1$ with 2 as a primitive root, define $X_i = 2^{i-1} \pmod{p}$. Then X is a tuscan-1 polygonal path of order $p - 1$.
4. For a prime $p = n + 1$ with α as a primitive root, define X_i as the root of $\alpha^{X_i} = i \pmod{p}$. Then X is a tuscan-$(n-1)$ polygonal path of order n. And $(X_1, X_2, \cdots, X_n, \infty)$ is a circular tuscan-$(n-1)$ polygonal path of order n.

62.14 Examples $(10, 1, 9, 2, 8, 3, 7, 4, 6, 5)$ is a tuscan-1 polygonal path from the "zig-zag" construction. $(1, 2, 4, 7, 3, 8, 6, 5)$ is a tuscan-1 polygonal path of order 8 from Construction 62.13(2). The tuscan square of order 4 in Example 62.4 uses Construction 62.13(3), which happens to be a Vatican square. The tuscan square of order 6 in Example 62.4 uses Construction 62.13(4).

62.15 Remarks

1. Polygonal paths only exist for n even and the resulting tuscan squares are also latin.
2. Construction 62.13(3) is a special case of Welch constructions for Costas arrays and Construction 62.13(4) is its log version. (See §VI.9.)
3. Construction 62.13(4) is the only known construction for Vatican squares.
4. Symmetric tuscan-2 squares of order n exist for all even n with $8 \le n \le 50$ [927].

▷ (n, k)-Sequences

62.16 Let $P = (a_1, a_2, \cdots, a_{kn})$ be a permutation over $\mathbb{Z}_{kn}$. Then (a_i, a_j) is a *comparable pair* if $\lfloor \frac{a_i}{n} \rfloor = \lfloor \frac{a_j}{n} \rfloor$. P is an (n, k)-*sequence* if $a_{s+d} - a_s \not\equiv a_{t+d} - a_t \pmod{n}$ whenever (a_s, a_{s+d}) and (a_t, a_{t+d}) are comparable pairs for every s, t, and d with $1 \le s < t < t + d \le kn$.

62.17 Example $(0, 3, 4, 6, 7, 1, 5, 2)$ is a $(4, 2)$-sequence. This can be verified by calculating the following difference triangle. According to the definition of comparable pairs, any pair of elements from $\{0, 1, 2, 3\}$ is a comparable pair and so is any pair of elements from $\{4, 5, 6, 7\}$.

0	3	4	6	7	1	5	2
3	*	2	1	*	*	*	
*	*	3	*	2	1		
*	*	*	3	*			
*	2	1	*				
1	*	*					
*	3						
2							

62.18 Construction From the $(4, 2)$-sequence in Example 62.17, one can construct a 4×8 array of 8 symbols in which the top row is $a_1, a_2, \cdots, a_8$ and the columns are cyclic shifts of either $0, 1, 2, 3$ or $4, 5, 6, 7$. The resulting 4×8 circular tuscan rectangle is shown in Examples 62.5.

62.19 Theorem [1937] If there exists an (n, k)-sequence, there exists an $n \times kn$ florentine rectangle. There also exists an $n \times (kn + 1)$ florentine rectangle by adding a column of asterisks to the left of the $n \times kn$ florentine rectangle.

62.20 Construction [1937] Let α be a primitive root modulo $p = kn + 1 > 2$ where p is a prime. For $i = 1, 2, \cdots, kn$, let $ind_\alpha(i)$ be the index of i with respect to α; namely,

$ind_\alpha(i) = j$ if and only if $i = \alpha^j$ for some $j = 0, 1, \cdots, kn-1$. Let q_i and r_i be integers such that $ind_\alpha(i) = kq_i + r_i$, where $0 \le r_i \le k-1$. Let $X_i = q_i + nr_i$ for $i = 1, 2, \cdots, kn$. Then $(X_1, X_2, \cdots, X_{kn})$ is an (n,k)-sequence.

62.21 Example Let $p = 13 = 4 \times 3 + 1$ and $\alpha = 2$. Then $(0, 4, 5, 8, 3, 9, 11, 1, 10, 7, 6, 2)$ is a $(4, 3)$-sequence.

62.22 Table The number $w_2(n)$ of essentially distinct $(n, 2)$-sequences. Here, $\star$ corresponds to the sequence from Construction 62.20.

n	$w_2(n)$	$(n,2)$-sequences
1	1	01*
2	1	0231*
3	2	035124, 013254*
4	2	01465372, 04217563
5	5	0159738246, 0513476928, 0589173246, 0596184237, 0514367928*
6	4	026B831A4957, 06218A7B4593, 061BA8452793, 0621A8B74593*
7	8	017B24D5CA3698, 017B64C3D825A9, 07148AB6539D2C, 071CA524D986B3 07A124958DC63B, 07B1395A48D62C, 0791AB8365D42C, 079A14D28C653B
8	6	0182AFD379BE6C54, 018AD3B26F79EC54, 018EB3D2697FAC54 089F27E51A36BDC4, 089F61E37A52BDC4, 0182E9B37FDA6C54*
9	1	$(2n+1 = 19$ is prime$)^\star$
10	0	-
11	1	$(2n+1 = 23$ is prime$)^\star$
12	0	-
13	0	-
14	≥ 1	$(2n+1 = 29$ is prime$)^\star$
15	≥ 1	$(2n+1 = 31$ is prime$)^\star$
16	?	?

▷ Other Constructions

62.23 Construction

1. If p is the smallest prime factor of n, then $C(x, y) \equiv xy \pmod n$ for $x = 1, 2, \cdots, p-1$ and $y = 0, 1, \cdots, n-1$ constructs a $(p-1) \times n$ circular florentine rectangle.
2. If a group of order n is sequenceable, there exists a tuscan square of order n whose transpose is also tuscan. (See §VI.6.)
3. Let $\mathbb{F}_q$ be the finite field with $q = p^r$. Let $\mathbb{F}_q^\star$ be the multiplicative group of $\mathbb{F}_q$, and $\mathbb{F}_q^k = \{\alpha^k \mid \alpha \in \mathbb{F}_q^\star\}$. Let s with $0 < s < r$ be an integer, and $d = gcd(p^s - 1, p^r - 1) = p^{gcd(s,r)} - 1$. Let $S = \mathbb{F}_q - \mathbb{F}_q^d$. For any $a \in S$ define $f_a(x) = x^{p^s} - ax$, and define $L_a = (f_a(\alpha^0), f_a(\alpha^1), \cdots, f_a(\alpha^{q-2}))$. Then $\{L_a \mid a \in S\}$ is a set of $1 + \frac{d-1}{d}(q-1)$ circular tuscan-l rows on $q-1$ elements of $\mathbb{F}_q^\star$, where $l = \frac{q-1}{d} - 1$ [509].

▷ Connections with Other Combinatorial Objects

62.24 Theorem

1. A tuscan square of order n is equivalent to a decomposition of the complete graph with n vertices into n hamiltonian directed paths [2033].

2. There exists a tuscan-$(n-1)$ polygonal path of order n if and only if there exists a singly periodic Costas array of order n [794]. (See §VI.9.)
3. An $n \times (n+1)$ circular tuscan-k rectangle induces k MOLS of order $n+1$ [794].
4. An $r \times n$ circular florentine rectangle induces r MOLS of order n [1935].
5. An $r \times n$ circular florentine array is equivalent to an $(n, r+1; 1)$ difference matrix over the cyclic group of order n [1935]. (See §VI.17.)
6. A pair of orthogonal latin squares cannot both be vatican [1935].

62.3 Existence and Enumeration

62.25 Theorems

1. If $n > 0$ and $n \neq 3, 5$, then there exists a tuscan square of order n [2033].
2. If n is even, there exists an $n \times n$ roman square (row complete latin square). (See Construction 62.13(1).)
3. For every odd composite n, there exists an $n \times n$ roman square [1095].
4. There does not exist a roman square of order 3, 5, or 7.
5. If p is a prime and either $p \equiv 7 \pmod{12}$ or $p \equiv 5 \pmod{24}$, there exists a tuscan-2 square of order $2p$ whose transpose is also a tuscan-2 square [89].
6. For any prime p and integers $r_2 > r_1 \geq 1$, there exists a $(2 + \frac{p^{r_1}-2}{p^{r_1}-1}(p^{r_1 r_2} - 1)) \times (p^{r_1 r_2} - 1)$ circular tuscan-l rectangle with $l = \frac{p^{r_1 r_2} - p^{r_1}}{p^{r_1}-1}$ [509].
7. A circular tuscan-$(n-1)$ polygonal path of order n exists if and only if $n+1$ is an odd prime [794].
8. If n is even, there does not exist a $2 \times n$ circular florentine rectangle [374].

62.26 Table [927, 930] The number of standard form tuscan-k squares of order n.

$k \backslash n$	2	3	4	5	6	7	8	9	10	11	12	13
1	1	0	1	0	736	466144	$\geq 3 \cdot 10^7$	$\geq 3 \cdot 10^7$	≥ 72	≥ 1	≥ 964	≥ 1
2		0	1	0	1	0	6	?	≥ 2	?	≥ 2	?
3			1	0	1	0	0	0	≥ 1	?	≥ 1	?
4				0	1	0	0	0	≥ 1	?	≥ 1	?
5					1	0	0	0	≥ 1	?	≥ 1	?
6						0	0	0	≥ 1	?	≥ 1	?
7							0	0	≥ 1	?	≥ 1	?
8								0	1	?	≥ 1	?
9									1	0	≥ 1	?
10										0	≥ 1	?
11											≥ 1	?
12												?

62.27 Let $F(n)$ denote the maximum integer F such that there exists an $F \times n$ florentine rectangle. Let $F_c(n)$ denote the maximum integer F_c such that an $F_c \times n$ circular florentine rectangle exists.

62.28 Table Possible values of $F_c(n)$ and $F(n)$ [1935, 1937].

n	$F_c(n)$	n	$F_c(n)$
1	1	21	$5\cdots\cdots19$
3	2	23	22
5	4	25	$4\cdots\cdots24$
7	6	27	$4\cdots\cdots26$
9	2	29	28
11	10	31	30
13	12	33	$3\cdots\cdots30$
15	4	35	$4\cdots\cdots33$
17	16	37	36
19	18	39	$3\cdots\cdots38$

n	$F(n)$	n	$F(n)$	n	$F(n)$
1	1	11	10	21	$7\cdots\cdots21$
2	2	12	12	22	22
3	2	13	12, 13	23	22, 23
4	4	14	$7\cdots\cdots14$	24	$6\cdots\cdots24$
5	4	15	$7\cdots\cdots15$	25	$6\cdots\cdots25$
6	6	16	16	26	$6\cdots\cdots26$
7	6	17	16, 17	27	$6\cdots\cdots27$
8	7	18	18	28	28
9	8	19	18, 19	29	28, 29
10	10	20	$6\cdots\cdots20$	30	30

62.4 Applications of Tuscan Squares

62.29 Remark In a sequence of visual impressions, one flash card may have some effect on the impression given by the next. This bias can be cancelled by using n sequences corresponding to the rows of an $n \times n$ tuscan-1 square [374].

62.30 Remark In frequency-hopped multiple-access communication systems, any two users should avoid hopping simultaneously to the same carrier frequency, an event termed a *hit*. Assigning a row of an $r \times n$ circular florentine rectangle to each user as a frequency hopping sequence minimizes the number of hits between any two users [1935, 1937].

See Also

§VI.9	A detailed description of Costas arrays.
§VI.6	A detailed description of sequenceable groups.
[1448]	A textbook on finite fields with a chapter contributing to *permutation polynomials*, which are used in Construction 62.23(3).

References Cited: [89, 374, 509, 794, 927, 930, 1095, 1448, 1935, 1936, 1937, 2033]

63 t-Wise Balanced Designs

Earl S. Kramer
Donald L. Kreher

63.1 Definitions

63.1 A *t-wise balanced design* (tBD) of type t-(v, K, λ) is a pair $(\mathbf{X}, \mathcal{B})$ where $\mathbf{X}$ is a v-element set of points and $\mathcal{B}$ is a collection of subsets of $\mathbf{X}$ (*blocks*) with the property that the size of every block is in the set K and every t-element subset of $\mathbf{X}$ is contained in exactly λ blocks.

63.2 If K is a set of positive integers strictly between t and v, then the tBD is *proper*. If $\mathcal{B}$ contains all k-subsets of $\mathbf{X}$ for some k, then $(\mathbf{X}, \mathcal{B})$ is a *trivial design*.

63.3 **Remark** While emphasis is generally placed on proper and nontrivial tBDs, improper tBDs are often required for minimal exact coverings and also trivial tBDs are convenient to include when listing general theorems.

63.4 A t-(v, K, λ) design is also denoted by $S_\lambda(t, K, v)$ or by $B_t[K, \lambda; v]$, when then one may write $v \in B_t(K, \lambda) = \{v : \text{there is a } t\text{BD of type } t\text{-}(v, K, \lambda)\}$. If $K = \{k\}$, so $|K| = 1$, then the tBD is a t-design. If $\lambda = 1$, the notation $S(t, K, v)$ is often used and the design is a *Steiner system*.

63.5 **Example** Let $\mathbf{X} = \{1, 2, \ldots, 12\}$ with base blocks {1 2 3 4 5 6}, {7 8 9 10 11 12}, {1 2 7 8}, {1 2 9 11}, {1 2 10 12}, {3 5 7 8}, {3 5 9 11}, {3 5 10 12}, {4 6 7 8}, {4 6 9 11} and {4 6 10 12}. Applying the automorphism (1 2 3 4 5)(7 8 9 10 11) yields $2 + 45 = 47$ blocks that form a 3-$(12, \{4, 6\}, 1)$ design. This tBD is not balanced for t=2 since some pairs appear four times while others appear five times.

63.6 A *graphical* (*bigraphical*) tBD is a tBD whose point set $\mathbf{X}$ is the edges of the complete graph $K_p(K_{m,n})$ and whose automorphism group is the symmetric group $S_p(S_m \times S_n)$ (see §VI.24).

63.7 **Remark** Although there are only finitely many graphical (bigraphical) Steiner tBDs for $t \geq 2$, these do provide nice presentations for such tBDs and t-designs. The Steiner cases for $t \geq 2$ are (1) graphical: $S(2, 3, 15)$, $S(2, \{3, 5\}, 15)$, $S(3, 4, 10)$, $S(4, \{5, 7\}, 15)$; (2) bigraphical: $S(2, 3, 9)$, $S(3, 4, 8)$, $S(3, 4, 16)$, $S(3, \{4, 6\}, 16)$, $S(5, \{6, 8\}, 16)$. See [500, 1117] and §VI.24 for details.

63.2 Elementary Properties

63.8 **Remark** By taking the derived incidence structure, Theorem 63.9 is immediate.

63.9 **Theorem** A t-(v, K, λ) design implies there exists a $(t-1)$-$(v-1, K-1, \lambda)$ design where $K - 1 = \{k_i - 1 : k_i \in K\}$.

63.10 **Remark** A t-design is always an s-design for $0 \leq s \leq t$, but a t-(v, K, λ) design is not necessarily a $(t-1)$-(v, K, λ) design. For example, there is a 13-(24,{14,15},11) (see [1334]) that is balanced for t=1, 2, 3, 4, 5, and 13, but is not balanced for $6 \leq t \leq 12$.

63.11 **Theorem** [1334] If $t \geq 2$, then there is a tBD that is not s-balanced for any $0 < s < t$.

63.12 **Example** Let $N_n = \{1, 2, \ldots, n\}$ and $\mathbf{X} = N_n \cup \{\infty\}$ for $t < n$. Let $\mathcal{B} = N_n \cup \{S \cup \{\infty\} : S \in \mathcal{P}_{t-1}(N_n)\}$, where $\mathcal{P}_{t-1}(N_n)$ is the set of all subsets of N_n of size $(t-1)$. Then $(\mathbf{X}, \mathcal{B})$ is a tBD that is not s-balanced for any $0 < s < t$.

63.13 **Remark** Under certain conditions a tBD does possess balance for other values of $0 < s < t$ (see [1244]).

63.14 **Theorem** If $(\mathbf{X}, \mathcal{B}_1 \cup \mathcal{B}_2)$ is a t-wise and a $(t-1)$-wise balanced design where the blocks in $\mathcal{B}_i$ have size $k_i, (i = 1, 2; k_1 \neq k_2)$, then each $(\mathbf{X}, \mathcal{B}_i), i = 1, 2$ is a $(t-1)$-design.

63.15 For $0 \leq s \leq t$ and with $t \leq k$ for all $k \in K$, define
$$\alpha(K, s) = \gcd\{(k-s)(k-s-1)\cdots(k-t+1) : k \in K\}.$$

63.16 **Theorem** [1334] If $v \in B_t(K, \lambda)$, then $\lambda(v-s)(v-s-1)\cdots(v-t+1) \equiv 0 \pmod{\alpha(K, s)}$, for $0 \leq s < t$.

63.17 **Remarks** The necessary conditions for tBDs given by Theorem 63.16 are not sufficient since such conditions are satisfied for the parameters 2-(45,{6,7},1), but such a tBD does not exist. However, the necessary conditions for PBDs are sufficient for large enough v [2151]. One would like to prove that the necessary conditions for a 3-

wise balanced design are sufficient if v is large enough (see [1060]). Hanani (see [1037, 1038, 1043]) pioneered the use of tBDs and gave several properties, listed in Theorem 63.18.

63.18 Theorems

1. $K \subset B_t(K, 1)$.
2. If $K' \subset K$, then $B_t(K', \lambda) \subset B_t(K, \lambda)$.
3. If λ' divides λ, then $B_t(K, \lambda') \subset B_t(K, \lambda)$.
4. $B_t(K, \lambda) \cap B_t(K, \lambda') \subset B_t(K, n\lambda + n'\lambda')$ where λ and λ' are any positive integers, and n and n' are any nonnegative integers.
5. If $v \in B_t(K', \lambda')$ and $K' \subset B_t(K, \lambda)$, then $v \in B_t(K, \lambda\lambda')$.

63.19 Remark There are several recursive results when $t = 3$ (see [1060] for references and discussion). One such result is Theorem 63.20.

63.20 Theorem If there exists an $S(3, K, g+u)$ with a subsystem $S(3, K, u)$, where u is even and $g \equiv u + 2 \pmod 6$, then there exists an $S(3, K \cup \{4, 6\}, 3g + u)$.

63.21 Theorem [1334] A nontrivial tBD with $t \geq 2$ and $\lambda = 1$ has $k \leq (v + t - 3)/2$ for all $k \in K$.

63.22 An *incomplete t-wise balanced design* (ItBD) of type t-(v, h, K, λ) is a triple $(X, H, \mathcal{B})$ where X is a v-element set of points, H is an h-element subset $H \subseteq X$ (the *hole*), and $\mathcal{B}$ is a collection of subsets of X (the *blocks*), such that every t-element subset of points is either contained in the hole or in exactly λ blocks, but not both.

63.23 Remarks An ItBD of type t-(v, h, K, λ) is equivalent to a tBD of type t-$(v, K \cup \{h\}, \lambda)$ having a block of size h that is repeated λ times. In particular, when $\lambda = 1$, a tBD of type t-(v, K, λ) is an ItBD of type t-$(v, h, K, 1)$ for any $h \in K$, provided of course that the tBD actually has a block of size h.

63.24 Theorem [1356] Let $(X, H, \mathcal{B})$ be a proper ItBD with $t \geq 2$. If $h = |H|$ is the size of the hole, then $h \leq (v - 1)/2$ when t is even, while $h \leq v/2$ when t is odd.

63.25 Remark Setting $\lambda = 1$, Theorem 63.26 is an immediate consequence of Theorem 63.24.

63.26 Theorem [1356] Given a proper tBD $(X, \mathcal{B})$ of type t-(v, K, λ) with a block of size $k \in K$, then $k \leq (v - 1)/2$ when t is even, while $k \leq v/2$ when t is odd.

63.27 Remark [1356] For every $t \geq 2$ and every $h \geq t + 1$, there exists an ItBD (with λ as a function of h and t) meeting the bounds of Theorem 63.24. Any ItBD meeting this bound must have $k = t + 1$ as its minimum block size.

63.28 Theorem [1357] If $(X, H, \mathcal{B})$ is a proper ItBD of type t-(v, h, K, λ) with $h \geq t \geq 2$ and $\min K = k \geq t + 1$, then

$$h \leq \frac{v + (k - t)(t - 2) - 1}{k - t + 1}.$$

63.29 Remark [53] The bound in Theorem 63.28 is sharp infinitely often for every t.

63.30 Remark Theorem 63.31 is an asymptotic result for $S(t, K, v)$s that permit blocks of size t.

63.31 Theorem [554] The number of nonisomorphic $S(t, K, v)$s is $v^{\binom{v}{t}/(t+1))(1+o(1))}$ for fixed $t \geq 2$.

63.3 H-Designs

63.32 An *H-design* $\mathrm{H}(m, g, k, t)$ is a set V of mg points with a partition into m *groups* each of size g. It is equipped with a set $\mathcal{B}$ of *blocks*, each of size k. Every block is *transverse* to the groups; that is, it meets every group in at most one point. Every transverse t-subset of V appears in exactly one block of $\mathcal{B}$.

63.33 Theorem [1613] For $m > 3, m \neq 5$, an $\mathrm{H}(m, g, 4, 3)$ exists if and only if mg is even and $g(m-1)(m-2) \equiv 0 \pmod 3$. An $\mathrm{H}(5, g, 4, 3)$ exists if g is divisible by 4 or 6.

63.34 Remark L. Ji has recently shown that an $\mathrm{H}(5, g, 4, 3)$ exists whenever g is even, $g \neq 2$, and $g \not\equiv 10, 26 \pmod{48}$.

63.4 Some Families of tBDs for t $\geq$ 3

63.35 Remarks Although there are no known infinite families of Steiner systems for $t \geq 4$, Wilson has constructed the family of designs with parameters $S(5, \{6, 8\}, 2^n)$ for all $n \geq 4$. From this family one can produce $S(5, \{6, 8, 2^{n-1}\}, 2^n)$, $S(4, \{5, 7\}, 2^n - 1)$, and $S(4, \{5, 7, 2^{n-1}-1\}, 2^n - 1)$ for all $n \geq 4$ (see [1334] for a discussion). In addition, Tonchev [2051] has constructed the infinite family $S(4, \{5, 6\}, 4^n + 1)$ for $n \geq 2$. Some of the following results may use trivial tBDs.

63.36 Theorem [1192] If $v \equiv 1, 2, 4, 5, 8, 10 \pmod{12}$ and $v \neq 13$, then $v \in B_3(\{4, 5\}, 1)$.

63.37 Theorem [1038] If v is even, then $v \in B_3(\{4, 6\}, 1)$.

63.38 Theorem [1193] If $v \equiv 0, 1, 2 \pmod 4$ and $v \notin \{9, 13\}$, then $v \in B_3(\{4, 5, 6\}, 1)$.

63.39 Theorem [1038, 1192] If $v \geq 4$, then $v \in B_3(\{4, 5, 6, 7, 9, 11, 13, 15, 19, 23, 27\}, 1)$.

63.40 Theorem [2170] If $v \geq 5$, then $v \in B_3(\{5, 6, \ldots, 40\} \setminus \{17, 21, 22, 25, 26\}, 1)$.

63.5 All Proper tBDs for t $\geq$ 3 with λ = 1 and v $\leq$ 16

63.41 Remark In [1341] the proper t-wise balanced designs t-$(v, K, 1)$ for $t \geq 3, \lambda = 1$, and $v \leq 16$ with at least two block sizes are characterized. While extensions of $S(3, 4, 16)$s are not examined there, all other possible extensions of $S(3, K, v)$s for $v \leq 16$ are determined. A particularly interesting extension is the $S(4, \{5, 6\}, 17)$ design. Table 63.42 summarizes the results from [1341].

63.42 Table The proper $S(t, K, v)$s for $t \geq 3$ and $v \leq 16$. For a given t and v, the number of blocks of each size k is listed. Also listed is the number of nonisomorphic proper $S(t, K, v)$ designs with the prescribed number of blocks of each size. For each entry, a reference number for a construction is given.

Con. #	t	v	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	Number
63.44	3	8	14					1
63.45	3	10	30					1
63.46	3	12	45		2			1
63.47	3	14	56		7			4
63.48	3	14	91					4
63.49	3	16	112				2	1932
63.49	3	16	126				1	66407
63.50	3	16	60		16			1

Con. #	t	v	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	Number
63.51	3	16	100		8			1
63.52	3	16	20	48				1
63.53	3	16	35	42				1
63.54	3	16	60	32				6
63.55	3	16	85	22				2
63.56	3	16	100	16				506
63.57	3	16	105	14				22
63.58	3	16	110	12				8
63.49	3	16	140					1054163
63.45	4	11		66				1
63.59	4	15		168		15		1
63.60	4	17		140	112			1
	4	17		476				?
63.45	5	12			132			1
63.59	5	16			448		30	1

63.43 Remark In the constructions to follow, a design of type $a^x b^y$ means there are x blocks of size a and y blocks of size b. A given subgroup H (G is the full automorphism group of the design) acts on the listed base blocks to generate the design. Any additional generators to produce G are mentioned, along with $|G|$.

63.44 Construction The $S(3,4,8)$ of type 4^{14}. $H = \langle(1\ 2\ 3\ 4\ 5\ 6\ 7)\rangle$. Base blocks: {1 2 4 8}, {3 5 6 7}. $G = \langle H,\ (2\ 3\ 6)(5\ 7\ 8)\rangle$ and $|G| = 1344$.

63.45 Construction The $S(3,4,10)$ of type 4^{30}; the $S(4,5,11)$ of type 5^{66}; the $S(5,6,12)$ of type 6^{132}. Let $X = \{1,2,3,...,9,a,b,c\}$ and $H = \langle(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ a\ b)\rangle$. To generate the $S(4,5,11)$ let H act on the base blocks: {1 2 3 4 6}, {1 2 3 7 a}, {1 2 3 8 9}, {1 2 4 5 8}, {1 2 4 7 9}, {1 2 6 8 a}. Taking the derived design through the point b produces the $S(3,4,10)$. To get the $S(5,6,12)$, add point c to each block of the $S(4,5,11)$ and then take the complement of each such block in X to get the needed $66+66=132$ blocks of size 6. The group for the $S(3,4,10)$ is $G = \langle(1\ 2\ 3\ 6\ 9\ 7\ 5\ 10\ 4\ 8),\ (2\ 7\ 6\ 5)(3\ 8\ 10\ 4)\rangle$ where $|G| = 1440$. The group for the $S(4,5,11)$ is $M_{11} = \langle H,\ (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ 10\ 8),\ (3\ 4\ 6)(5\ 9\ 10)(7\ 8\ 11)\rangle$ where $|M_{11}| = 7920$. The group for the $S(5,6,12)$ is $M_{12} = \langle M_{11},\ (1\ 10)(2\ 5)(3\ 7)(4\ 8)(6\ 9)(11\ 12)\rangle$ where $|M_{12}| = 95040$.

63.46 Construction An $S(3,\{4,6\},12)$ of type $4^{45}6^2$. $H = \langle(1\ 2\ 3\ 4\ 5)(7\ 8\ 9\ 10\ 11)\rangle$. Base blocks: {1 2 3 4 5 6}, {7 8 9 10 11 12}, {1 2 7 8}, {1 2 9 11}, {1 2 10 12}, {3 5 7 8}, {3 5 9 11}, {3 5 10 12}, {4 6 7 8}, {4 6 9 11}, {4 6 10 12}. $G = \langle H$,(1 7)(2 8)(3 9)(4 10)(5 11)(6 12), (3 4 5 6)(9 10 11 12)$\rangle$ and $|G| = 240$.

63.47 Construction An $S(3,\{4,6\},14)$ of type $4^{56}6^7$. $H = \langle(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)\rangle$. Base blocks: {1 2 5 7}, {1 2 6 10}, {1 2 12 14}, {1 3 6 9}, {1 2 4 8 9 11}. $G = \langle H,\ (1\ 2)(3\ 6)(8\ 9)(10\ 13)\rangle$ and $|G| = 2688$.

63.48 Construction An $S(3,4,14)$ of type 4^{91}. $H = \langle(1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9\ 10\ 11\ 12\ 13\ 14)\rangle$. Base blocks: {1 2 3 6}, {1 2 4 14}, {1 2 8 9}, {1 2 10 11}, {1 2 12 13}, {1 3 8 10}, {1 3 9 11}, {1 4 8 11}, {1 4 10 13}, {1 5 9 13}, {1 6 10 12}, {1 11 13 14}, {8 9 10 12}. $G = \langle H,\ (2\ 3\ 5)(7\ 6\ 4)(11\ 14\ 13)(9\ 10\ 12)\rangle$ and $|G| = 42$.

63.49 Construction An $S(3,4,16)$ of type 4^{140}; an $S(3,\{4,8\},16)$ of type $4^{126}8^1$; and an $S(3,\{4,8\},16)$ of type $4^{112}8^2$. To generate an $S(3,4,16)$ of type 4^{140} (here it is the geometry $AG(4,2)$), use $H = \langle(1\ 2\ 5\ 3\ 11\ 6\ 13\ 4\ 12\ 8\ 15\ 7\ 16\ 14)\ (9\ 10)\rangle$, along with base blocks: {1 2 3 9}, {1 2 4 12}, {1 2 5 6}, {1 2 7 13}, {1 2 8 16}, {1 2 10 15}, {1 3 4 15}, {1 3 10 12}, {1 4 5 8}, {1 4 9 10}, {1 5 9 13}, {1 5 11 15}. $G = \langle H$, (4

5 16)(6 8 12)(7 14 15)(10 13 11), (5 7)(6 13)(8 11)(14 16)⟩. Then $|G| = 322,560$ and G is triply transitive on {1,2,...,16}. To get an $S(3,\{4,8\},16)$ of type $4^{126}8^1$ replace the 14 blocks (from the $S(3,4,16)$) of an $S(3,4,8)$ whose points lie entirely in the set $X = \{1,2,3,5,6,7,9,13\}$, by the single 8-block whose points are precisely those of X. For this design $G = \langle$(1 2 6 7 9 5 3) (8 10 16 14 11 15 12), (1 2 3 7 13 5)(4 12 15 11 14 8)(6 9)(10 16)⟩ and $|G|$=10752. To get an $S(3,\{4,8\},16)$ of type $4^{112}8^2$, replace the 14 blocks (from the $S(3,\{4,8\},16)$) of an $S(3,4,8)$ whose points lie entirely in the set $Y = \{4,8,10,11,12,14,15,16\}$ by the single 8-block whose points are those of Y. For this design $G = \langle$(1 2 6 7 9 5 3) (8 10 16 14 11 15 12), (1 4 2 8 3 15 9 11) (5 10 13 16 7 12 6 14)⟩ and $|G|$=21504.

63.50 Construction The $S(3,\{4,6\},16)$ of type $4^{60}6^{16}$. $H = \langle$(1 2 3 4 5 6 7 8) (9 10 11 12 13 14 15 16)⟩. Base blocks: {1 2 3 6 9 11}, {1 3 10 13 14 15}, {1 2 4 13}, {1 2 7 14}, {1 2 12 15}, {1 3 5 7}, {1 4 10 11}, {1 5 9 13}, {1 5 11 15}, {1 9 10 12}, {1 9 14 16}, {9 11 13 15}. $G = \langle H$, (2 3 11)(5 15 12 8 14 7)(6 9)(10 13 16)⟩. $|G|$=11520 and G is doubly transitive on points.

63.51 Construction The $S(3,\{4,6\},16)$ of type $4^{100}6^8$. $H = G = \langle$(1 2 3 4)(5 6 7 8) (9 10 11 12)(13 14 15 16), (3 4)(5 16)(7 15)(8 9)(10 14)(12 13)⟩. Base blocks: {1 2 3 5 9 13}, {5 6 10 11 13 15}, {1 2 6 11}, {1 2 7 14}, {1 5 6 14}, {1 5 7 12}, {1 5 8 15}, {1 5 11 16}, {1 6 7 8}, {5 6 9 12}, {5 7 9 11}. $|G| = 24$ and G has two orbits on points 1 to 4 and 5 to 16.

63.52 Construction The $S(3,\{4,5\},16)$ of type $4^{20}5^{48}$. $H = \langle$(1 2 3 4 5 6 7 8 9 10 11 12 13 14 15)⟩. Base blocks: {1 2 3 6 13}, {1 2 4 8 16}, {2 4 6 11 12}, {3 6 9 12 15}, {1 2 10 14}, {1 6 11 16}. $G = \langle H$, (2 4 5 13)(3 8 9 14)(6 16)(7 15 10 12)⟩. $|G|$=960 and G is 2-transitive on points.

63.53 Construction The $S(3,\{4,5\},16)$ of type $4^{35}5^{42}$. $H = \langle$(1 4 7 11 12 5 14)(2 13 6 3 15 9 10)⟩. Base blocks: {1 2 3 6 8}, {1 2 4 12 13}, {1 2 5 7 15}, {1 3 4 7 9}, {1 4 5 8 10}, {1 9 10 13 15}, {1 2 9 16}, {1 3 10 16}, {1 4 11 16}, {1 6 13 16}, {1 8 15 16}. $G = \langle H$, (1 3 12 15 11)(2 6 9 4 10)(5 7 14 8 13)⟩. $|G|$= 2520 and G fixes 16 and is doubly transitive on 1,...,15. This design uniquely extends to an $S(4,\{5,6\},17)$.

63.54 Construction An $S(3,\{4,5\},16)$ of type $4^{60}5^{32}$. $|H| = 32$ and $H = \langle$(1 7 3 12) (2 8 15 5)(4 14 13 6)(9 10 16 11), (1 9 3 16)(2 13 14 5)(4 6 8 15) (7 12)⟩. Base blocks: {1 2 3 7 14}, {1 2 4 15 16}, {1 2 12 13}, {1 3 9 16}, {1 7 9 10}, {1 7 13 15}, {1 8 13 16}, {2 4 5 14}, {2 6 14 15}. $G = \langle H$, (3 5 4 6)(7 9 15 11) (8 16 10 14)(12 13)⟩. $|G|$=320 and G is point-transitive.

63.55 Construction An $S(3,\{4,5\},16)$ of type $4^{85}5^{22}$. $|H| = 24$ where $H = \langle$(1 2 3 6) (7 14 8 10)(9 16)(11 13 15 12), (1 4 6)(2 3 5)(7 8 12)(11 14 15)⟩. Base blocks: {1 2 3 11 14}, {1 2 4 15 16}, {7 8 9 12 13}, {1 2 10 13}, {1 3 9 16}, {1 7 9 11}, {1 7 13 14}, {1 8 13 16}, {7 8 11 15}, {7 9 15 16}. $G = \langle H$, (1 2 3 5 4) (7 8 9 12 13)(10 15 11 16 14)⟩. $|G|$=120 and G has orbits on point sets of sizes 6 and 10.

63.56 Construction An $S(3,\{4,5\},16)$ of type $4^{100}5^{16}$. $H = \langle$(1 2 9 10 13 11 5 16 4 14 15 6)(3 12 8 7)⟩. Base blocks: {1 2 3 4 16}, {1 4 7 12 13}, {1 2 6 8}, {1 2 10 15}, {1 2 13 14}, {1 3 5 8}, {1 3 7 10}, {1 3 9 15}, {1 4 5 9}, {1 5 10 14}, {1 7 8 14}, {1 7 11 15}, {3 7 8 12}. $G = \langle H$, (1 2 9 10 6)(3 5 4 8 7) (11 12 14 15 13)⟩. $|G|$= 1920 and G is transitive on points.

63.57 Construction An $S(3,\{4,5\},16)$ of type $4^{105}5^{14}$. $|G| = 42$ and $H = G = \langle$(1 2 11 13 3 12 4)(5 9 6 8 10 7 16), (1 5 12 10 3 16)(2 7 11 8 4 6)(9 13)(14 15)⟩. Base blocks: {1 2 3 4 16}, {1 2 6 9}, {1 2 7 10}, {1 2 13 14}, {1 7 14 15}.

63.58 Construction An $S(3,\{4,5\},16)$ **of type** $4^{110}5^{12}$**.** $|G| = 12$ and $H = G = \langle$(1 6 2 5 9 11 8 4 7 10 3 16)(12 14 15 13)$\rangle$. Base blocks: {1 2 3 4 16}, {1 2 5 15}, {1 2 7 14}, {1 2 8 12}, {1 2 11 13}, {1 4 6 8}, {1 4 7 12}, {1 4 13 14}, {1 5 8 10}, {1 5 12 13}, {1 6 13 15}, {1 7 9 13}, {12 13 14 15}.

63.59 Construction The $S(4,\{5,7\},15)$ **of type** $5^{168}7^{15}$. $H = \langle$(1 2 5 8 15 11 13 7 12 10 6 3 14 4 9)$\rangle$. Base blocks:{1 2 3 4 13 14 15}, {1 2 3 5 9}, {1 2 3 6 10}, {1 2 3 7 11}, {1 2 3 8 12}, {1 2 4 5 10}, {1 2 4 7 12}, {1 2 4 8 11}, {1 2 6 7 14}, {1 2 6 8 13}, {1 2 10 11 14}, {1 3 4 5 11}, {1 8 10 13 14}. $G = \langle H$,(1 6 9 4 7 12) (2 8 10)(3 5 11)(14 15)$\rangle$ and $|G|$=20,160. **For the** $S(5,\{6,8\},16)$ **of type** $6^{448}8^{30}$, add 16 to each of the blocks of the given $S(4,\{5,7\},15)$ to get 183 blocks. For the remaining 295 blocks, use the given H and the additional base blocks: {1 2 3 4 5 6 7 8}, {1 2 3 5 10 15}, {1 2 3 5 11 14}, {1 2 3 5 12 13}, {1 2 3 6 11 13}, {1 2 3 6 12 14}, {1 2 3 7 9 14}, {1 2 3 7 10 13}, {1 2 3 7 12 15}, {1 2 3 8 9 13}, {1 2 3 8 10 14}, {1 2 4 5 9 15}, {1 2 4 6 10 15}, {1 2 4 6 11 14}, {1 2 4 6 12 13}, {1 2 4 7 9 13}, {1 2 4 7 10 14}, {1 2 4 8 10 13}, {1 2 5 7 10 11}, {1 3 4 5 10 13}, {1 4 6 8 11 12}. $G = \langle H$, (1 2 5 15 10)(4 8 9 6 12)(7 14 16 13 11)$\rangle$ and $|G|$=322,560 where $G = AGL(4,2)$.

63.60 Construction The $S(4,\{5,6\},17)$ **of type** $5^{140}6^{112}$. $H = \langle$(1 2 3 4 5 6 7 8) (9 10 11 12 13 14 15 16) (17)$\rangle$. Base blocks:{1 2 3 4 6 11}, {1 2 5 9 12 14}, {1 2 6 9 15 16}, {1 10 12 13 14 15}, {1 2 3 7 14 15}, {1 2 9 10 11 13}, {1 2 3 12 13 16}, {1 3 6 9 10 14}, {1 2 4 5 13 15}, {1 7 9 13 14 16}, {1 2 4 10 14 16}, {1 3 5 11 13 14}, {1 2 5 7 11 16}, {1 4 9 11 14 15}, {1 2 3 9 17}, {1 2 4 12 17}, {1 2 5 6 17}, {1 2 10 15 17}, {1 3 4 15 17}, {1 3 5 7 17}, {1 3 6 13 17}, {1 3 10 12 17}, {1 3 14 16 17}, {1 4 9 10 17}, {1 4 13 14 17}, {1 5 9 13 17}, {1 5 10 14 17}, {1 5 11 15 17}, {1 5 12 16 17}, {1 8 10 13 17}, {1 9 11 16 17}, {1 9 12 15 17}, {1 11 12 13 17}, {1 13 15 16 17}, {9 10 13 14 17}, {9 11 13 15 17}. $G = \langle H$, (4 5 16)(6 8 12)(7 14 15)(10 13 11)$\rangle$. $|G|$=40320, where G fixes 17 and is triply transitive on {1,2,...,16}.

See Also

§IV.1	PBDs are tBDs with $t = 2$.
§VI.24	Graphical designs are sometimes t-wise balanced designs.

References Cited: [53, 500, 554, 1037, 1038, 1043, 1060, 1117, 1192, 1193, 1244, 1334, 1341, 1356, 1357, 1613, 2051, 2151, 2170]

64 Whist Tournaments

Ian Anderson
Norman J. Finizio

64.1 Definitions and Examples

64.1 A *whist tournament* Wh($4n$) for $4n$ players is a schedule of games each involving two players opposing two others, such that

1. the games are arranged into $4n - 1$ rounds, each of n games;
2. each player plays in exactly one game in each round;
3. each player partners every other player exactly once;
4. each player opposes every other player exactly twice.

64.2 Each game is denoted by an ordered 4-tuple (a, b, c, d) in which the pairs $\{a, c\}$, $\{b, d\}$ are *partner pairs*. $\{a, c\}$ is a *partner pair of the first kind*, and $\{b, d\}$ is a *partner pair of the second kind*. The other pairs are *opponent pairs*; in particular $\{a, b\}$, $\{c, d\}$ are *opponent pairs of the first kind*, and $\{a, d\}$, $\{b, c\}$ are *opponent pairs of the second kind*.

64.3 Example A Wh(8) with players $\infty, 0, 1, \ldots, 6$.

Round			Round		
1	$(\infty, 4, 0, 5)$	$(1, 2, 3, 6)$	5	$(\infty, 1, 4, 2)$	$(5, 6, 0, 3)$
2	$(\infty, 5, 1, 6)$	$(2, 3, 4, 0)$	6	$(\infty, 2, 5, 3)$	$(6, 0, 1, 4)$
3	$(\infty, 6, 2, 0)$	$(3, 4, 5, 1)$	7	$(\infty, 3, 6, 4)$	$(0, 1, 2, 5)$
4	$(\infty, 0, 3, 1)$	$(4, 5, 6, 2)$			

64.4 A *whist tournament* Wh$(4n + 1)$ for $4n + 1$ players is defined as for $4n$, except that Conditions 1, 2 are replaced by

1′. the games are arranged into $4n + 1$ rounds each of n games;

2′. each player plays in one game in each of $4n$ rounds, but does not play in the remaining round.

64.5 Remarks

1. Think of (a, b, c, d) as giving the order in which the players sit around a table, a and c playing north-south, b and d playing east-west.
2. A Wh$(4n)$ is an RBIBD$(4n, 4, 3)$ in which the blocks are ordered so that each pair of elements occurs as a partner (opponent) pair once (twice).

64.6 Theorem A Wh$(4n)$ and a Wh$(4n + 1)$ exist for all $n \geq 1$ (see [94, 141]).

64.2 Z-Cyclic Whist Tournaments

64.7 A Wh$(4n)$ is $\mathbb{Z}$-cyclic if the players are $\infty, 0, 1, \ldots, 4n-2$ and each round is obtained from the previous one by adding 1 modulo $4n-1$ to each non-∞ entry. A Wh$(4n+1)$ is $\mathbb{Z}$-cyclic if the players are $0, 1, \ldots, 4n$ and the rounds are similarly developed modulo $4n + 1$.

64.8 Example A $\mathbb{Z}$-cyclic Wh(5) with players $0, 1, 2, 3, 4$.

Round	1	2	3	4	5
Games	(1,2,4,3)	(2,3,0,4)	(3,4,1,0)	(4,0,2,1)	(0,1,3,2)

64.9 Remarks

1. By convention ∞, 0 are partners in the initial round of a $\mathbb{Z}$-cyclic Wh$(4n)$, and 0 is absent from the initial round of a $\mathbb{Z}$-cyclic Wh$(4n + 1)$.
2. Example 64.3 is $\mathbb{Z}$-cyclic.
3. The partner pairs in the initial round of a $\mathbb{Z}$-cyclic Wh$(4n + 1)$ form a starter in $\mathbb{Z}_{4n+1}$. See §VI.55.
4. $\mathbb{Z}$-cyclic whist tournaments are given by presenting only the initial round.

64.10 Theorem If $p = 4n + 1$ is prime and w is a primitive root of p, then the games $(w^i, w^{i+n}, w^{i+2n}, w^{i+3n})$, $0 \leq i \leq n-1$, form the initial round of $\mathbb{Z}$-cyclic Wh$(4n+1)$.

64.11 Remark Let P denote any product of primes p with each $p \equiv 1 \pmod 4$, and let q, r denote primes with both $q, r \equiv 3 \pmod 4$.

64.12 Theorem A $\mathbb{Z}$-cyclic Wh$(4n)$ is known to exist when:

1. $4n \leq 132$ (see [38, 93]).
2. $4n = 2^\alpha (\alpha \geq 2)$ (see [96]).
3. $4n = qP + 1,\ q \in \{3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127\}$ (see [38]).
4. $4n = 3P + 1$ (see [96]).
5. $4n = 3^{2m+1} + 1,\ m \geq 0$ [99].
6. $4n = qr^2P + 1$, q and r distinct, $q < 60,\ r < 100$ (see [38]).

64.13 Theorem A $\mathbb{Z}$-cyclic Wh$(4n + 1)$ is known to exist when:

1. $4n + 1 = P$ or r^2P and $r \leq 100$ (see [38, 100]).
2. $4n + 1 \leq 149$ (see [38]).
3. $4n + 1 = 3^{2m}$ or $3^{2m}P$ [99].
4. $4n + 1 = 3sP,\ s \in \{7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47\}$ (see [38]).

64.14 Examples Initial rounds of $\mathbb{Z}$-cyclic Wh$(4n)$, $n \leq 12$.

$4n =$ 4 $(\infty, 1, 0, 2)$.

8 $(\infty, 4, 0, 5), (1, 2, 3, 6)$.

12 $(\infty, 4, 0, 5), (1, 2, 10, 8), (3, 6, 7, 9)$.

16 $(\infty, 5, 0, 10), (1, 4, 2, 8), (6, 13, 9, 7), (11, 12, 3, 14)$.

20 $(\infty, 13, 0, 17), (8, 2, 10, 1), (3, 18, 15, 4), (7, 12, 16, 9), (11, 14, 5, 6)$.

24 $(\infty, 22, 0, 10), (14, 20, 7, 12), (19, 18, 15, 8), (4, 6, 13, 9), (11, 3, 17, 5)$, $(21, 1, 16, 2)$.

28 $(\infty, 23, 0, 15), (18, 9, 21, 20), (14, 19, 2, 25), (4, 1, 22, 5)$, $(6, 12, 7, 26), (8, 24, 10, 17), (13, 11, 3, 16)$.

32 $(\infty, 18, 0, 25), (12, 4, 2, 5), (6, 28, 9, 20), (23, 11, 8, 24)$, $(15, 13, 29, 19), (1, 14, 3, 10), (17, 16, 22, 27), (21, 7, 30, 26)$.

36 $(\infty, 16, 0, 32), (28, 14, 3, 27), (31, 13, 4, 2), (20, 24, 34, 33)$, $(26, 1, 19, 6), (7, 12, 8, 15), (17, 23, 21, 29), (18, 9, 30, 11)$, $(22, 10, 5, 25)$.

40 $(\infty, 0, 13, 26), (1, 8, 25, 5), (2, 16, 11, 10), (4, 32, 22, 20)$, $(14, 38, 18, 21), (15, 24, 23, 29), (17, 35, 33, 6), (27, 31, 34, 12)$, $(28, 36, 3, 37), (30, 7, 19, 9)$.

44 $(\infty, 43, 38, 2), (21, 19, 34, 10), (35, 23, 31, 4), (6, 5, 42, 32)$, $(37, 14, 12, 17), (33, 18, 39, 30), (26, 1, 25, 36), (22, 9, 8, 29)$, $(15, 11, 20, 28), (40, 3, 7, 24), (16, 13, 27, 41)$.

48 $(\infty, 13, 9, 15), (30, 17, 11, 4), (39, 20, 34, 31), (23, 22, 37, 25)$, $(43, 27, 2, 19), (46, 35, 42, 10), (47, 18, 21, 1), (41, 16, 29, 6)$, $(38, 36, 45, 7), (33, 12, 32, 28), (44, 5, 24, 14), (40, 26, 8, 3)$.

64.15 Examples Initial rounds of $\mathbb{Z}$-cyclic Wh$(4n + 1)$, $3 \leq n \leq 12$.

$4n + 1 =$ 13 $(1, 8, 12, 5), (2, 3, 11, 10), (4, 6, 9, 7)$.

17 $(1, 13, 16, 4), (3, 5, 14, 12), (9, 15, 8, 2), (10, 11, 7, 6)$.

21 $(1, 12, 2, 15), (5, 6, 3, 18), (4, 7, 11, 20), (8, 13, 19, 17), (14, 10, 9, 16)$.

25 $(5, 3, 1, 14), (9, 17, 16, 20), (15, 6, 21, 7), (10, 4, 8, 13)$, $(2, 12, 19, 22), (11, 18, 24, 23)$.

29 $(1, 2, 9, 27), (16, 3, 28, 26), (24, 19, 13, 10), (7, 14, 5, 15)$, $(25, 21, 22, 8), (23, 17, 4, 12), (20, 11, 6, 18)$.

33 $(1, 3, 5, 20), (4, 17, 28, 29), (31, 25, 26, 2), (9, 12, 22, 30)$, $(13, 27, 24, 19), (6, 16, 7, 23), (32, 11, 18, 14), (15, 8, 21, 10)$.

37 $(1, 2, 17, 4), (16, 32, 13, 27), (34, 31, 23, 25), (26, 15, 35, 30), (9, 18, 5, 36)$, $(33, 29, 6, 21), (10, 20, 22, 3), (12, 24, 19, 11), (7, 14, 8, 28)$.

41 $(1,17,4,15),(36,12,21,13),(10,6,40,27),(32,38,5,7),$
$(18,19,31,24),(33,11,9,29),(16,26,23,35),(2,28,8,3),$
$(37,14,25,22),(20,34,39,30).$

45 $(42,14,22,41),(21,7,12,39),(8,15,25,36),(17,29,13,28),$
$(5,37,16,18),(23,32,9,38),(33,11,30,40),(6,3,1,26),$
$(35,34,20,44),(2,10,4,43),(19,24,27,31).$

49 $(1,2,3,6),(4,8,25,40),(7,42,16,32),(12,48,13,45),$
$(18,36,5,10),(23,46,9,34),(28,21,43,37),(20,31,38,26),$
$(30,11,41,33),(22,44,15,24),(14,35,39,29),(17,19,47,27).$

64.3 Whist Tournaments with Additional Properties

64.16 A *directed whist tournament* DWh(v) is a Wh(v) with Condition 4 replaced by
($4'$) each player has every other player as an opponent once on the right and once on the left.

64.17 Theorem [2205] A DWh($4n+1$) exists for all $n \geq 1$, and a DWh($4n$) exists at least for all $n \geq 48$.

64.18 Theorem

1. No $\mathbb{Z}$-cyclic DWh($4n$) exists.
2. A $\mathbb{Z}$-cyclic DWh($4n+1$) exists when $4n+1$ is a product of primes $p \equiv 1 \pmod 4$; also when $4n+1 \in \{21,33,45,49,57,69,77,81\}$ (see [30]).
3. A $\mathbb{Z}$-cyclic DWh($2^{2n}+2^n+1$) exists for all $n \geq 2$ [395].

64.19 Examples $\mathbb{Z}$-cyclic DWh(m)s for $m = 21$ and 33.

$m = 21$ $(1,8,2,14),(3,7,6,11),(4,10,12,15),(5,19,16,17),(9,20,18,13)$

$m = 33$ $(25,27,14,32),(26,6,10,29),(23,21,4,13),(16,12,7,15),$
$(3,2,24,31),(5,17,20,11),(30,22,28,9),(18,8,19,1)$

64.20 Remarks

1. A DWh(v) is a resolvable perfect Mendelsohn design with block size 4 (§VI.35).
2. The Wh(p) constructed in Theorem 64.10 are all DWh(p).

64.21 A *triplewhist tournament* TWh(v) is a Wh(v) with Condition 4 replaced by
($4''$) each player has every other player once as an opponent of the first kind and once as an opponent of the second kind.

64.22 Theorem A TWh($4n+1$) exists for all $n \geq 5$, and possibly for $n = 4$. A TWh($4n$) exists for all $n \geq 1$ except for $n = 3$ (see [1485, 38]).

64.23 Theorem A $\mathbb{Z}$-cyclic TWh($4n+1$) exists when:

1. $4n+1$ is a prime $p \equiv 1 \pmod 4$, $p \geq 29$ [383];
2. $4n+1 = q^2$ where q is prime, $q \equiv 3 \pmod 4$, $7 \leq q \leq 83$ [32];
3. $4n+1 = 5^n$ or 13^n ($n \geq 2$) [32];
4. $4n+1$ is the product of any values in the above three items [100].

64.24 Theorem A $\mathbb{Z}$-cyclic TWh($4n$) exists when:

1. $4n = qP+1$, $q \in \{3,7,19,23,31,43,47,59,67,71,79,83,103,107,127,131\}$ [38];
2. $4n = 2^n$ ($n \geq 2$) (see [96]);
3. $4n = 3^m+1$ (m odd) [99].

64.25 Theorem A $\mathbb{Z}$-cyclic directed TWh(p) exists for all primes p, $p \equiv 1 \pmod 4$, $29 \le p < 10,000$, with the possible exceptions of $97, 193, 257, 449, 641, 769, 1153, 1409$, and 7681, and for the products of all such primes. [98]

64.26 Remark The Wh($4n$) in Example 64.14 are TWh($4n$) except in the case $4n = 12$. The Wh($4n+1$) in Example 64.15 are TWh($4n+1$) in the cases $4n+1 \ge 21$.

64.27 Table Initial rounds of $\mathbb{Z}$-cyclic TWh(p), p prime, $p \equiv 1 \pmod 4$, $50 < p < 100$. Elements in $\mathbb{Z}_p$. Those for $p = 53, 61, 73, 89$ are also directed.

$$\begin{aligned}
p = 53: &\quad (1,2,23,11) \times 1, 2^4, 2^8, \ldots, 2^{48} \\
61: &\quad (1,2,38,3) \times 1, 2^4, 2^8, \ldots, 2^{56} \\
73: &\quad (1,26,47,36) \times 26^{8i+2j} \quad (0 \le i \le 8,\ 0 \le j \le 1) \\
89: &\quad (1,3,88,61) \times 3^{8i+2j} \quad (0 \le i \le 10,\ 0 \le j \le 1) \\
97: &\quad (1,7,90,62) \times 7^{32i+2j} \quad (0 \le i \le 2,\ 0 \le j \le 7).
\end{aligned}$$

64.28 An *ordered whist tournament* OWh(v) is a Wh(v) with Condition 4 replaced by ($4'''$) each player has every other player as an opponent once while being a partner of the first kind, and once while being a partner of the second kind.

64.29 Theorem An OWh($4n+1$) exists for all $n \ge 1$, but no OWh($4n$) exists.

64.30 Theorem [30] A directed OWh($4n+1$) exists for all $n \ge 1$.

64.31 Theorem [30] A $\mathbb{Z}$-cyclic OWh($4n+1$) exists whenever $4n+1$ is a product of primes $p \equiv 1 \pmod 4$; also when $4n+1 \le 81$, $4n+1 \ne 9$.

64.32 Theorem A $\mathbb{Z}$-cyclic ordered TWh(p) and a $\mathbb{Z}$-cyclic directed TWh(p) exist for all primes $p \equiv 5 \pmod 8$, $p \ge 29$, and for all primes $p \equiv 9 \pmod{16}$. [97]

64.33 Remark The Wh(p) of Theorem 64.10 are all OWh(p).

64.34 A whist tournament has the *three-person property* if no three players appear together in more than one game; that is, if the underlying block design is supersimple. A Wh(v) with the 3-person property is denoted by 3PWh(v).

64.35 Theorem [874] A 3PWh(v) exists for all $v \equiv 0$ or $1 \pmod 4$, $v \ge 8$, except for $v = 12$.

64.36 Examples $\mathbb{Z}$-cyclic 3PWh(v)s for $v = 8$ and 13.

$v = 8$: $(\infty, 1, 0, 5), (6, 2, 3, 4)$ $\qquad$ $v = 13$: (1,2,4,8),(3,6,2,11),(5,9,7,10)

64.4 Generalized Whist Tournaments

64.37 Let t, e, k, v be integers such that $k = et$ and $v \equiv 0$ or $1 \pmod k$. A (t,k) *generalized whist tournament design* on v players, denoted by $(t,k)GWhD(v)$, is a (near)-resolvable BIBD($v, k, k-1$) whose blocks can be partitioned into e subblocks in such a way that

1. each subblock consists of t players;
2. each player partners (appears in the same subblock as) every other player $t-1$ times; and
3. each player opposes (appears in the same block but not the same subblock as) every other player $k-t$ times.

64.38 Examples Initial round of some $\mathbb{Z}$-cyclic generalized Whist tournament designs.

$(3,6)GWhD(12)$: $(\infty, 0, 1; 2, 4, 7), (3, 8, 10; 5, 6, 9)$
$(2,10)GWhD(20)$: $(\infty, 6; 1, 4; 16, 7; 9, 17; 11, 5), (0, 2; 3, 10; 8, 12; 14, 15; 13, 18)$
$(4,8)GWhD(17)$: $(1, 13, 16, 4; 9, 15, 8, 2), (3, 5, 14, 12; 10, 11, 7, 6)$

64.39 Remarks

1. A $(2,4)GWhD(v)$ is therefore a $Wh(v)$.
2. A$(4,8)GWhD(v)$ is known as a *pitch tournament*.
3. Generalized whist tournament designs form a special class of (near) resolvable nested BIBDs. See §VI.36.

64.40 Theorem [35] A $(2,6)GWhD(6n+1)$ exists for all $n \geq 1$, and a $(2,6)GWhD(6n)$ exists for all $n \geq 1$ except possibly for $n = 3, 18, 22, 29, 44$.

64.41 Theorem [33] A $(3,6)GWhD(6n+1)$ exists for all $n \geq 1$, and a $(3,6)GWhD(6n)$ exists for all n with 73 possible exceptions, the largest of which is $n = 199$.

64.42 Theorem [34, 36] A $(4,8)GWhD(8n+1)$ exists for all $n \geq 1$, with at most 28 exceptional values, the largest of which is $n = 224$, and a $(4,8)GWhD(8n)$ exists for all $n \geq 1$, with at most 187 exceptions, the largest of which is 1615.

64.5 Connections with Other Combinatorial Structures

64.43 Theorem [140] If TWh(v) exists, then a resolvable spouse avoiding mixed doubles round robin tournament for v couples (SAMDRR(v)) exists (see §VI.51.11).

64.44 Theorem [140] If a resolvable SAMDRR(n) exists, then a TWh($4n$) exists.

64.45 Theorem [140] If a $\mathbb{Z}$-cyclic TWh($4n+1$) or DWh($4n+1$) exists, then there are 4 MOLS of order $4n+1$.

See Also

§VI.35	Resolvable Mendelsohn designs are generalizations of DWh(v).
§III.5	TWh(v) are related to SOLSSOMs and to SAMDRRs, as in Theorems 64.43 and 64.44.
[94]	Contains a chapter on whist tournaments.
[93]	Surveys the development of constructions of whist tournaments up to 1993, and contains much of the information in this chapter.
[37]	Provides an introduction to generalized whist tournaments.

References Cited: [30, 32, 33, 34, 35, 36, 37, 38, 93, 94, 96, 97, 98, 99, 100, 140, 141, 383, 395, 874, 1485, 2205]

65 Youden Squares and Generalized Youden Designs

Donald A. Preece
Charles J. Colbourn

65.1 Definition and Example

65.1 Let S be a set of v *symbols* (or *treatments*). A *Youden square* of size $k \times v$ (or $k \times v$ Youden square) is a $k \times v$ rectangular array of symbols, $k < v$, satisfying

1. each symbol of S occurs exactly once in each row, and
2. the symbols in each column constitute a k-subset of S, and the v such subsets constitute the blocks of a symmetric design.

65.2 Example A 3×7 Youden square.

4	7	2	3	1	5	6
6	5	1	7	4	2	3
7	1	6	2	3	4	5

65.3 Remarks Youden squares were first discussed in [2195]. A $k \times v$ Youden square Y with $S = \{1, 2, ..., v\}$ is equivalent to a $v \times v$ array A such that

1. $A(i, j) = p$ for $i, j = 1, 2, \ldots, v$, if $Y(p, j) = i$ for $p = 1, 2, \ldots, k$,
2. $A(i, j)$ is empty, otherwise.

The squareness of A is the historical reason for the rectangular Y being described as a Youden square, not a Youden rectangle.

65.4 Remark If the entry in each nonempty cell of A is replaced by the entry 1, and the entry 0 is put into each empty cell of A, then A becomes the incidence matrix of the symmetric design on which Y is based.

65.2 Existence

65.5 Theorem A Youden square can be constructed from any symmetric design by suitably ordering the elements of each block of the symmetric design. (See §II.6 and Construction 65.31.)

65.6 Remark A $(v-1) \times v$ Youden square can be obtained by deleting any row of any $v \times v$ latin square.

65.7 Remark Any $k \times v$ Youden square can be completed to a $v \times v$ latin square by the addition of $v - k$ rows (Theorem III.1.77). If $k < v - 1$, the added rows constitute a $(v - k) \times v$ Youden square.

65.3 Enumeration of Youden Squares

65.8 Let Y_1 and Y_2 be $k \times v$ Youden squares with $S = \{1, 2, \ldots, v\}$.

1. Y_1 and Y_2 belong to the same *transformation set (isotopy class)* if Y_2 can be obtained from Y_1 by any combination of permuting the rows, permuting the columns, and permuting the symbols.
2. Y_2 is the *dual* of Y_1 if, given that the $(i, j)th$ element of Y_2 is q $(i = 1, 2, \ldots, k; j = 1, 2, \ldots, v)$, then the $(i, q)th$ element of Y_1 is j $(i = 1, 2, \ldots, k; q = 1, 2, \ldots, v)$.
3. Y_1 and Y_2 belong to the same *species (main class)* if Y_1 and either Y_2 or the dual of Y_2 belong to the same transformation set.

65.9 Table The number of transformation sets and species of small Youden squares.

$k \times v$	2×3	3×4	3×7	4×5	4×7	5×6	6×7
Transformation Sets	1	2	1	3	6	40	3479
Species	1	2	1	3	6	33	1986

65.10 Table The six species of 4×7 Youden squares.

1	2	3	4	5	6	7
2	3	4	5	6	7	1
3	4	5	6	7	1	2
5	6	7	1	2	3	4

1	2	5	6	7	3	4
2	4	3	1	5	6	7
3	6	4	5	2	7	1
5	3	7	4	6	1	2

1	6	5	4	2	3	7
2	4	3	5	7	6	1
3	2	7	6	5	1	4
5	3	4	1	6	7	2

1	6	5	4	2	3	7
2	3	7	6	5	1	4
3	2	4	5	7	6	1
5	4	3	1	6	7	2

1	6	5	4	2	3	7
2	3	4	5	6	7	1
3	2	7	6	5	1	4
5	4	3	1	7	6	2

1	6	5	4	2	3	7
2	3	4	5	7	6	1
3	2	7	6	5	1	4
5	4	3	1	6	7	2

65.4 Double Youden Rectangles

65.11 Let S be a set of v elements and T be a distinct set of k elements. A *double Youden rectangle* of size $k \times v$ (or $k \times v$ double Youden rectangle) is a $k \times v$ rectangular array, $k < v$, such that

1. Each entry is an ordered pair $(x, y) \in S \times T$.
2. If the elements from T are disregarded, the array becomes a $k \times v$ Youden square whose symbols are taken from S.
3. Each element from T is paired exactly once with each element from S.
4. Each element from T occurs exactly once in each column.
5. Each element from T occurs exactly n or $n+1$ times in each row, where n is the integral part of v/k, and if n occurrences of each element from T are removed from each row, leaving $v - nk$ elements from T in each row, then either (i) $v - nk = 1$ or (ii) the k sets of $v - nk$ remaining elements of T in the k rows constitute the blocks of a symmetric design with k blocks.

65.12 Example A 4×13 double Youden rectangle that can be constructed from a standard deck of 52 playing cards, with $S = \{\text{A}, 2, 3, ..., 10, \text{J}, \text{Q}, \text{K}\}$ and $T = \{\spadesuit, \diamondsuit, \clubsuit, \heartsuit\}$.

A♠	3♣	4♡	7♡	8♣	2♣	10♢	J♠	5♠	6♢	Q♢	K♠	9♡
2♢	5♡	3♢	4♠	6♠	7♢	8♠	9♣	10♣	K♡	J♡	Q♣	A♢
4♣	J♢	6♣	K♢	5♢	9♠	7♣	8♡	Q♡	10♠	A♣	2♡	3♠
10♡	2♠	Q♠	5♣	A♡	6♡	3♡	4♢	9♢	J♣	7♠	8♢	K♣

65.13 Table Existence results for double Youden rectangles, $k \leq 15$.

$k \times v$	3×7	4×7	4×13	5×11	5×21	6×11	6×31
Existence	No	Yes	Yes	Yes	Yes	Yes	Yes

$k \times v$	7×15	8×15	8×57	9×19	9×37	9×73	10×19
Existence	Yes	Yes	Yes	Yes	Yes	?	Yes

$k \times v$	10×31	10×91	11×23	11×56	12×23	12×133	13×27
Existence	?	?	Yes	?	Yes	?	Yes

$k \times v$	13×40	13×79	13×157	14×27	14×183	15×31
Existence	Yes	?	?	?	?	?

65.14 Remark For all known double Youden rectangles, $v - nk = 1$ or $v - nk = k - 1$.

65.15 Theorem If $k \equiv 1$ or $3 \pmod 4$ is a prime power, $k \geq 7$, then there exists a $k \times (2k+1)$ double Youden rectangle.

65.5 Balanced Superimpositions of Two Youden Squares

65.16 Let S_1 and S_2 each be v-sets. A *balanced superimposition* of two $k \times v$ Youden squares (or a *Freeman–Youden rectangle*) is a $k \times v$ rectangular array D such that

1. Each entry is an ordered pair $(x, y) \in S_1 \times S_2$.
2. If the elements from S_1 (or S_2) are disregarded, the array becomes a $k \times v$ Youden square whose symbols are taken from S_2 (or S_1).
3. If n_{21} is the $v \times v$ $(0,1)-$matrix whose (i,j)th element $(i, j = 1, 2, \ldots, v)$ is the number of times that the ith element of S_2 is paired with the jth element of S_1, then n_{21} is the incidence matrix of a symmetric design.
4. If n_1 is the $v \times v$ $(0,1)-$matrix whose (i,j)th element $(i, j = 1, 2, \ldots, v)$ is the number of times that the ith element of S_1 occurs in the jth column of D, and n_2 is defined likewise for S_2, then $n_{21}^t n_2 n_1^t + n_1 n_2^t n_{21} = n_{21} n_1 n_2^t + n_2 n_1^t n_{21}^t = dI + eJ$ where d and e are integers, I is the $v \times v$ identity matrix, and J is the $v \times v$ matrix whose elements are all 1.

65.17 Example Two balanced superimpositions of two 3×7 Youden squares with $S_1 = S_2 = \{1, 2, \ldots, 7\}$.

23	34	45	56	67	71	12
35	46	57	61	72	13	24
52	63	74	15	26	37	41

$(d = -2,\ e = 8)$

24	35	46	57	61	72	13
37	41	52	63	74	15	26
56	67	71	12	23	34	45

$(d = 5,\ e = 7)$

65.18 Remark A balanced superimposition of two $(v-1) \times v$ Youden squares can be obtained by deleting any row of any $v \times v$ graeco-latin square.

65.19 Theorem If q is any positive integer such that $4q + 3$ is a prime power, then balanced superimpositions of two Youden squares exist for the sizes $(2q + 1) \times (4q + 3)$ and $(2q + 2) \times (4q + 3)$.

65.20 Remark Balanced superimpositions of two Youden squares have also been found for sizes 7×15, 8×15, and $(2^{2n-1} \pm 2^{n-1}) \times 2^{2n}$, $n \geq 2$.

65.6 Generalized Youden Designs

65.21 A *generalized Youden design* GYD(v, b_1, b_2) is a $b_1 \times b_2$ array B with $b_1 = m_1 v + c_1$ and $b_2 = m_2 v + c_2$, $0 \leq c_1, c_2 < v$, such that

1. each cell contains one element from a set V of v elements;
2. every element occurs either m_1 or $m_1 + 1$ times in each row and either m_2 or $m_2 + 1$ times in each column;
3. every pair of distinct elements occur together in a row the same number of times and together in a column the same number of times.

65.22 Example A GYD(4,6,6). (All GYD(4,6,6)s are enumerated in [1762].)

a	b	c	d	b	d
b	a	d	c	c	b
c	d	a	b	d	a
d	c	b	a	a	c
c	a	d	b	a	b
d	b	a	c	c	d

65.23 Examples A GYD(6,10,15) and a GYD(9,12,12).

a	b	c	d	e	f	a	b	c	d	e	f	c	d	b
b	c	d	e	f	a	b	c	d	e	f	a	b	c	a
c	d	e	f	a	b	c	d	e	f	a	b	d	a	e
d	e	f	a	b	c	d	e	f	a	b	c	a	f	d
e	f	a	b	c	d	e	f	a	b	c	d	f	e	c
f	a	b	c	d	e	f	a	b	c	d	e	e	b	f
c	e	a	f	e	d	c	b	a	f	d	b	a	e	c
f	c	b	a	b	e	a	d	e	d	f	c	e	d	b
b	a	e	d	f	a	d	c	f	c	b	e	f	b	a
a	b	d	b	a	c	f	e	d	e	c	f	c	f	d

a	b	c	d	e	f	g	h	i	a	b	c
b	c	d	e	f	g	h	i	a	d	e	f
c	d	e	f	g	h	i	a	b	g	h	i
d	e	f	g	h	i	a	b	c	i	a	e
e	f	g	h	i	a	b	c	d	c	d	h
f	g	h	i	a	b	c	d	e	f	g	b
g	h	i	a	b	c	d	e	f	h	f	a
h	i	a	b	c	d	e	f	g	b	i	d
i	a	b	c	d	e	f	g	h	e	c	g
a	b	c	i	h	g	f	d	e	a	d	g
d	e	f	a	c	b	h	i	g	b	e	h
g	h	i	e	d	f	a	b	c	c	f	i

65.24 A *balanced block design* BBD(v, b_1, b_2) is a collection $\mathcal{B}$ of b_1 multisets (*blocks*) of elements from a v-set V, each of size b_2, so that

1. $b_2 = m_2 v + c_2$, $0 \le c_2 < v$, and every $x \in V$ appears in every $B \in \mathcal{B}$ either m_2 or $m_2 + 1$ times; and
2. every pair of distinct elements occur together in the same block of $\mathcal{B}$ the same number of times.

65.25 Remark A GYD(v, b_1, b_2) is equivalent to an array in which the multisets defined by the rows form a BBD(v, b_1, b_2), and the multisets defined by the columns form a BBD(v, b_2, b_1). When $b_1 < v$ and $b_2 = v$, a GYD is a Youden square, and the BBD(v, b_2, b_1) is a symmetric BIBD.

65.26 Remarks If a BBD(v, b_1, b_2) $(V, \mathcal{B})$ exists with $b_2 = m_2 v + c_2$, $0 \le c_2 < v$, then by removing m_2 copies of each element from each $B \in \mathcal{B}$, one obtains a collection $\widehat{\mathcal{B}}$ for which $(V, \widehat{\mathcal{B}})$ is a BIBD. Thus, the existence of a BBD(v, b_1, b_2) is equivalent to that of a BIBD with parameters $(v, b = b_1, r = \frac{b_1 c_2}{v}, k = c_2, \lambda = \frac{b_1 c_2 (c_2 - 1)}{v(v-1)})$. Hence, one obtains a necessary condition for the existence of a GYD(v, b_1, b_2).

65.27 Theorem (*necessary conditions*) If a GYD(v, b_1, b_2) exists with $b_1 = m_1 v + c_1$ and $b_2 = m_2 v + c_2$, $0 \le c_1, c_2 < v$, then (1) $v \mid c_1 c_2$, (2) $v - 1 \mid b_1 c_2 (c_2 - 1)$, and (3) $v - 1 \mid b_2 c_1 (c_1 - 1)$.

65.7 Regular GYDs

65.28 A GYD(v, b_1, b_2) is *doubly regular* if $v \mid b_1$ and $v \mid b_2$.

65.29 Construction A doubly regular GYD. Let $b_1 = m_1 v$ and $b_2 = m_2 v$. Let (ℓ_{ij}), $0 \le i, j < v$ be a $v \times v$ latin square. Then define a $b_1 \times b_2$ array $R = (r_{ij})$ by setting $r_{av+i, bv+j} = \ell_{ij}$, for $0 \le a < m_1$, $0 \le i < v$, $0 \le b < m_2$, and $0 \le j < v$. In other words, R can be blocked into a $m_1 \times m_2$ pattern in which each block is a copy of L. Then R is a GYD(v, b_1, b_2).

65.30 A GYD(v, b_1, b_2) is (*simply*) *regular* if $v \mid b_1$ or $v \mid b_2$.

65.31 Construction A regular GYD(v, b_1, b_2). If $v \mid b_1$ and $v \mid b_2$, apply Construction 65.29. Otherwise, if $v \mid b_2$, use the following to form a GYD(v, b_2, b_1), and transpose the result. Suppose that $b_1 = m_1 v$ and $b_2 = m_2 v + c_2$, with $0 < c_2 < v$. If no BBD(v, b_1, b_2) exists, there is no GYD(v, b_1, b_2). Otherwise, let $(V, \mathcal{B})$ be a BBD(v, b_1, b_2). Let $V = \{p_1, \ldots, p_v\}$, and let $\mathcal{B} = \{B_1, \ldots, B_{b_1}\}$. Form a bipartite multigraph G on the vertices $\{p_1, \ldots, p_v\} \cup \{\ell_1, \ldots, \ell_{b_1}\}$; vertices p_i and ℓ_j are connected by σ edges if p_i

appears exactly σ times in B_j. Now using Algorithm 65.32, assign colors to the edges of G. The edge colors are used to form a $b_1 \times b_2$ array R; each edge color determines the column in which the corresponding element of the block is to be placed. When edge $e = \{p_i, \ell_j\}$ gets color c, place p_i in cell (i, c) of R. The resulting array R is a GYD provided that

1. the number of edge colors is b_2;
2. for each vertex ℓ_j and for each color c, there is exactly one edge colored c incident at ℓ_j; and
3. for each vertex p_i and for each color c, there are exactly m_1 edges colored c incident at p_i.

Algorithm 65.32 guarantees that these conditions hold.

65.32 Algorithm Balanced edge-coloring.

1. Initialize by arbitrarily assigning different colors to each of the b_2 edges incident at each vertex p_i (using a total of b_2 colors).
2. While there is a vertex p_i and a color c for which fewer than m_1 edges incident at p_i are colored c (a *deficient vertex*), one finds an "alternating path" as follows. Choose a second color c' that is the color of more than m_1 edges incident at p_i. Starting at $p_{s_0} = p_i$, form a sequence of distinct edges $e_0, \ldots, e_{2n-1}$, where $e_{2i} = \{p_{s_i}, \ell_{t_i}\}$ is an edge of color c' for $0 \le i < n$, and $e_{2i+1} = \{\ell_{t_i}, p_{s_{i+1}}\}$ is an edge of color c for $0 \le i < n$. This can be formed in a greedy manner, stopping only when color c appears on more edges incident at p_n than does color c'. When such a vertex s_n is encountered, interchange the colors c and c' on all of the edges $e_0, \ldots, e_{2n-1}$. If a deficient vertex still exists, repeat this step; otherwise, stop.

65.33 Remark Let γ_{ij} denote the number of edges colored j that are incident at p_i. Considering $M = \sum_{i=1}^{v} \sum_{j=1}^{b_2} |\gamma_{ij} - m_1|$ as the total deficiency, Algorithm 65.32 reduces the total deficiency by at least two whenever an alternating path is switched. Thus, the method is efficient, taking at most $vb_2m_1/2$ alternating paths.

65.34 Theorem A GYD(v, b_1, b_2) with $v|b_1$ exists if and only if the "row" BBD(v, b_1, b_2) exists.

65.8 Nonregular GYDs

65.35 Lemma If a GYD(v, m_1v, b_2) and a GYD(v, b_1, b_2) both exist, then a GYD$(v, m_1v + b_1, b_2)$ exists.

65.36 Theorem [1296] Let v, b_1, and b_2 be positive integers, and write $b_i = m_iv + c_i$ with $0 \le c_i < v$ for $i = 1, 2$. Let $c_1c_2 = tv$. If there exists a BBD(v, b_1, c_2) $(V, \mathcal{B})$ and a BBD(v, b_2, c_1) $(V, \mathcal{D})$, so that $\mathcal{B}$ contains a collection $\widehat{\mathcal{B}}$ of c_1 blocks and every element occurs exactly t times, and the blocks of $\widehat{\mathcal{B}}$ can be arranged as the rows of a $c_1 \times c_2$ array whose columns appear as blocks of $\mathcal{D}$, then a GYD(v, b_1, b_2) exists.

65.37 Corollary If $c_1c_2 = v$, and a BBD(v, b_1, c_2) and a BBD(v, b_2, c_1) both exist having a parallel class of blocks, then a GYD(v, b_1, b_2) exists.

65.38 Lemma If a GYD(v, b_1, a_2v) contains a GYD(v, b_1, b_2), complementing the rows of the latter with respect to those of the former gives a GYD$(v, b_1, a_2v - b_2)$.

65.39 Theorem [1878] Let q be a prime power and $v = q^m$, $m \ge 2$. Then, for all integers $t_1, t_2 \ge 0$, there exists a GYD$(v, (t_1q + 1)q^{m-1}\frac{q^m-1}{q-1}, (t_2q + 1)q^{m-1}\frac{q^m-1}{q-1})$.

65.40 Remark Ash [115] gives explicit examples to show that, for $v \le 25$ and $b_1, b_2 \le 50$, the necessary conditions of Theorem 65.27 are sufficient except when $v = 15$ and $\{b_1, b_2\} = \{21, 35\}$ (since no BIBD(15,21,7,5,2) exists), and possibly when $v = 25$ and $b_1 = b_2 = 40$. In particular, she lists nonregular solutions for $(v, b_1, b_2) \in \{(4,6,6), (6,10,15), (6,15,20), (8,14,28), (8,28,28), (8,28,42), (9,12,12), (9,12,24), (9,24,24), (10,15,36), (10,18,45), (12,33,44), (16,20,20), (21,30,35), (25,30,30)\}$.

See Also

§II.1	Existence of BIBDs.
§II.6	Existence of symmetric designs.
[115]	A table of explicit solutions of GYDs for $v \le 25$, $b_1, b_2 \le 50$.
[419]	"Multi-letter" Youden rectangles.
[1759]	Comprehensive survey and bibliography for Youden squares.
[1760, 1761]	Together these give a basic account of double Youden rectangles.
[1764]	Basic details of Freeman–Youden rectangles.

References Cited: [115, 419, 1296, 1759, 1760, 1761, 1762, 1764, 1878, 2195]

Part VII

Related Mathematics

1 Codes

Vladimir D. Tonchev

1.1 A Brief Introduction to Coding Theory

1.1 A *code* C of *length* n over an alphabet F_q of size q (or a *q-ary* code) is a subset $C \subseteq F_q^n$ of the set of all n-tuples with components from F_q. A code is *binary* if $q = 2$, *ternary* if $q = 3$, and so on. If q is a prime power and F_q is the finite field $\mathbb{F}_q$ of order q, then *linear codes* are linear subspaces of the n-dimensional vector space $\mathbb{F}_q^n$. A k-dimensional subspace of $\mathbb{F}_q^n$ is a (linear) $[n, k]$ code over $\mathbb{F}_q$. The elements of a code are the *words* or the *codewords*.

1.2 A *generator matrix* of a linear $[n, k]$ code C is any matrix of rank k (over $\mathbb{F}_q$) with rows from C.

1.3 The *dual* (or *orthogonal*) code $C^\perp$ of a code C is its orthogonal space with respect to the usual dot product in $\mathbb{F}_q^n$:

$$C^\perp = \{\ y \in \mathbb{F}_q^n \mid yx = 0 \text{ for all } x \in C\}.$$

The dual code of an $[n, k]$ code is an $[n, n-k]$ code.

1.4 A *parity check matrix* of C is any generator matrix of $C^\perp$.

1.5 **Remark** If $G = (I_k, A)$ is a generator matrix of C, then $H = (-A^T, I_{n-k})$ is a generator matrix of $C^\perp$ or, equivalently, a parity check matrix of C.

1.6 The set F_q^n becomes a metric space when equipped with the *Hamming distance*:

$$d(x, y) = |\{\ i \mid x_i \neq y_i\ \}| \text{ for } x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n),\ x, y \in F_q^n.$$

1.7 The norm induced by the Hamming distance is the (Hamming) *weight*:

$$w(x) = d(x, \overline{0}) = |\{\ i \mid x_i \neq 0\}| \text{ for } x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n,$$

where $\overline{0} = (0, \ldots, 0)$ is the *zero* vector.

1.8 **Proposition** The Hamming distance is invariant under translation:

$$d(x + z, y + z) = d(x, y) \text{ for } x, y, z \in \mathbb{F}_q^n.$$

1.9 An important parameter of a code C is its *minimum distance* d where $d = \min_{x,y \in C,\ x \neq y} d(x, y)$, or equivalently, in the case of a linear code, its *minimum weight*: $d = \min_{x \in C,\ x \neq \overline{0}} w(x)$. An $[n, k, d]$ *code* is an $[n, k]$ code with minimum distance (or weight) d.

1.10 **Theorem** The minimum distance of a linear code with a parity check matrix H is d if and only if every $d - 1$ columns in H are linearly independent, and there is a set of d linearly dependent columns in H.

1.11 The *weight distribution* of a code C is the sequence $\{A_i\}_{i=0}^n$, where A_i is the number of codewords of weight i. The polynomial $A(x) = \sum_{i=0}^n A_i x^i$ is the *weight enumerator* of C.

1.12 **Theorem** (*MacWilliams identity*) Let C be an $[n, k]$ code over $\mathbb{F}_q$ with weight enumerator $A(x)$, and let $B(x)$ be the weight enumerator of $C^\perp$. Then

$$q^k B(x) = (1 + (q-1)x)^n A(\tfrac{1-x}{1+(q-1)x}).$$

1.13 Two codes are *equivalent* if one of the codes can be obtained from the other by permuting the coordinates (in all codewords) and permuting the symbols within one or more coordinate positions.

1.14 **Remark** Permutations of the symbols within a coordinate position that are realized by multiplication of a coordinate with a nonzero field element preserve the linearity of a code.

1.15 Two codes are *isomorphic* if they differ by a permutation of the coordinates only.

1.16 An *automorphism* of a code is any equivalence of the code with itself.

1.17 **Example** The rows of the matrices

$$C_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \end{pmatrix}, \; C_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 1 \\ 2 & 0 & 0 & 2 \end{pmatrix},$$

form equivalent (but not isomorphic) ternary codes of length $n = 4$ and minimum distance $d = 3$. The code C_2 is obtained from C_1 by interchanging the first two coordinate positions and applying the permutation $(0, 1, 2)$ on the symbols in the third position. Any permutation that fixes the first coordinate and permutes the coordinates $2, 3, 4$ arbitrarily is an automorphism of C_1. The code C_1 is linear (of dimension $k = 1$), while C_2 is nonlinear. The minimum weight of C_2 is 1. The weight enumerator of C_1 is $1 + 2x^3$.

1.18 A *sphere* of radius r about a vector $x \in F_q^n$ is the set of all n-tuples whose distance is at most r from x.

1.19 **Proposition** The spheres of radius $e = \lfloor \frac{d-1}{2} \rfloor$ about the codewords of a code with minimum distance d are disjoint.

1.20 **Remarks** The minimum distance determines the *error-correcting ability* of the code. More precisely, a code C with minimum distance d can correct up to $e = \lfloor \frac{d-1}{2} \rfloor$ errors, or C is an *e-error-correcting* code. Suppose that the codewords of C are used as communication messages that are transmitted via a noisy channel. The noise may result in random changes of the values of some coordinates in the transmitted words. Assume that the number of errors (the number of coordinates being changed) in any single codeword x does not exceed $e = \lfloor \frac{d-1}{2} \rfloor$, where d is the minimum distance. The errors in the received vector can be corrected by using the *maximum likelihood principle*: At the receiving end, consider any received word y as the image of the codeword from C that is closest to y in terms of the Hamming distance. By Proposition 1.19, the codeword x being sent is properly determined by this procedure provided that $d(x, y) \leq e$.

The length n, the minimum distance d, and the total number of codewords (or *size*) $M = |C|$ are the basic parameters of a code C. Increasing d is usually possible at the expense of decreasing M or increasing n. If d and M are fixed, the most interesting codes for the given d, M are those of shortest length n. If d and n are fixed, one looks for a code of largest possible size M.

In general, there are three fundamental optimization problems imposed by fixing two of the parameters n, d, M and optimizing with respect to the third. Explicit solutions of any of these optimization problems are rarely known in general. However, there are estimates (*bounds*) for the optimal values in terms of inequalities. On many occasions, the codes that are optimal with respect to a given bound are closely related to combinatorial designs. This chapter is a brief survey of such relations between codes and designs.

1.21 **Remark** The codes defined in this chapter are *block* codes, or fixed-length codes. There are other types of codes that allow codewords of variable length, or even streams of symbols rather than words of a fixed length. Such codes are not discussed here since the relationships between codes and combinatorial designs are best studied and understood in the case of block codes.

1.2 Designs in Codes

1.22 The *support* of a nonzero vector $x = (x_1, \ldots, x_n),\ x_i \in F_q = \{0, 1, \ldots, q-1\}$ is the set of indices of its nonzero coordinates: $supp(x) = \{\ i \mid x_i \neq 0\}$.

1.23 **Example** The support of any nonzero word in C_1 from Example 1.17 is $\{2, 3, 4\}$, while the support of the first codeword in C_2 is $\{3\}$.

1.24 The (*support*) *design* of a code of length n for a given nonzero weight w is the design with points the n coordinate indices and blocks the supports of all codewords of weight w.

1.25 **Example** The matrix G on the left is a generator matrix of a binary $[7, 4, 3]$ code (the *Hamming code* of length 7) with weight distribution $A_0 = A_7 = 1,\ A_3 = A_4 = 7$. The seven codewords of weight 3 form the incidence matrix given on the right of a 2-(7,3,1) design (the projective plane of order 2). The seven codewords of weight 4 support the complementary 2-(7,4,2) design.

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$\begin{array}{|ccccccc|} \hline 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline \end{array}$$

1.26 **Remark** To avoid repeated blocks in the nonbinary case ($q > 2$), only one support is taken for all words with the same support (for example, one support for all $q-1$ nonzero multiples of a word in a linear q-ary code). The regularity of a support design depends on the structure of the underlying code. For example, if the code is *cyclic*, that is, having the cyclic permutation $(1\ 2\ \ldots\ n)$ as an automorphism, the supports of any weight $w \neq 0$ form a 1-(n, w, r) design for some r.

1.27 **Theorem** If a code is invariant under a permutation group that acts t-homogeneously (in particular, t-transitively) on the coordinates, the supports of the codewords of any nonzero weight form a t-design.

1.28 **Remark** The Hamming code of Example 1.25 is cyclic. The full automorphism group of the code ($\mathrm{PSL}_3(2)$) is of order 168 and acts 2-transitively on the set of coordinates.

1.29 **Example** The *Reed–Muller* (RM) code $\mathrm{RM}(r, m)$ of order r $(0 \leq r \leq m)$ is a binary $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$ code consisting of all binary vectors of length 2^m that are value-vectors of polynomials in binary variables $v_1, \ldots, v_m$ of degree at most r. The dual code of $\mathrm{RM}(r, m)$ is $\mathrm{RM}(m-r-1, m)$. Any RM code is invariant under the 3-transitive group of all affine transformations of the 2^m-dimensional binary vector space. Consequently, the codewords of any fixed weight support a 3-design.

1.3 Perfect Codes

1.30 **Theorem** (*sphere packing or Hamming bound*) A q-ary code C of length n and minimum distance $d = 2e + 1$ satisfies

$$|C| \leq \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i}(q-1)^i}.$$

1.31 A code that attains the sphere packing bound is *perfect*. Equivalently, a code is perfect if the spheres of radius e around all codewords cover the whole space.

1.32 **Examples** Perfect codes.

- (The *trivial* perfect codes):
  - The whole space F_q^n is a perfect code with $e = 0$.
  - The zero vector and the all-one vector of odd length n form a binary perfect code with $e = \frac{n-1}{2}$.
  - The zero vector itself is a perfect code for $e = n$.
- *The binary Golay code* G_{23} is a linear $[23, 12, 7]$ code with a generator matrix being the circulant with first row the incidence vector of the (nonzero) quadratic residues modulo 23.
- *The ternary Golay code* G_{11} is a linear $[11, 6, 5]$ code with a generator matrix $A = \left(I_6 \begin{smallmatrix} 1 & 1 & 1 & 1 & 1 \\ & & C & & \end{smallmatrix}\right)$, where C is the circulant with first row $(0, 1, 2, 2, 1)$.
- *The Hamming code* over $\mathbb{F}_q$ is a linear $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3]$ code with a parity check matrix having as columns a set of representatives of all 1-dimensional subspaces of $\mathbb{F}_q^m$. In particular, the parity check matrix of the binary Hamming code of length $2^m - 1$ consists of all nonzero binary columns of length m.

1.33 If C is a code of length n over $\mathbb{F}_q$, the *extended* code $\overline{C}$ is

$$\overline{C} = \{(c_1, \ldots, c_n, c_{n+1}) \mid (c_1, \ldots, c_n) \in C,\ c_{n+1} = \textstyle\sum_{i=1}^{n} c_i\}.$$

Conversely, C is the *shortened* (or *punctured*) code of $\overline{C}$.

1.34 **Theorems** (Assmus and Mattson [123])

1. A linear $[n, k, d = 2e+1]$ code over $\mathbb{F}_q$ is perfect if and only if the support design of the minimum weight codewords is an $(e+1)$-$(n, 2e+1, (q-1)^e)$ design.
2. A binary (linear or nonlinear) code of length n and minimum distance $d = 2e+1$ that contains the zero vector is perfect if and only if the support design of the minimum weight codewords is a Steiner system $S(e+1, 2e+1, n)$. Moreover, the supports of the minimum weight codewords in the extended code form a Steiner system $S(e+2, 2e+2, n+1)$.

1.35 **Table** Perfect codes and their designs. The designs obtained from trivial perfect codes are trivial. The parameters of *all* nontrivial perfect codes and related designs are

e	q	n	Code	Design
1	Any prime power	$\frac{q^m-1}{q-1}$	Hamming code	2-$(\frac{q^m-1}{q-1}, 3, q-1)$
2	3	11	Ternary Golay code G_{11}	4-(11,5,1)
3	2	23	Binary Golay code G_{23}	4-(23,7,1)

1.36 **Remark** Theorem 1.34(1) guarantees only a 3-(11,5,4) design in the ternary Golay code G_{11}. Because G_{11} is invariant under the 4-transitive Mathieu group M_{11}, this 3-design is a 4-design by Theorem 1.27.

1.37 **Remark** The minimum weight vectors in the extended Golay codes $\overline{G_{11}}$ and $\overline{G_{23}}$ support a 5-(12,6,1) and a 5-(24,8,1) design, respectively. These codes and the related designs are invariant under the 5-transitive Mathieu groups M_{12} and M_{24}, respectively.

1.38 **Remark** The Hamming codes and the Golay codes are (up to equivalence) the only nontrivial linear perfect codes. Any (nontrivial) nonlinear perfect code over a finite field is a translate of either a Hamming or a Golay code, or is a single-error-correcting code ($e = 1$) with parameters of a Hamming code. There are many examples of nonlinear perfect codes with $e = 1$ (binary and nonbinary) that are not translates of the Hamming code [1505, 2046, 796, 1735, 1736].

1.39 **Remark** The extended code of the binary Hamming code of length $2^m - 1$ is the Reed–Muller code $\mathrm{RM}(m-2, m)$ of Example 1.29.

1.4 The Assmus–Mattson Theorem

1.40 **Remark** Theorem 1.41, proved by Assmus and Mattson in 1969, provides an important method for the construction of t-designs as support designs in linear codes with relatively few nonzero weights.

1.41 **Theorem** (*Assmus–Mattson theorem*) Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ and $C^\perp$ be the dual $[n, n-k, d^\perp]$ code. Denote by n_0 the largest integer $\leq n$ such that $n_0 - \frac{n_0+q-2}{q-1} < d$, and define $n_0^\perp$ similarly for the dual code $C^\perp$. Suppose that for some integer t, $0 < t < d$, there are at most $d - t$ nonzero weights w in $C^\perp$ such that $w \leq n - t$. Then, the support design:

1. for any weight u, $d \leq u \leq n_0$ in C is a t-design;
2. for any weight w, $d^\perp \leq w \leq min\{n - t, n_0^\perp\}$ in $C^\perp$ is a t-design.

1.42 **Remark** The largest value of t for any known t-design derived from a code via the Assmus–Mattson Theorem is $t = 5$. All such 5-designs come from self-dual codes (Table 1.61).

1.43 **Remark** Tanabe [2000] proves a version of the Assmus–Mattson Theorem for $\mathbb{Z}_4$-codes.

1.44 An $[n, k]$ code C is *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$. The length of a self-dual code is even and $n = 2k$. An $[n, \frac{n}{2}]$ code C is *formally* self-dual if C and $C^\perp$ have the same weight distribution.

1.45 **Remark** Self-orthogonal and, in particular, self-dual codes over $\mathbb{F}_2$ and $\mathbb{F}_3$, as well as some formally self-dual codes over $\mathbb{F}_4$, have regular gaps in their weight distribution: all weights are divisible by 2 if $q = 2$, by 3 if $q = 3$, and by 2 if $q = 4$ and $C^\perp$ coincides with the hermitian conjugate of C.

1.46 A code is *even* if all weights are even, and *doubly-even* if all weights are divisible by 4. A code is *singly-even* if it is even but not doubly-even.

1.47 **Remark** Binary doubly-even self-dual codes exist for any $n \equiv 0 \pmod 8$.

1.48 A self-dual code whose distance achieves equality in Theorem 1.49 is *extremal*.

1.49 **Theorem** The minimum distance d of a self-dual $[n, \frac{n}{2}]$ code C satisfies

$$d \leq \begin{cases} 2[\frac{n}{8}] + 2 & \text{if } q = 2 \text{ and } C \text{ is singly-even,} \\ 4[\frac{n}{24}] + 4 & \text{if } q = 2 \text{ and } C \text{ is doubly-even,} \\ 3[\frac{n}{12}] + 3 & \text{if } q = 3 \\ 2[\frac{n}{6}] + 2 & \text{if } q = 4 \text{ and } C \text{ is even.} \end{cases}$$

1.50 **Example** The matrix $(I_4, J_4 - I_4)$ generates an extremal binary $[8, 4, 4]$ doubly-even self-dual code with weight distribution $A_0 = A_8 = 1$, $A_4 = 14$. Because $d = 4$ and there is only one nonzero weight smaller than $n = 8$, the support design for weight $w = 4$ is a 3-design ($d - t = 4 - 3 = 1$), hence a 3-(8,4,1) design (the unique SQS(8)).

This code is equivalent to the extended Hamming code of Example 1.25, or the Reed–Muller code RM$(1,3)$ of Example 1.29, and the related 3-design can also be explained by Theorems 1.27 or 1.34(2).

1.51 Theorems

1. An extremal binary singly-even $[n, \frac{n}{2}]$ code yields 3-, 2-, or 1-designs provided that $n \equiv 0, 2$, or $4 \pmod 8$.
2. An extremal binary doubly-even $[n, \frac{n}{2}]$ code yields 5-, 3-, or 1-designs provided that $n \equiv 0, 8$, or $16 \pmod{24}$.
3. An extremal ternary code with $n \equiv 0 \pmod{12}$ yields 5-designs.
4. An extremal even quaternary code with $n \equiv 0 \pmod 6$ yields 5-designs.

1.52 Theorem [1278] If C is an extremal binary even formally self-dual code of length $n \equiv 2 \pmod 8$, then the words of any fixed weight in $C \cup C^{\perp}$ form a 3-design.

1.53 Remark Extremal self-dual codes can exist only for finitely many values of n, but the spectrum is unknown.

1.54 Construction (*quadratic residue (QR) codes*) Let $n = p$ be a prime and q be a quadratic residue modulo p. The quadratic residue code of length p over $\mathbb{F}_q$ is a $[p, \frac{1}{2}(p+1), d \geq \sqrt{p}]$ code with a generator matrix the zero-one circulant of order p with first row the incidence vector of the (nonzero) quadratic residues modulo p. If $p \equiv 3 \pmod 4$, the extended QR code is self-dual.

1.55 Examples

- The binary QR code for $p = 7$ is the Hamming code of Example 1.25.
- The binary QR code for $p = 23$ is the $[23, 12, 7]$ binary Golay code.
- The ternary QR code for $p = 11$ is the $[11, 6, 5]$ ternary Golay code.
- The binary extended QR code of length 18 ($p = 17$) is an extremal even $[18, 9, 6]$ formally self-dual code with weight distribution

  $$A_0 = A_{18} = 1,\ A_6 = A_{12} = 102,\ A_8 = A_{10} = 153.$$

  By Theorem 1.51(1), the words of any fixed weight form a 2-design. By Theorem 1.52, the union of the 102 words of weight 6 in the code and the 102 words of weight 6 in the dual code form a 3-design, hence, a 3-(18,6,5) design.

1.56 Construction (*Pless symmetry codes* [1749, 1750]) Let p be a prime and $Q = (q_{ij})_{p\times p} = (\chi(j-i))$ where χ is the Legendre symbol modulo p. Let S_p be the matrix displayed on the right. Then the *symmetry code* $C(p)$ is the $[2p+2, p+1]$ ternary code with generator matrix (I, S_p). The code $C(p)$ is self-dual if $p \equiv 2 \pmod 3$.

$$S_p = \begin{pmatrix} 0 & 1 & \dots & 1 \\ \chi(-1) & & & \\ \vdots & & Q & \\ \chi(-1) & & & \end{pmatrix}$$

1.57 Remark The symmetry code $C(11)$ is equivalent to the extended ternary Golay code.

1.58 Construction (*self-dual codes from Hadamard matrices* [2048, 1054]) Let H be a Hadamard matrix of order $n = 8t + 4$ such that the number of $+1$s in each row is congruent to $s \pmod 4$, s odd. Then $(I, (H + J)/2)$ is a generator matrix of a binary self-dual $[2n, n]$ code. The code is singly-even if $s = 1$, and doubly-even if $s = 3$.

1.59 Examples

1. The Hadamard matrix of order 4 produces the extended Hamming $[8, 4, 4]$ code of Example 1.50.
2. The Hadamard matrix of order 12 yields the extended Golay $[24, 12, 8]$ code [2048].

3. The three inequivalent Hadamard matrices of order 20 produce 118 inequivalent doubly-even extremal $[40, 20, 8]$ codes [2048, 406], and 6 singly-even $[40, 20, 8]$ codes [1054].
4. The Paley matrix of order 28 produces 5 inequivalent extremal doubly-even $[56, 28, 12]$ codes [405, 1299].

1.60 **Remark** For other constructions of extremal self-dual codes from combinatorial designs, see [245, 1752, 1948, 2047, 2049].

1.61 **Table** 5-designs from self-dual codes.

Design	Code	Comments
5-(12,6,1)	$[12, 6, 6]$, $q = 3$	Extended ternary Golay code
5-(18,8,6) 5-(18,10,180)	$[18, 9, 8], q = 4$	Extended cyclic code [1504]
5-(24,8,1) 5-(24,12,48)	$[24, 12, 8]$, $q = 2$	Extended binary Golay code
5-(24,9,6) 5-(24,12,576) 5-(24,15,8580)	$[24, 12, 9]$, $q = 3$	Extended QR code, Pless symmetry code $C(11)$
5-(24,10,36) 5-(24,12,1584) 5-(24,12,1632)	$[24, 12]$, $\mathbb{Z}_4$	Lifted Golay $\mathbb{Z}_4$-code [992] Lifted Golay $\mathbb{Z}_4$-code [1049] Lifted Golay $\mathbb{Z}_4$-code [1049]
5-(30,12,220) 5-(30,14,5390) 5-(30,16,123000)	$[30, 15, 12]$, $q = 4$	Extended QR code
5-(36,12,45) 5-(36,15,5577) 5-(36,18,209685) 5-(36,21,2438973)	$[36, 18, 12]$, $q = 3$	Pless symmetry code $C(17)$
5-(48,12,8) 5-(48,16,1365) 5-(48,20,36176) 5-(48,24,190680)	$[48, 24, 12]$, $q = 2$	Extended QR code
5-(48,15,364) 5-(48,18,50456) 5-(48,21,2957388) 5-(48,24,71307600) 5-(48,27,749999640)	$[48, 24, 15]$, $q = 3$	Extended QR code, Pless symmetry code $C(23)$
5-(60,18,3060) 5-(60,21,449820) 5-(60,24,34337160) 5-(60,27,1271766600) 5-(60,30,24140500956) 5-(60,33,239329029060)	$[60, 30, 18]$, $q = 3$	Pless symmetry code $C(29)$, Extended QR code

1.5 Nonlinear Codes and Designs

1.62 An (n, M, d) *code* is a binary code C of length n, minimum distance d, and size $M = |C|$.

1.63 The *distance distribution* of an (n, M, d) code C is the sequence $\{B_i\}_{i=0}^n$ where B_i is the number of ordered pairs of codewords at distance i apart, divided by M.

1.64 **Remark** The distance and weight distribution of a linear code coincide.

1.65 The *MacWilliams transform* $\{B'_i\}_{i=0}^n$ of the distance distribution $\{B_i\}_{i=0}^n$ of an (n, M, d) code C is defined by the identity

$$2^n \sum_{j=0}^n B_j x^j = M \sum_{i=0}^n B'_i (1+x)^{n-i}(1-x)^i.$$

Let $\sigma_1 < \sigma_2 < \ldots < \sigma_{s'}$ be the nonzero subscripts i for which $B'_i \neq 0$. Then $d' = \sigma_1$ is the *dual distance* of C, and s' is the *external distance* of C.

1.66 **Remark** If $\{B_i\}_{i=0}^n$ is the distance distribution of a linear code C, then $\{B'_i\}_{i=0}^n$ is the weight distribution of the dual code $C^\perp$ (see Theorem 1.12).

1.67 **Theorem** [674] Let s be the number of distinct nonzero distances in an (n, M, d) code C with distance distribution$\{B_i\}_{i=0}^n$ such that $\overline{0} \in C$. Let $\overline{s} = s$ if $B_n = 0$ and $\overline{s} = s - 1$ if $B_n = 1$.

1. If $\overline{s} < d'$, then the codewords of any weight $w \geq d' - \overline{s}$ in C form a $(d' - \overline{s})$-design.
2. If $d - s' \leq s' < d$, the codewords of any fixed weight form a $(d - s')$-design.

1.68 **Construction** (*Nordstrom–Robinson or Semakov–Zinov'ev code* [1505]) The codewords in the extended binary $[24, 12, 8]$ Golay code that have at most one nonzero coordinate among the 8 nonzero positions of a given minimum weight codeword, after deleting those 8 coordinates, form a nonlinear (16,256,6) code with weight and distance distribution $B_0 = B_{16} = 1$, $B_6 = B_{10} = 112$, $B_8 = 30$, and MacWilliams transform $\{B'_i = B_i\}$. Hence, $d = d' = 6$, $s = s' = 4$, and by Theorem 1.67(1), the nonzero codewords support 3-designs (with parameters 3-(16,6,4), 3-(16,8,3), and 3-(16,10,24)).

1.69 **Theorem** For any binary $(n, M, d = 2t + 1)$ code

$$M \leq \frac{2^n}{\sum_{i=0}^t \binom{n}{i} + \frac{1}{\lfloor n/(t+1) \rfloor} \binom{n}{t} \left(\frac{n-t}{t+1} - \left\lfloor \frac{n-t}{t+1} \right\rfloor \right)}.$$

1.70 A binary code for which equality holds in Theorem 1.69 is *nearly perfect*.

1.71 **Remark** If $t + 1$ divides $n + 1$, then the bound of Theorem 1.69 coincides with the sphere packing bound of Theorem 1.30. Thus, any perfect code is also nearly perfect.

1.72 **Theorem**

1. The minimum weight codewords in a nearly perfect $(n, M, d = 2t + 1)$ code C that contains the zero vector form a t-$(n, 2t + 1, [(n - t)/(t + 1)])$ design.
2. The minimum weight codewords in the extended code $\overline{C}$ form a $(t + 1)$-$(n + 1, 2t + 2, [(n - t)/(t + 1)])$ design.

1.73 **Remark** The code of Construction 1.68 is the first member of an infinite class of nonlinear binary codes, *Preparata codes*. The shortened Preparata codes are nearly perfect; thus, the minimum weight vectors yield designs via Theorem 1.72. By Theorem 1.67, the codewords of any other weight also yield designs.

1.74 **Remark** The nearly perfect codes are a subclass of a more general class of *uniformly packed codes* (see [1882, 162, 922, 2093] and [424, Ch. 16]) that also yield designs via Theorem 1.67. The Goethals code C (Table 1.75) is a nonlinear uniformly packed code.

1.75 Table Some nonlinear binary codes that yield 3-designs.

(n, M, d)	Weight w	Comment
$(2^m, 2^{2^m-m-1}, 4)$	even $w \geq 4$	Extended perfect code
$(4^m, 2^{4^m-4m}, 6)$	even $w \geq 6$	Preparata code [1505]
$(4^m, 2^{4m}, 2^{2m-1} - 2^{m-1})$	$2^{2m-1} \pm 2^{m-1}$ 2^{2m-1}	Kerdock code [1505]
$(4^m, 2^{4^m-6m+1}, 8)$	even $w \geq 8$	Goethals code C [916]
$(4^m, 2^{6m-1}, 2^{2m-1} - 2^m)$	$2^{2m-1} \pm 2^m$ $2^{2m-1} \pm 2^{m-1}$ 2^{2m-1}	Goethals code D [916]

1.76 Remark The Preparata and Kerdock codes for $m = 2$ coincide with the code of Construction 1.68.

1.77 Remark The Preparata, Kerdock, and Goethals codes were found in the 1970s as nonlinear binary codes that contained more codewords than any linear binary code of the same length and minimum distance. In addition, the distance distribution of the Preparata and Kerdock codes, as well as those of the Goethals codes C and D, of Table 1.75 are related by the MacWilliams transform as they are dual linear codes (see Theorem 1.12). Some Preparata and Kerdock codes, as well as the Goethals codes, can be viewed as binary images of linear codes over the ring $\mathbb{Z}_4$, and the corresponding linear codes over $\mathbb{Z}_4$ are indeed dual codes [1032].

1.78 Remark The paper [1091] by Helleseth, Rong, and Yang contains an excellent survey on t-designs arising from codes over $\mathbb{Z}_4$. This includes several infinite series of 3-designs and some 5-designs.

1.79 Remark The 3-designs supported by codewords of weight 8 in the Goethals code over $\mathbb{Z}_4$ were used by Ranto [1774] for the construction of several infinite families of 3-designs with various values of λ. One such family has parameters 3-$(2^m, 8, \frac{14}{3}(2^m - 8))$ for all odd $m \geq 5$.

1.80 Theorem [128] Let D be the 3-$(4^m, 6, \frac{1}{3}(4^m - 4))$ design formed by the minimum weight words in the Preparata code.

1. The 4-subsets of coordinate indices that are not covered by any block of D form a Steiner system $S = S(3, 4, 4^m)$.
2. The 3-$(4^m, 4, 2)$ design S^* consisting of two identical copies of S is extendible to a 4-$(4^m + 1, 5, 2)$ design F by adding one new point to all blocks of S^* and adding, as further new blocks, all 5-subsets that are contained in blocks of D.

1.81 Remark The class of 4-designs of Theorem 1.80(2) is the only known infinite class of 4-designs derived from codes. Although these designs contain repeated blocks, they provide an infinite class of 4-designs with the smallest known fixed λ $(= 2)$.

A slight modification of the construction yields Steiner 4-wise balanced designs with blocks of size 5 and 6.

1.82 Theorem [2051] The minimum weight vectors in the Preparata code together with the blocks of the Steiner system $S(3, 4, 4^m)$ from Theorem 1.80, extended by one new point, yield a Steiner system $S(4, \{5, 6\}, 4^m + 1)$.

1.6 Codes with Majority Decoding

1.83 A linear code whose dual code supports the blocks of a t-design (see §1.2) admits one of the simplest decoding algorithms, *majority decoding*. Essentially, for each symbol y_i of the received codeword $y = (y_1, \ldots, y_n)$, a set of values $y_i^{(j)}$, $j = 1, \ldots, r$ of certain linear functions defined by the blocks of the design are computed, and the "true" value of y_i is decided to be the one that appears most frequently among $y_i^{(1)}, \ldots, y_i^{(r)}$.

1.84 **Theorem** [1771] Assume that the dual code of a linear code C supports a t-(n, w, λ) design $\mathcal{D}$ ($t \geq 2$). Let $A_l = \sum_{j=0}^{l-1} (-1)^j \binom{l-1}{j} \lambda_{j+2}$, where $\lambda_i = \lambda \binom{n-i}{t-i} / \binom{w-i}{t-i}$, $(0 \leq i \leq t)$ is the number of blocks of $\mathcal{D}$ containing a set of i fixed points. Define further

$$A'_l = \begin{cases} A_l & \text{if} \quad l \leq t-1, \\ A_{t-1} & \text{if} \quad l > t-1. \end{cases}$$

Then C can correct up to l errors by majority decoding, where l is the largest integer that satisfies the inequality $\sum_{i=1}^{l} A'_i \leq \lfloor (\lambda_1 + A'_l - 1)/2 \rfloor$. In particular, if $t = 2$, the code can correct up to $l \leq \lfloor (r + \lambda - 1)/(2\lambda) \rfloor$ errors by majority decoding, where $r = \lambda(n-1)/(w-1)$ [1831].

1.85 **Remark** One way to construct a code over $\mathbb{F}_p$ whose dual code contains designs is to start with a given t-(v, k, λ) design and consider the code having the block-by-point incidence matrix A of that design as a parity check matrix. The number of errors correctable by majority decoding is determined by the design parameters, while the dimension of the code is $v - rank_p A$, where $rank_p A$ (the *p-rank* of A) is the rank of A over $\mathbb{F}_p$.

1.86 **Theorem** [1023] Let A be the incidence matrix of a 2-design with parameters v, k, λ, r, b, and let p be a prime.

1. If p does not divide $r(r - \lambda)$, then $rank_p A = v$.
2. If p divides r but does not divide $r - \lambda$, then $rank_p A \geq v - 1$.
3. If $rank_p A < v - 1$, then p divides $r - \lambda$.

1.87 **Table** Small 2-(v, k, λ) designs and their p-ranks. N_d denotes the number of nonisomorphic designs for the given parameters, and l is the number of correctable errors (Theorem 1.84). The designs 1, 3, 6, 12 are finite desarguesian projective planes, while 2, 5, 11 are finite affine planes (see §VII.2).

No.	v	k	λ	r	N_d	# errors l	$r - \lambda$	p	$\rho = rank_p A$	$dim C = v - \rho$
1	7	3	1	3	1	1	2	2	4	3
2	9	3	1	4	1	2	3	3	6	3
3	13	4	1	4	1	2	3	3	7	6
4	6	3	2	5	1	1	3	3	5	1
5	16	4	1	5	1	2	4	2	9	7
6	21	5	1	5	1	2	4	2	10	11
7	11	5	2	5	1	1	3	3	6	5
8	13	3	1	6	2	3	5	5	13	0
9	7	3	2	6	4	1	4	2	4,5,6,7	3,2,1,0
10	10	4	2	6	3	1	4	2	5,6,7	5,4,3
11	25	5	1	6	1	3	5	5	15	10
12	31	6	1	6	1	3	5	5	16	15
13	16	6	2	6	3	1	4	2	6,7,8	10,9,8
14	15	3	1	7	80	3	6	2	$11 \leq \rho \leq 15$	$0 \leq dim \leq 4$
15	8	4	3	7	4	1	4	2	4,5,6,7	4,3,2,1

1.88 **Remark** The p-ranks of the geometric designs defined by the points and subspaces of a given dimension in a finite projective or affine space have been determined [917, 1023, 1503, 1930]. Theorem 1.89 gives the ranks of the designs formed by the hyperplanes in a finite projective or affine space.

1.89 **Theorem** Let $q = p^m$, p prime.

1. The p-rank of the 2-$(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1})$ design formed by the hyperplanes in the n-dimensional projective space $\mathrm{PG}(n,q)$ over $\mathbb{F}_q$ is $\binom{p+n-1}{n}^m + 1$.
2. The p-rank of the 2-$(q^n, q^{n-1}, \frac{q^{n-1}-1}{q-1})$ design formed by the hyperplanes in the n-dimensional affine space $\mathrm{AG}(n,q)$ over $\mathbb{F}_q$ is $\binom{p+n-1}{n}^m$.

1.90 **Remark** Among the 80 (15,3,1) designs (or STS(15)s) (Table 1.87, No. 14), there is a unique design with minimal 2-rank 11, being the geometric design formed by the lines in $\mathrm{PG}(3,2)$. The binary code generated by this design is equivalent to the Hamming code of length 15 (see §1.3). Similarly, the 2-(8,4,3) design with minimal 2-rank 4 (Table 1.87, No. 15) is a geometric design formed by the planes in $\mathrm{AG}(3,2)$.

1.91 **Conjecture** (Hamada [1023]) The p-rank of any design $\mathcal{D}$ with the parameters of a geometric design $\mathcal{G}$ in $\mathrm{PG}(n,q)$ or $\mathrm{AG}(n,q)$ $(q = p^m)$ is at least the p-rank of $\mathcal{G}$, with equality if and only if $\mathcal{D}$ is isomorphic to $\mathcal{G}$.

1.92 **Remark** Hamada's conjecture is true for the hyperplane design in a binary affine or projective space [1025], the design of the lines in a binary projective or a ternary affine space (STS($2^n - 1$) or STS(3^n)) [746], and the design of the planes in a binary affine space (SQS(2^m)), [2044]. The only known parameters for which there is more than one design with the same rank as a geometric design (hence, showing that the "only if" part of the Hamada's conjecture is not true in general) are 2-(31,7,7) ($\mathrm{PG}(4,2)$), 2-(32,8,35) (or 3-(32,8,7), $\mathrm{AG}(5,2)$) [2043], and 2-(64,16,5) ($\mathrm{AG}(3,4)$) [1050, 1560]. All these designs arise from codes; see Examples 1.99 and 1.102.

1.93 A *generalized incidence matrix* of a design $\mathcal{D}$ over $\mathbb{F}_q$ is any matrix obtained from the $(0,1)$-incidence matrix A of $\mathcal{D}$ by replacing nonzero entries of A with nonzero elements from $\mathbb{F}_q$.

1.94 **Remark** A revised version of Hamada's conjecture was proved in [2054] for the designs having the same parameters as the complementary designs of the classical geometric designs with blocks being hyperplanes in a projective or affine space.

1.95 **Theorem** [2054] The q-rank d of a generalized incidence matrix over $\mathbb{F}_q$ of a 2-$(\frac{q^{n+1}-1}{q-1}, q^n, q^{n-1})$ design $(n \geq 2)$ is at least $n+1$. The equality $d = n+1$ holds if and only if the design is isomorphic to the complementary design of the geometric design having as blocks the hyperplanes in $PG(n,q)$.

1.96 **Theorem** [2054] The q-rank d of a generalized incidence matrix over $\mathbb{F}_q$ of a 2-$(q^n, q^n - q^{n-1}, q^n - q^{n-1} - 1)$ design $(n \geq 2)$ is at least $n+1$. The equality $d = n+1$ holds if and only if the design is isomorphic to the complementary design of the geometric design having as blocks the hyperplanes in $\mathrm{AG}(n,q)$.

1.7 Designs, Intersection Numbers, and Codes

1.97 **Remark** Linear codes provide a powerful tool for the study of designs having constant block intersection numbers modulo some prime p, in particular, symmetric and quasi-symmetric designs (see §II.6 and §VI.48), both for their construction and for deriving necessary conditions for their existence.

1.98 Theorems [2043, 2044] Assume that $\mathcal{D}$ is a 2-(v, k, λ) design with block intersection numbers $s_1, s_2, \ldots, s_m$. Denote by C the binary code spanned by the block-by-point incidence matrix of $\mathcal{D}$ and by $\overline{C}$, the extended binary code.

1. If $k, s_1, \ldots, s_m$ are all even, then C is self-orthogonal.
2. If $v, k, s_1, \ldots, s_m$ are all odd, then $\overline{C}$ is self-orthogonal.
3. If $v, k, s_1, \ldots, s_m$ are all even, then C is contained in a length v self-dual code.
4. If $v \equiv 0 \pmod 8$, $k \equiv 0 \pmod 4$ and $s_1, \ldots, s_m$ are all even, then C is contained in a doubly-even self-dual code of length v.
5. If $v \equiv 7 \pmod 8$, $k \equiv 3 \pmod 4$ and $s_1, \ldots, s_m$ are all odd, then $\overline{C}$ is contained in a doubly-even self-dual code of length $v + 1$.
6. The dual code $C^\perp$ has minimum distance $d^\perp \geq (r + \lambda)/\lambda$.
7. The dual of the extended code $\overline{C}^\perp$ has minimum distance
$$\overline{d}^\perp \geq \min\{(b + r)/r, (r + \lambda)/\lambda\}.$$

1.99 Example [2043] Assume that $\mathcal{D}$ is a quasi-symmetric 2-(31,7,7) design with intersection numbers $x = 1, y = 3$ (an example being the design of the planes in the binary projective 4-space, PG(4, 2)). By Theorem 1.98, 5 and 7, $\overline{C}^\perp$ is contained in a *doubly-even* self-dual $[32, 16, D]$ code with minimum distance $D \geq \overline{d}^\perp \geq 5$, hence $D \geq 8$. On the other hand, $D \leq 8$ for any self-dual doubly-even [32,16] code by Theorem 1.49. Thus $\overline{C}^\perp$ is contained in an extremal doubly-even [32,16,8] code. Up to equivalence, there are precisely five such codes [600], one of these five codes being the Reed–Muller code RM(3, 5) (see Example 1.29). Any doubly-even self-dual [32,16,8] code contains exactly 620 codewords of minimum weight 8 that support a 3-(32,8,7) design (with intersection numbers 0, 2, 4) by Theorem 1.41. Therefore, any quasi-symmetric 2-(31,7,7) design is a derived design of a 3-(32,8,7) design supported by a doubly-even extremal [32,16,8] code. Consequently, because the five doubly-even [32,16,8] codes all have transitive automorphism groups [600] and are generated by their minimum weight codewords, there are exactly five nonisomorphic quasi-symmetric 2-(31,7,7) designs with intersection numbers $x = 1, y = 3$. Similarly, there are exactly 5 nonisomorphic 3-(32,8,7) designs with intersection numbers 0, 2, 4.

1.100 Example [2043] The 5-(48,12,8) design supported by the minimum weight codewords in the extended binary QR code, being a doubly-even self-dual [48,24,12] code (see Table 1.61), has intersection numbers 0, 2, 4, 6. The derived design consisting of all blocks through a given triple of points, after having that triple deleted, is a 2-(45,9,8) design with intersection numbers 1, 3, that is, a quasi-symmetric design with $x = 1, y = 3$.

1.101 Remark A doubly-even self-dual [48,24,12] code is unique up to isomorphism [1137]. The uniqueness of this code implies that a self-orthogonal 5-(48,12,8) design, as well as its derived and residual designs, including the quasi-symmetric 2-(45,9,8) design, are all unique up to isomorphism [1052].

1.102 Example A class of self-orthogonal 1-(64,16,16) designs such that every two blocks are either disjoint or meet in four points, and every two points occur together in either none or four blocks, were enumerated recently in [1050]. The classical example of such design is obtained by taking a collection of planes in AG(3, 4) that do not contain any line from a given parallel class of lines. The incidence matrix of any such design spans a self-orthogonal binary code of length 64. Among these codes, one finds the geometric code spanned by the planes in AG(3, 4), as well as two other inequivalent codes that support affine 2-(64,16,5) designs having the same 2-rank (equal to 16) as

the classical design in AG$(3, 4)$, thus providing new counter-examples to the "only if"-part of Hamada's conjecture [1050].

1.103 Example [1151] Table 1.104 contains two generating permutations and the base blocks of a quasi-symmetric 2-(49,9,6) design with $x = 1, y = 3$. The extended code $\overline{C}$ is a self-dual [50,25,10] code, which is extremal with respect to an improved bound for self-dual codes given in [602]. The minimum weight codewords correspond to the incidence vectors of the blocks extended by an overall parity check. The weight enumerator of the code is $A(x) = 1+196x^{10}+11368x^{12}+31752x^{14}+\cdots$. Other quasi-symmetric 2-(49,9,6) designs were obtained recently from other extremal [50,25,10] codes in [312, 1051].

1.104 Table A quasi-symmetric 2-(49,9,6) design with an automorphism group of order 21.

Generating permutations:
$\varphi = (1\ \ 2\ \ \ldots\ \ 7)(8\ \ 9\ \ \ldots\ \ 14)\cdots(43\ \ 44\ \ \ldots\ \ 49)$;
$\psi = (1\ 8\ 22)(2\ 12\ 24)(3\ 9\ 26)(4\ 13\ 28)\ (5\ 10\ 23)\ (6\ 14\ 25)(7\ 11\ 27)$
$(15)(16\ 19\ 17)(18\ 20\ 21)(29\ 46\ 37)(30\ 43\ 39)(31\ 47\ 41)(32\ 44\ 36)$
$(33\ 48\ 38)(34\ 45\ 40)(35\ 49\ 42)$
Base blocks:
1 3 7 16 33 34 39 45 46; 4 5 6 12 14 22 30 32 33; 4 13 15 24 29 36 44 45 49;
5 6 9 19 21 25 30 34 36; 14 15 23 27 31 34 35 40 42; 1 9 11 16 17 19 33 35 36;
3 4 8 9 10 15 29 37 41; 1 2 4 11 16 25 31 39 43; 3 8 15 17 21 28 32 38 43;
32 34 35 39 41 42 46 48 49; 4 7 12 14 25 26 35 40 43; 5 8 15 19 20 27 34 37 43.

1.105 Example [1659] Table 1.106 lists the base blocks and generating permutations for a quasi-symmetric 2-(56,16,6) design with block intersection numbers $x = 4,\ y = 6$, supported by codewords of weight 16 in a self-orthogonal binary code of length 56 spanned by the blocks of a quasi-symmetric design with the same parameters originally found in [2045] by using subgroups of the Mathieu group M_{22}. This code contains a total of 152,425 vectors of weight 16.

1.106 Table A quasi-symmetric 2-(56,16,6) design.

Generating permutations
$\alpha = (2\ 3\ 5)(4\ 7\ 6)(8\ 15\ 22)(9\ 17\ 26)(10\ 19\ 23)(11\ 21\ 27)(12\ 16\ 24)$ $(13\ 18\ 28)(14\ 20\ 25)(30\ 31\ 33)(32\ 35\ 34)(36\ 43\ 50)(37\ 45\ 54)$ $(38\ 47\ 51)(39\ 49\ 55)(40\ 44\ 52)(41\ 46\ 56)(42\ 48\ 53)$
$\beta = (2\ 23)(3\ 10)(4\ 25)(5\ 19)(6\ 20)(7\ 14)(9\ 16)(11\ 18)(12\ 26)(13\ 27)$ $(17\ 24)(21\ 28)(30\ 51)(31\ 38)(32\ 53)(33\ 47)(34\ 48)(35\ 42)(37\ 44)$ $(39\ 46)(40\ 54)(41\ 55)(45\ 52)(49\ 56)$
$\gamma = (1\ 8)(3\ 24)(4\ 11)(5\ 26)(6\ 20)(7\ 21)(10\ 17)(12\ 19)(13\ 27)(14\ 28)$ $(15\ 22)(18\ 25)(29\ 36)(31\ 52)(32\ 39)(33\ 54)(34\ 48)(35\ 49)(38\ 45)$ $(40\ 47)(41\ 55)(42\ 56)(43\ 50)(46\ 53)$

Base blocks:	orbit length
1 8 15 22 32 34 35 39 41 42 46 48 49 53 55 56	1
11 14 20 21 25 27 29 32 34 35 36 41 43 46 50 56	2
7 14 21 28 30 32 33 37 39 40 44 46 47 51 53 54	3
3 10 17 24 29 33 35 36 40 42 43 47 49 50 54 56	3
5 7 8 14 15 19 29 31 33 35 38 42 45 47 50 52	6
3 13 17 19 20 26 32 38 39 41 46 47 48 52 53 54	6
1 2 14 15 22 24 25 26 27 31 36 39 44 47 48 49	8
2 9 10 11 13 16 21 22 26 31 33 42 44 46 48 50	24
1 2 6 7 10 11 13 19 27 35 36 37 38 40 53 55	24

1.107 Remark By further exploration of the relationship between quasi-symmetric designs and self-dual codes (Theorem 1.98(4,5)), and an appropriate generalization for codes over other fields, one obtains numerical necessary conditions for the existence of 2-designs with constant block intersection numbers modulo some prime, in particular, quasi-symmetric designs.

1.108 Theorem [410] Let $\mathcal{D}$ be a 2-(v, k, λ) design with intersection numbers $s_1 \equiv s_2 \equiv \ldots \equiv s_m \equiv s \pmod 2$. Then

1. $r \equiv \lambda \pmod 4$;
2. $s \equiv 0 \pmod 2$, $k \equiv 0 \pmod 4$, $v \equiv \pm 1 \pmod 8$; or
3. $s \equiv 1 \pmod 2$, $k \equiv v \pmod 4$, $v \equiv \pm 1 \pmod 8$.

1.109 Theorem [411] Let p be an odd prime and let $\mathcal{D}$ be a 2-(v, k, λ) design with intersection numbers $s_1 \equiv s_2 \equiv \ldots \equiv s_m \equiv s \pmod p$. Then either

1. $r \equiv \lambda \pmod{p^2}$;
2. $v \equiv 0 \pmod 2$, $v \equiv k \equiv s \equiv 0 \pmod p$, $(-1)^{\frac{v}{2}}$ is a square in $\mathbb{F}_p$;
3. $v \equiv 1 \pmod 2$, $v \equiv k \equiv s \not\equiv 0 \pmod p$, $(-1)^{\frac{v-1}{2}}$ is a square in $\mathbb{F}_p$; or
4. $r \equiv \lambda \equiv 0 \pmod p$, and
   (a) $v \equiv 0 \pmod 2$, $v \equiv k \equiv s \not\equiv 0 \pmod p$;
   (b) $v \equiv 0 \pmod 2$, $k \equiv s \not\equiv 0 \pmod p$, v/s is a nonsquare in $\mathbb{F}_p$;
   (c) $v \equiv 1 \pmod{2p}$, $r \equiv 0 \pmod{p^2}$, $k \equiv s \not\equiv 0 \pmod p$;
   (d) $v \equiv p \pmod{2p}$, $k \equiv s \equiv 0 \pmod p$;
   (e) $v \equiv 1 \pmod 2$, $k \equiv s \equiv 0 \pmod p$, v is a nonsquare in $\mathbb{F}_p$; or
   (f) $v \equiv 1 \pmod 2$, $k \equiv s \equiv 0 \pmod p$, v and $(-1)^{\frac{v-1}{2}}$ are squares in $\mathbb{F}_p$.

1.110 Table Some nonexistent quasi-symmetric designs ruled out by Theorems 1.108 and 1.109.

Number	v	k	λ	r	s_1	s_2	Theorem
1	21	9	12	30	3	5	1.108
2	21	8	14	40	2	4	1.108
3	35	7	3	17	1	3	1.108
4	41	17	34	85	5	8	1.109
5	43	18	51	126	6	9	1.109
6	51	21	14	35	6	9	1.109
7	51	15	7	25	3	5	1.108
8	57	27	117	252	12	17	1.109
9	57	24	23	56	9	12	1.109
10	69	33	176	374	15	21	1.108

1.111 Remark Theorems 1.108 and 1.109 apply to any symmetric 2-(v, k, λ) design, but are no more restrictive than the Bruck–Ryser–Chowla Theorem (see §II.6.2).

1.112 The *orbit matrix* $M = (m_{ij})$ of a 2-(v, k, λ) design $\mathcal{D}=(X, \mathcal{B})$ with respect to an automorphism group G is an integral matrix with rows indexed by the orbits of G on the point set X and columns indexed by the orbits of G on the block set $\mathcal{B}$, where m_{ij} is the number of points from the ith point orbit contained in a fixed block from the jth block orbit.

1.113 Theorem If G is a cyclic group of a prime order p that does not fix any point or block and $p|r - \lambda$, then the rows of the orbit matrix M generate a self-orthogonal code over $\mathbb{F}_p$.

1.114 Remark Theorem 1.113 can be used for finding orbit matrices of designs by means of codes [1751, 2040]. Theorem 1.115, due to Anstee, Hall, and Thompson [102] and

Bridges, Hall, and Hayden [326] (see also [1016], Ch. 17), combined with Theorem 1.12, is especially useful in the study of automorphisms of symmetric designs and finite planes, as well as for the construction of self-dual codes with given automorphism of a prime order [601, 1150].

1.115 Theorem Let V be an n-dimensional vector space over a field F. Assume that G is a permutation group on the coordinates of V and that $|G|$ has an inverse in F. Suppose that $C \subseteq V$ is a G module and $\Theta = \frac{1}{|G|}\sum_{g\in G} g,\ H = C\Theta,\ W = V\Theta$. Then with an appropriate orthonormal basis for W, $(C\Theta)^{\perp}_{W} = H^{\perp}_{W} = (C^{\perp})\Theta$.

1.8 Steiner Triple Systems and Linear Codes

1.116 Given a design $\mathcal{D}$ with v points and b blocks and a point by block $(v \times b)$ incidence matrix A, the *code of points* (or *point code*) of $\mathcal{D}$ over $\mathbb{F}_p$ is the linear span of the rows of A over $\mathbb{F}_p$, while the *code of blocks* is the linear span of the columns of A. The point code is of length b, while the code of blocks has length v. The dimension of either code is $rank_p A$.

1.117 Remark Most known results about codes of designs, including Theorem 1.41, are about codes spanned by the blocks. The notion of a code of blocks or points is essentially the same if the design is symmetric ($v = b$). However, if the design is not symmetric, the information provided by these two codes may differ significantly.

1.118 Remark An important step in the study of the code of a design is the computation of the dimension (see Theorem 1.86). The p-rank of a Steiner triple system is determined by Theorem 1.119 due to Doyen, Hubaut, and Vandensavel [746] using the projective and affine dimension as defined by Teirlinck [2010].

1.119 Theorem The p-rank of the incidence matrix of an STS(v), S, is

1. v if p is a prime greater than 3,
2. $v - d_P - 1$ if $p = 2$ and d_P is the projective dimension of S, and
3. $v - d_A - 1$ if $p = 3$ and d_A is the affine dimension of S.

1.120 Remark The computation of the binary codes of Steiner triple systems on 15 or fewer points [2061] showes that nonisomorphic STS(v)s generate inequivalent point codes (see Tables 1.129, 1.131). At the same time, the point code of a given Steiner triple system on v points may and does sometimes contain several nonisomorphic systems with incidence matrices formed by codewords of weight $r = (v-1)/2$ (Table 1.129). In contrast, the binary codes generated by the blocks of any two systems with the same parameters and 2-rank are equivalent (see Table 1.130). The latter is a general property of the binary codes of blocks of Steiner triple systems.

1.121 Theorem [121] Any two Steiner triple systems on v points with the same 2-rank have equivalent binary codes of blocks.

1.122 Remark The binary code of blocks of a given S = STS(v) can be used for the construction of all STS(v)s having the same 2-rank as S [121]. The data from Tables 1.129 and 1.131 and some further results from [129] suggest that the binary point codes of nonisomorphic Steiner triple systems are inequivalent. However, this is not true, in general; there are examples of nonisomorphic STS(19) that have equivalent point codes [1269].

1.123 Remark The results of [746, 2010] imply that the 2-rank of an STS($2^n - 1$) or an SQS(2^n) is greater than or equal to $2^n - n - 1$, and the minimum 2-rank $2^n - n - 1$ is achieved if and only if the corresponding STS($2^n - 1$) (resp. SQS(2^n)) is isomorphic

to the geometric design having as blocks the lines in $\mathrm{PG}(n-1,2)$ (resp. the planes in $\mathrm{AG}(n,2)$). The structure of the binary code spanned by the blocks of a Steiner triple or quadruple system can be used to find an exact formula for the total number of different $\mathrm{STS}(2^n-1)$ and $\mathrm{SQS}(2^n)$ with 2-rank one higher than the minimum, that is, 2^n-n.

1.124 Theorem [2055] The total number of distinct Steiner triple systems of 2-rank 2^n-n on a given set of 2^n-1 points is

$$\frac{(2^n-1)!(2^{\frac{(2^{n-1}-1)(2^{n-2}-1)}{3}}-2^{2^{n-1}-n})}{2^{2^{n-1}-1}(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-2})}.$$

1.125 Theorem [2056] The total number of distinct $\mathrm{SQS}(2^n)$'s of 2-rank 2^n-n on a given set of 2^n points is

$$\frac{(2^n)!(2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}}-2^{2^{n-1}-n})}{2^{2^{n-1}+n-1}(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-2})}. \tag{1.1}$$

1.126 Remark The formulas of Theorems 1.124 and 1.125 can be used for deriving lower bounds on the number of nonisomorphic Steiner systems of 2-rank 2^n-n and for classifying all systems up to isomorphism for relatively small n.

1.127 Theorem [1273, 2056] There are exactly 1, 15, 4131, 708103, and 341913 isomorphism classes of SQS(16) of 2-rank 11, 12, 13, 14, and 15, respectively.

1.128 Theorem [1709] There are exactly 1239 isomorphism classes of STS(31) of 2-rank 31.

1.129 Table The point codes of the 80 STS(15)s (see Table II.1.28).

No.	2-Rank	STS(15)s in C	A_4	A_7	A_8	A_{11}	A_{12}	A_{15}
1	11	1	0	15	0	0	105	448
2	12	1,2	1	21	3	33	199	851
3	13	1,2,3	3	33	9	99	387	1657
4	13	1,2,4	2	29	10	112	389	1644
5	13	1,2,5	2	28	11	117	384	1634
6	13	6	0	22	15	137	382	1612
7	13	1,7	0	18	15	153	378	1588
8	14	1,2,3,4,5,8	4	44	25	275	764	3220
9	14	1,2,4,9	3	39	23	289	777	3213
10	14	1,2,4,5,10	3	38	24	294	772	3203
11	14	6,11	1	30	26	320	776	3177
12	14	1,2,4,12	3	40	24	286	774	3215
13	14	1,2,4,5,13	3	40	26	288	766	3207
14	14	1,2,3,4,14	4	45	24	270	769	3230
15	14	6,15	1	31	29	319	765	3171
16	14	1,2,3,16	7	57	21	231	763	3269
17	14	1,2,7,17	1	30	30	324	760	3161
18	14	1,2,6,18	1	32	28	314	770	3181
19	14	1,19	0	22	27	349	774	3140
20	14	1,20	0	28	27	325	780	3176
21	14	1,21	0	28	27	325	780	3176
22	14	1,22	0	25	24	334	789	3170
23	15	1,2,4,5,9,10,12,23	4	51	46	668	1567	6330

No.	2-Rank	STS(15)s in C	A_4	A_7	A_8	A_{11}	A_{12}	A_{15}
24	15	1,2,4,9,12,24	4	53	48	662	1561	6334
25	15	1,2,4,5,9,10,12,13,25	4	54	51	661	1550	6328
26	15	1,2,3,4,5,8,10,12,14,26	5	60	52	642	1542	6345
27	15	6,11,15,27	2	42	49	699	1566	6294
28	15	1,2,4,6,11,18,28	2	44	51	693	1560	6298
29	15	1,2,4,9,12,29	4	53	48	662	1561	6334
30	15	6,11,30	2	42	49	699	1566	6294
31	15	1,2,4,5,10,31	4	49	48	678	1557	6310
32	15	6,11,32	2	41	46	700	1577	6300
33	15	1,2,20,33	1	39	49	707	1573	6291
34	15	1,2,20,34	1	39	49	707	1573	6291
35	15	1,2,21,35	1	41	51	701	1567	6295
36	15	36	0	35	50	720	1575	6278
37	15	37	0	27	42	744	1599	6262
38	15	38	0	32	49	731	1576	6264
39	15	1,2,21,39	1	39	49	707	1573	6291
40	15	1,2,21,40	1	41	51	701	1567	6295
41	15	1,2,21,41	1	39	49	707	1573	6291
42	15	42	0	30	47	737	1582	6260
43	15	6,43	0	34	51	725	1570	6268
44	15	44	0	32	45	727	1592	6280
45	15	1,45	0	33	48	726	1581	6274
46	15	46	0	30	43	733	1598	6276
47	15	1,2,21,47	1	36	44	714	1590	6293
48	15	48	0	32	45	727	1592	6280
49	15	49	0	30	43	733	1598	6276
50	15	50	0	26	43	749	1594	6252
51	15	1,51	0	33	48	726	1581	6274
52	15	1,52	0	34	47	721	1586	6284
53	15	1,2,22,53	1	36	44	714	1590	6293
54	15	1,2,22,54	1	37	47	713	1579	6287
55	15	55	0	33	48	726	1581	6274
56	15	1,56	0	32	45	727	1592	6280
57	15	57	0	26	39	745	1610	6268
58	15	1,2,22,58	1	32	40	726	1602	6285
59	15	1,2,20,59	1	41	51	701	1567	6295
60	15	60	0	28	45	743	1588	6256
61	14	1,61	0	22	21	343	798	3164
62	15	1,2,22,62	1	32	36	722	1618	6301
63	15	1,2,19,63	1	29	39	737	1603	6271
64	15	1,2,61,64	1	35	45	719	1585	6283
65	15	65	0	30	43	733	1598	6276
66	15	66	0	28	41	739	1604	6272
67	15	67	0	26	39	745	1610	6268
68	15	68	0	29	40	734	1609	6282
69	15	69	0	26	39	745	1610	6268
70	15	1,70	0	33	48	726	1581	6274
71	15	71	0	27	38	740	1615	6278
72	15	72	0	26	39	745	1610	6268
73	15	73	0	25	44	754	1589	6242
74	15	74	0	31	46	732	1587	6270

No.	2-Rank	STS(15)s in C	A_4	A_7	A_8	A_{11}	A_{12}	A_{15}
75	15	75	0	28	45	743	1588	6256
76	15	1,76	0	35	50	720	1575	6278
77	15	77	0	23	30	748	1643	6286
78	15	1,78	0	25	44	754	1589	6242
79	15	1,7,79	0	21	48	774	1569	6202
80	15	80	0	15	30	780	1635	6238

1.130 Table The codes of blocks of the 80 STS(15)s.

2-Rank	A_1	A_2	A_3	A_4	A_5	A_6	A_7	Remark
11	0	0	35	105	168	280	435	Hamming code
12	1	7	63	189	357	595	835	
13	3	21	119	357	735	1225	1635	
14	7	49	231	693	1491	2485	3235	
15	15	105	455	1365	3003	5005	6435	Complete space

1.131 Table The point codes of STS(v)s with $v < 15$.

v	b	2-Rank	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}
7	7	4	0	7	7	0	0	1					
9	12	9	12	0	135	0	216	0	135	0	12	0	1
13_1	26	13	0	0	13	0	52	0	403	0	1144	0	2483
13_2	26	13	0	0	8	0	47	0	423	0	1164	0	2453

1.9 Designs with the Symmetric Difference Property

1.132 A symmetric 2-design has the *symmetric difference property*, or is an *SDP design* [1253], if the symmetric difference of any *three* blocks is either a block or the complement of a block. The parameters of a symmetric 2-(v, k, λ) SDP design with $k < v/2$ are of the form

$$(*) \qquad v = 2^{2m},\ k = 2^{2m-1} - 2^{m-1},\ \lambda = 2^{2m-2} - 2^{m-1}.$$

1.133 Remark The designs with the symmetric difference property provide a number of interesting links between two-weight codes, uniformly-packed codes, Reed–Muller codes, and codes achieving the Grey–Rankin bound. They are also closely related to quasi-symmetric designs, difference sets, bent functions, strongly regular graphs, and point sets in a projective space having prescribed intersection numbers with the hyperplanes.

1.134 A nonsymmetric 2-(v, k, λ) design with parameters of the form

$$(**) \qquad v = 2^{2m-1} - 2^{m-1},\ k = 2^{2m-2} - 2^{m-1},\ \lambda = 2^{2m-2} - 2^{m-1} - 1,$$

or

$$(***) \qquad v = 2^{2m-1} + 2^{m-1}A,\ k = 2^{2m-2},\ \lambda = 2^{2m-2} - 2^{m-1}$$

has the *symmetric difference property*, or is an *SDP design*, if the symmetric difference of any *two* blocks is either a block or the complement of a block.

1.135 Remark Any nonsymmetric SDP design is quasi-symmetric. However, there are quasi-symmetric designs with parameters $(**)$ or $(***)$ that are not SDP designs [1235, 1379].

1.136 Theorems

1. [1236] A derived (residual) design of a symmetric SDP design is a quasi-symmetric SDP design with parameters $(**)$ ($(***)$, respectively).

2. [2050] Any quasi-symmetric SDP design is embeddable as a derived or residual design into a unique symmetric SDP design. Moreover, two derived or residual designs of a symmetric SDP design $\mathcal{D}$ with respect to blocks B', B'' are isomorphic if and only if B' and B'' are in the same orbit under the automorphism group of $\mathcal{D}$.

1.137 Theorem [708] The rows of the incidence matrix of any symmetric SDP design are the minimum weight codewords in a binary linear code spanned by the first order Reed–Muller code $\mathrm{RM}(1, 2m)$ and the characteristic function of an elementary abelian difference set in $\mathrm{AG}(2m, 2)$ (or equivalently, the vector of values of a *bent function* on $2m$ variables [1829]).

1.138 An (n, k, h_1, h_2) *set* S in the projective space $\mathrm{PG}(k-1, q)$ is a set of n points with the property that every hyperplane meets S in either h_1 or h_2 points.

1.139 A linear code C is *projective* if the minimum distance of $C^\perp$ is at least 3 and is a *two-weight code* if there are only two distinct nonzero weights in C.

1.140 Theorem [672] The existence of a projective $[n, k]$ two-weight code over $\mathbb{F}_q$ with weights $w_1,\ w_2$ is equivalent to the existence of an $(n, k, n-w_1, n-w_2)$ set in $\mathrm{PG}(k-1, q)$.

1.141 Theorem [672]. The graph whose vertices are the codewords in a projective 2-weight code, in which two words are adjacent if their mutual distance is w_1, is strongly regular (see §VII.11).

1.142 Theorem [2086, 2093] A single-error-correcting code C is uniformly packed if and only if $C^\perp$ is a two-weight code.

1.143 A set of *elliptic* type is an (n, k, h_1, h_2) set in $\mathrm{PG}(2m-1, 2)$ with parameters
$$n = 2^{2m-1} - 2^{m-1} - 1,\ k = 2m,\ h_1 = 2^{2m-2} - 2^{m-1} - 1, h_2 = 2^{2m-2} - 1.$$

1.144 A set of *hyperbolic* type is an (n, k, h_1, h_2) set in $\mathrm{PG}(2m-1, 2)$ with parameters
$$n = 2^{2m-1} + 2^{m-1} - 1,\ k = 2m,\ h_1 = 2^{2m-2} + 2^{m-1} - 1,\ h_2 = 2^{2m-2} - 1.$$

1.145 Theorems [2050]

1. The rows of the point by block incidence matrix of any quasi-symmetric SDP design are the minimum weight codewords in a binary linear code spanned by the dual code of the Hamming code of length $2^{2m} - 1$ and the incidence vector of a set of elliptic or hyperbolic type in $\mathrm{PG}(2m-1, 2)$.
2. The point orbits under the full automorphism group of an SDP quasi-symmetric design correspond to equivalence classes of sets of elliptic or hyperbolic type in $\mathrm{PG}(2m-1, 2)$.

1.146 A binary linear code is *self-complementary* if it contains the all-one vector.

1.147 Theorem (Grey–Rankin bound) If C is a self-complementary $[n, k, d]$ code, then $|C| \le 8d(n-d)/(n-(n-2d)^2)$, provided the denominator is positive.

1.148 Theorem [1235] The linear span of the block-by-point incidence matrix of a quasi-symmetric SDP design is a self-complementary code optimal with respect to the Grey–Rankin bound.

1.149 Theorem The 2-rank of any symmetric 2-design with parameters $(*)$ is at least $2m+2$. The 2-rank is exactly $2m+2$ if the design is an SDP design.

1.150 Theorem [1568] The 2-rank of a symmetric 2-design with parameters $(*)$ is $2m+2$ if and only if the design is an SDP design.

1.151 Remark Theorem 1.150 was known for a long time as the *Dillon Conjecture*.

1.152 Conjecture (*all-one vector conjecture*) The all-one vector is contained in the binary code of any symmetric design with parameters $(*)$.

1.153 Remark Conjecture 1.152 (also due to Dillon) implies Theorem 1.150. Conjecture 1.152 is true for designs on 64 or fewer points [1236].

1.154 Example There are exactly four affine equivalence classes of bent functions on six variables [1829], which give rise to four nonisomorphic symmetric 2-(64,28,12) SDP designs via Theorem 1.137. These designs all have transitive automorphism groups [1715]; hence, by Theorem 1.136, there are four nonisomorphic quasi-symmetric 2-(28,12,11) (2-(36,16,12)) SDP designs obtained as derived (residual, respectively) designs. By Theorem 1.145(2), the point orbits of these quasi-symmetric SDP designs give rise to five projective equivalence classes of sets of elliptic type, and seven classes of sets of hyperbolic type in PG$(5, 2)$ [2050]. By Theorems 1.140 and 1.142, the classification of these sets implies that up to equivalence, there are exactly five two-weight binary $[27, 6, 12]$ codes (uniformly packed $[27, 21, 3]$ codes), and exactly seven binary two-weight $[35, 6, 16]$ codes (uniformly packed $[35, 29, 3]$ codes, respectively). Tables 1.155 and 1.156 contain generator matrices of these 2-weight codes [2052].

1.155 Table Generator matrices for the binary projective two-weight [27,6,12] codes.

Code C	Generator Matrix	$\lvert AutC\rvert$
1	0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 1 0 1 0 1 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 0 0 0 1 1 1 0 1 1 1 0 1 1 1 0 1	51840
2	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 0 0 0 0 0 1 1 0 0 0 0 0 1 1 0 0 1 0 0 0 1 1 1 0 1 1 1 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 1 1 1 0 0 1 1 1 0 1 0 1 1 1 0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 0 1 0 0 1 1 1 1 1 0 1 0 0 0	384
3	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 1 1 1 0 1 0 0 0 1 0 0 0 1 0 1 0 1 0 1 1 1 0 0 0 1 0 1 0 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 0 0 0 1 1 1 0 0 1 1 0 0 1 1 1 1 1 1 1 1 0 0 1 0 0 1 1	160
4	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 0 1 0 1 0 1 1 0 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 1 0 0 0 0 1 1 1 0 1 0 0 1 0 1 0 0 0 1 1 0 0 1 1 0 1 0 1 0 0 0 0	120
5	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 1 0 0 1 0 0 1 0 1 1 0 1 1 0 0 0 0 1 1 0 1 1 0 0 1 0 1 1 0 1 0 1 1 0 0 0 1 1 0 1 0 0 1 0 0 0 1 0 1 0 1 0 1 1 0 0 1 1 0 1 0 0 0 0 0 1 0 0 1 0 1 0 1	24

1.156 Table Generator matrices for the binary projective two-weight [35,6,16] codes.

Code C	Generator Matrix	$\lvert AutC\rvert$
1	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 1 0 0 1 1 0 1 0 0 1 1 0 1 0 1 0 1 1 1 0 1 0 0 0 1 0 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 0 1 0 1 1 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 1 1 0 1	40320
2	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 0 0 0 0 1 1 1 1 1 1 0 0 1 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 0 1 1 1 0 1 0 0 0 1 0 1 1 0 0 1 0 0 0 1 0 1 1 0 1 1 1 0 1 0 0 0 1 0 1 1 0 0 1 1 0 0 0 1 0 1 0 1 0 1 1 1 0 1 1 0 0 1 0 0 1 1 1 1 0 0 1 1 1 0 1 0 1 1	1344
3	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 0 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 0 0 1 0 0 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 0 0 0 1 1 1 0 1 1 1 0 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 1 0 0 0 0 1 0 1 1 0 0 1 0 0 0 1 0 1 1 0 0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 0 1 0 0 0 1 0 1 0 0 0 1 1 1 0 1 0 1 1	384
4	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 1 1 1 1 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 0 1 1 1 0 0 0 0 1 1 1 0 1 0 0 0 1 0 0 0 1 0 1 0 1 1 0 1 1 0 0 1 0 1 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0 1 1 0 0 1 1 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 1 1 0 1 0 0 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1	96
5	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 1 1 0 0 1 1 1 0 0 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 0 0 1 0 0 0 1 1 1 0 1 0 1 0 1 1 0 1 1 0 0 1 0 0 0 1 0 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 1 0 0 1 1 1 0 1 1 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 1 0 1 0 1 1 0 1 0 0	120
6	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 0 0 0 1 1 1 1 1 0 0 0 0 0 1 1 1 0 0 0 0 0 1 1 1 0 0 0 1 1 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 0 0 1 1 0 1 1 0 1 1 1 1 0 1 1 0 1 1 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 0 0 1 0 1 0 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 1 0 1 0 1 0 1 0 1 1 0 1	24
7	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 0 0 0 1 1 1 1 1 0 0 0 1 1 1 1 1 0 0 0 1 1 1 1 1 0 0 0 1 1 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 1 1 0 0 0 1 1 0 0 0 0 0 0 1 1 0 1 1 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 1 0 0 1 0 0 1 0 1 0 0 1 0 1 1 1 1 1 0 1 0 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 0 0 0 0 1 1 0 1 0 1 0 0 0 1 0 1	84

1.10 Maximal Codes and Hadamard Matrices

1.157 Given n, d $(d \le n)$, $A(n,d)$ denotes the maximum size of a binary code of length n and minimum distance d.

1.158 Theorem (*Plotkin bound* [1753]) If d is even and $d > n/2$, then

$$A(n,d) \le 2\left\lfloor \tfrac{d}{2d-n} \right\rfloor, \text{ and } A(2d,d) \le 4d.$$

If d is odd and $d > (n-1)/2$, then

$$A(n,d) \le 2\left\lfloor \tfrac{d+1}{2d+1-n} \right\rfloor, \text{ and } A(2d+1,d) \le 4d+4.$$

1.159 An (n, M, d) code of size M that achieves equality in the Plotkin bound (Theorem 1.158) for the given n and d is *maximal*.

1.160 Examples Let $n = 4\lambda$ and A be the incidence matrix of a symmetric Hadamard 2-$(4\lambda - 1, 2\lambda, \lambda)$ design. Then,

1. The rows of A and the zero vector form a maximal $(n-1, n, n/2)$ code $\mathcal{C}_n$ that achieves equality in Theorem 1.158(1).
2. The words of $\mathcal{C}_n$ together with their complements, obtained by replacing 0 by 1 and vice versa, form a maximal $(n-1, 2n, n/2-1)$ code $\mathcal{B}_n$ that achieves equality in Theorem 1.158(2).
3. The words of $\mathcal{C}_n$ beginning with zero after deleting the first coordinate form a maximal $(n-2, n/2, n/2)$ code $\mathcal{C}'_n$ that achieves equality in Theorem 1.158(1).

1.161 Theorem [1432] Maximal codes exist for all admissible values of n and d provided that Hadamard matrices exist of any order divisible by 4.

1.162 Given two codes C_1, C_2 with parameters (n_1, M_1, d_1) and (n_2, M_2, d_2), respectively, and nonnegative integers $a,\ b$, the code $C = aC_1 \oplus bC_2$ is an (n, M, d) code with $n = an_1 + bn_2,\ M = \min(M_1, M_2)$, and $d \geq ad_1 + bd_2$, defined as follows: glue together a copies of C_1 followed by b copies of C_2; then delete the last $M_2 - M_1$ rows if $M_2 > M_1$, or the last $M_1 - M_2$ rows if $M_1 \geq M_2$.

1.163 Construction [1432] A maximal (n, M, d) code, for d even and $2d > n \geq d$, attaining the bound in Theorem 1.158(1). Let

$$k = \lfloor \tfrac{d}{2d-n} \rfloor,\ a = d(2k+1) - n(k+1),\ b = kn - d(2k-1).$$

Then $a,\ b$ are nonnegative integers, $n = (2k-1)a + (2k+1)b,\ d = ka + (k+1)b$, and the code

$$C = \begin{cases} \frac{a}{2}\mathcal{C}'_{4k} \oplus \frac{b}{2}\mathcal{C}'_{4k+4} & \text{if } n \text{ is even;} \\ a\mathcal{C}'_{2k} \oplus \frac{b}{2}\mathcal{C}'_{4k+4} & \text{if } n \text{ is odd and } k \text{ is even;} \\ \frac{a}{2}\mathcal{C}'_{4k} \oplus b\mathcal{C}_{2k+2} & \text{if } n \text{ and } k \text{ are odd,} \end{cases}$$

is a code of length n, minimum distance d, and size $M = 2k = 2\lfloor d/(2d-n) \rfloor$.

1.164 Remark An analogue of Plotkin's bound for q-ary codes was proved in [277]. The q-ary analogue of Levenshtein's construction that uses generalized Hadamard matrices for the construction of maximal q-ary codes was given in [1495].

1.11 Equidistant Codes, Designs and Orthogonal Arrays

1.165 An $(n, M, d; q)$ *code* is a q-ary code of length n, size M, and minimum (Hamming) distance d.

1.166 An $(n, M, d; q)$ code is *equidistant* if the distance between any two codewords is d.

1.167 Theorem The distance of any equidistant $(n, M, d; q)$ code satisfies $d \leq \frac{nM(q-1)}{(M-1)q}$.

1.168 An equidistant code that achieves equality in Theorem 1.167 is an *optimal equidistant* code.

1.169 Construction [1880] An optimal equidistant $(n, M, d; q)$ code exists if and only if there exists a resolvable 2-design with parameters $v = M,\ k = \frac{M}{q},\ \lambda = n - d,\ r = n,\ b = nq$. Label the rows of the identity matrix of order q, I_q by the symbols $0, 1, \ldots, q-1$. Let $\mathcal{D}$ be a resolvable 2-design with parameters v, k, λ, r, b and $v \times b$ incidence matrix $A = [A_1 \ldots A_i \ldots A_r]$, where A_i is the incidence matrix of the $q = \frac{v}{k}$ blocks from the ith parallel class. Replace each row of A_i $(1 \leq i \leq r)$ by the corresponding symbol from $\{0, 1, \ldots, q-1\}$ according to the labeling of the rows of the identity matrix.

The resulting array is an optimal equidistant $(n, M, d; q)$-code. In the other direction, given an optimal equidistant $(n, M, d; q)$ code C, replace each symbol i in C by the row of I_q with label i. The resulting (0,1)-matrix is the incidence matrix of a resolvable 2-design.

1.170 Theorem

1. The columns of an $M \times n$ array, being an optimal equidistant $(n, M, d; q)$ code, form an orthogonal array $\mathrm{OA}(M, n, q, 1)$.
2. The columns of an optimal equidistant $(n, M, d; q)$ code corresponding to an affine resolvable 2-design, form an orthogonal array $\mathrm{OA}(M, n, q, 2)$ meeting the Bose–Bush bound (see §III.6).

1.171 Remark Any affine resolvable 2-design has a unique resolution. Therefore, there is a one-to-one correspondence between the isomorphism classes of affine resolvable designs with given parameters and the equivalence classes of corresponding optimal equidistant codes or orthogonal arrays.

1.172 Remark The number of affine 2-designs with parameters 2-$(q^m, q^{m-1}, (q^{m-1}-1)/(q-1))$, q a prime power, $(m \geq 3)$ grows exponentially [1223, 1374]. Among all such designs, one is the classical geometric design having as blocks the hyperplanes in $\mathrm{AG}(m, q)$. Theorem 1.173 characterizes this classical design in terms of the minimum q-rank of the related orthogonal array.

1.173 Theorem [2057] For every prime power q and every $m \geq 2$, there exists only one, up to monomial equivalence, $OA(q^m, (q^{m-1}-1)/(q-1), q, 2)$ of minimum q-rank equal to m. The related affine 2-design is isomorphic to the classical design having as blocks the hyperplanes in $\mathrm{AG}(m, q)$.

1.174 Example Up to isomorphism, there are exactly 68 affine resolvable 2-designs with parameters $v = 27, k = 9, \lambda = 4, r = 13, b = 39$ [1380], hence, 68 optimal equidistant $(13, 27, 9; 3)$ codes, and 68 $\mathrm{OA}(27, 13, 3, 2)$. Table 1.175 contains the six $\mathrm{OA}(27, 13, 3, 2)$ corresponding to the six designs with point transitive automorphism groups.

1.175 Table $\mathrm{OA}(27, 13, 3, 2)$ and $(13, 27, 9; 3)$ codes derived from transitive affine 2-(27,9,4) designs

1:	2:
11111111200220022020202021	11111111200220022020202021
11200202111111022020020220 1	11200202111111200202202002 1
11200202022002111111202002 1	11200202200220111111020220 1
11200202200220200202111111	11200202022002022020111111
20101022110202112002112020 1	20101022112020110220110202 1
20101022021120201120021102 1	20101022201102021102201120 1
20101022020110202112002111	20101022020211202011022011 1
20012201110202201120200211 1	20012201112020021102022011 1
20012201202011112002021102 1	20012201020211110220201120 1
20012201021120020211112020 1	20012201201102202011110202 1
20220110110202020211021102 1	20220110101022102210210101
20220110021120112002200211 1	20220110012210221001100122 1
20220110202011201120120201	20220110220101010122012201 1

3:	4:
11111111200022022020020220 1	11111111200220202002022002 1
11002022111111022020202002 1	11200202111111020220022002 1
11002022022200111111020220 1	11200202200220111111200220 1
11002022200022002021111111	11200202022002202002111111 1
20121002110202112002112020 1	20101022110202112020112020 1
20011202121002201120021102 1	20101022021120021102201102 1
20201102102102020211200211 1	20101022202011200211020211 1
20120021221010120012001212 1	20012201112200001122220011 1
20010221202110212100210021 1	20012201020121210201012120 1
20200121210210001221122100 1	20012201201012122010101202 1
20122010002121101022220101 1	20220110110022002211221100 1
20012210010221220110102210 1	20220110021210211020010212 1
20202110021021012201011022 1	20220110202101120102102021 1

5:	6:
11111111200220200202020220 1	11111111220200002022202002 1
11002022111111022020020220 1	11020202111111220200202002 1
11002022200220111111202002 1	11020202220200111111020220 1
11002022022002200202111111	10102022120202122200111100 1
20121002110202110220110202 1	21001202012002012002112211 1
20121002021120021102201120 1	20211002101220021102021012 1
20011202121200202011022011 1	20221100020112101202200121 1
20120021202011102210221010 1	20100221211020022110200121 1
20200121221010010122012201 1	22010021000211001210112222 1
20200121102201221001100122 1	20002211102201100221220011 1
20012210210012121200002121 1	20120120022101212010021012 1
20012210002121210021211200 1	20012012021120210021102120 1
20202110010122002112120012 1	20022110210012020121011202 1

1.12 Constant Weight Codes and Designs

1.176 A *constant weight code* consists of words of a given fixed weight.

1.177 Given n, d, w $(d \leq n,\ w \leq n)$, $A(n, d, w)$ denotes the maximum size of a binary constant weight code of length n, minimum distance d, and weight w.

1.178 Examples

1. The incidence vectors of the blocks of a t-(v, k, λ) design with maximum block intersection number s form a constant weight code of weight $w = k$, length $n = v$, and minimum distance $d = 2(k - s)$. In particular, the incidence vectors of a t-$(v, k, 1)$ packing form a constant weight code of weight $w = k$, length $n = v$, and minimum distance $d = 2(k - t + 1)$. See §VI.40.
2. The rows of the point by block incidence matrix of a 2-design with parameters v, k, λ, r, b form a constant weight code with $n = b,\ w = r,\ d = 2(r - \lambda)$.

1.179 Theorem (*Johnson bound* [1210])

1. If $w \geq \delta$, then $A(n, 2\delta, w) \leq \left\lfloor \frac{n}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \ldots \left\lfloor \frac{n-w+\delta}{\delta} \right\rfloor \ldots \right\rfloor \right\rfloor \right\rfloor$.
2. If $w^2 - nw + n\delta > 0$, then $A(n, 2\delta, w) \leq \left\lfloor \frac{n\delta}{w^2-nw+n\delta} \right\rfloor$.

1.180 Remark The inequalities of Theorem 1.179 have the relaxations

1. $A(n, 2\delta, w) \leq \frac{n(n-1)\ldots(n-w+\delta)}{w(w-1)\ldots\delta}$, and
2. $A(n, 2\delta, w) \leq \frac{n\delta}{w^2-nw+n\delta}$.

These weaker bounds are equivalent to the bounds of Theorem 1.179 if the numbers encountered happen to be integer.

1.181 Theorem [1881]

1. An $(n, M, 2\delta)$ code C of a constant weight w achieves equality in Remark 1.180(1) if and only if C is the block by point incidence matrix of a Steiner system $S(t, k, v)$ with $v = n,\ k = w,\ t = w - \delta + 1$.
2. An $(n, M, 2\delta)$ code C of a constant weight w achieves equality in Remark 1.180(2) if and only if C is the point by block incidence matrix of a 2-design with $b = n,\ r = w,\ \lambda = w - \delta$.

1.182 Remark By Theorem 1.181, the existence of a Steiner system or a 2-design implies the existence of an optimal constant weight code meeting either of the bounds in Remark 1.180. Therefore, any table for such designs gives a table of values for $A(n, 2\delta, w)$. For example, the existence of an $S(5, 6, 12)$ implies that $A(12, 4, 6) = 132$.

1.183 Example It is not known whether a Steiner system $S(4, 5, 17)$ exists, but its existence would imply that $A(17, 4, 5) = 476$. The current record (see [2053]) is $A(17, 4, 5) \geq 441$.

See Also

§II.6	Symmetric designs.
§III.6, III.7	Orthogonal arrays.
§VI.1	Hadamard matrices.
§VI.40	Packings with constant block size are constant weight codes.
§VI.48	Quasi-symmetric designs.
§VII.9	Finite groups and designs.
§VII11	Strongly regular graphs.
§VII.2	Projective and affine geometries.
[349]	A table of binary linear codes with largest minimum distance for given length and dimension. Brouwer's tables for the minimum distance of linear codes are also available online at `http://www.cwi.nl/htbin/aeb/lincodbd/`$q/n/k$, where $q = 2, 3$, or 4, n is the code length, and k is the code dimension.
[347]	An extensive table of constant weight codes of length $n \leq 28$.
[1505]	An extensive general introduction.
[2032, 2085, 2218]	More on perfect codes (§1.2).
[1733, 1766, 1852]	Tables of cyclic codes.
[424, 1505, 2086]	More on nonlinear codes (§1.5).
[122, 2046]	More on codes with majority decoding (§1.6).
[1016, 1371, 1379, 2041, 2042, 2049],	More on intersection numbers and codes (§1.7).
[121, 122, 129, 1281, 1282, 2061]	More on STS and codes (§1.8).
[412, 736, 1255]	More on codes and designs with the symmetric difference property (§1.9).
[1380, 2046]	More on orthogonal arrays, resolvable designs, and optimal equidistant codes (§1.11).
[2046, §2.4]	More on constant weight codes (§1.12).

References Cited: [102, 121, 122, 123, 128, 129, 162, 245, 277, 312, 326, 347, 349, 405, 406, 410, 411, 412, 424, 600, 601, 602, 672, 674, 708, 736, 746, 796, 916, 917, 922, 992, 1016, 1023, 1025, 1032, 1049, 1050, 1051, 1052, 1054, 1091, 1137, 1150, 1151, 1210, 1223, 1235, 1236, 1253, 1255, 1269, 1273, 1278, 1281, 1282, 1299, 1371, 1374, 1379, 1380, 1432, 1495, 1503, 1504, 1505, 1560, 1568, 1659, 1709, 1715, 1733, 1735, 1736, 1749, 1750, 1751, 1752, 1753, 1766, 1771, 1774, 1829, 1831, 1852, 1880, 1881, 1882, 1930, 1948, 2000, 2010, 2032, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2061, 2085, 2086, 2093, 2218]

2 Finite Geometry

Leo Storme

2.1 Projective Planes

2.1 A *finite incidence structure*, or *finite geometry*, $P = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is a finite set of *points* $\mathcal{P}$, a finite set of *lines* $\mathcal{L}$, and an *incidence* relation I between them.

2.2 A *finite projective plane* P is a finite incidence structure such that:

1. any two distinct points are incident with exactly one line;
2. any two distinct lines are incident with exactly one point;
3. there exists a quadrangle, four points no three collinear.

2.3 For a finite projective plane P, there is a positive integer n such that any line of P has exactly $n+1$ points. This number n is the *order* of P.

2.4 **Proposition** A finite projective plane of order n has n^2+n+1 points, n^2+n+1 lines, and $n+1$ lines through each point.

2.5 **Remark** One of the most difficult questions in finite geometry is: *What positive integers are orders of finite projective planes?* Very little is known; all known examples have prime power order. The Bruck–Ryser–Chowla theorem (§II.6.2) excludes an infinite number of integers. Only one further number has been excluded: there is no projective plane of order 10. See Remark VII.6.27 for a discussion of the computer search for a projective plane of order 10.

2.6 **Table** An overview of the state of knowledge concerning small projective planes.

order n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
existence	y	y	y	y	n	y	y	y	n	y	?	y	n	?	y
number	1	1	1	1	0	1	1	4	0	≥ 1	?	≥ 1	0	?	≥ 22

2.7 **Theorem** Let P be a geometry consisting of a finite number of points and a finite number of at least two lines for which any two distinct points are on exactly one line, and there is an integer $n \geq 2$ such that any line has exactly $n+1$ points. Then these assertions are equivalent:

1. P is a projective plane.
2. Any point of P is on at most $n+1$ lines.
3. Any point of P is on exactly $n+1$ lines.
4. There are exactly n^2+n+1 points in P.
5. P is a 2-$(n^2+n+1, n+1, 1)$ design (or, in other words, an $S(2, n+1, n^2+n+1)$ Steiner system).

2.8 **Construction** The most important class of finite projective planes can be obtained as follows. Let V be the 3-dimensional vector space over the finite field $F = \mathbb{F}_q$ of order q. The geometry $P(V)$ that has as its *points* the 1-dimensional subspaces of V and as its *lines* the 2-dimensional subspaces of V is a projective plane.

Another way of describing this plane is as follows. Let $(a, b, c) \in V \setminus \{(0, 0, 0)\}$. Let $(a : b : c) = \{(fa, fb, fc) | f \in F \setminus \{0\}\}$. Similarly define $[x : y : z] = \{[fx, fy, fz] | f \in F \setminus \{0\}\}$ for any $(x, y, z) \in V \setminus \{(0, 0, 0)\}$. Now consider the symbols $(a : b : c)$ as points and the symbols $[x : y : z]$ as lines and say that a point $(a : b : c)$ lies on the line $[x : y : z]$ if and only if $ax + by + cz = 0$. This gives a projective plane.

These projective planes are denoted by $\mathrm{PG}(2, F)$. In addition, if $F = \mathbb{F}_q$ is a finite field of order q, then the projective plane obtained in this way has order q and is also denoted by $\mathrm{PG}(2, q)$. Since for any prime power q there is a finite field of order q, for any prime power q there is a projective plane of order q.

2.9 $(a : b : c)$ and $[x : y : z]$ are the *homogeneous coordinates* of the corresponding point and line of $\mathrm{PG}(2, F)$.

2.10 **Remarks** The finite projective planes $\mathrm{PG}(2, F)$ are exactly the finite *desarguesian* projective planes, those finite projective planes in which the theorem of Desargues is valid (Theorem 2.152). Equivalently, the finite projective planes $\mathrm{PG}(2, F)$ are precisely those finite projective planes that can be embedded as a plane in a higher-dimensional projective space. Sections 2.14 to 2.22 discuss nondesarguesian projective planes.

2.2 Affine Planes

2.11 A *finite affine plane* is a finite incidence structure such that:

1. any two distinct points are on exactly one line;
2. for any point P outside a line ℓ there is exactly one line through P that has no point in common with ℓ (this is the *euclidean parallel axiom*);
3. there exist three points not on a common line.

2.12 **Remark** If one defines a *parallelism* among the lines by saying that two lines are parallel if they are equal or have no point in common, then the parallelism of an affine plane is an equivalence relation such that any two nonparallel lines meet. The equivalence classes belonging to the parallelism are *parallel classes*. By axiom (2), any parallel class of an affine plane is a partition of the point set by lines.

2.13 **Construction** Given an affine plane A one can define a new geometry P: the points of P are the points of A and the parallel classes of A; the lines of P are the lines of A and one new line $g^\star$. The incidence is: Line $g^\star$ is incident with all parallel classes, and each line ℓ of A is now incident with its points in A together with the parallel class to which it belongs. Then P is a projective plane. Conversely, if one removes a line g together with all its points from a projective plane P, one gets an affine plane $A = P_g$. Two lines of the affine plane P_g are parallel if and only if the projective lines containing them meet the line g in the same point. Then g is the *infinite line* of A and the points of g the *infinite points* of A.

2.14 For a finite affine plane A, there is a positive integer n such that any line of A has exactly n points. This number n, which is also the order of the corresponding projective plane, is the *order* of A.

2.15 **Proposition** A finite affine plane of order n has n^2 points, $n^2 + n$ lines, and $n + 1$ lines through each point.

2.16 **Theorem** Let A be a finite geometry consisting of points and at least two lines for which any two distinct points are on exactly one line, and there is an integer $n \geq 2$ such that any line has exactly n points. Then these assertions are equivalent:

1. A is an affine plane.
2. Any point of A is on exactly $n+1$ lines.
3. There are exactly n^2 points in A.
4. A is a 2-$(n^2, n, 1)$ design (equivalently, an $S(2, n, n^2)$ Steiner system).

2.17 **Construction** The usual way to construct finite affine planes is as follows. Let F be a finite field $\mathbb{F}_q$. Then the geometry $\mathrm{AG}(2, F)$ has as points the pairs (a, b) with $a, b \in F$, and its lines are the sets of points (x, y) satisfying an equation $Y = mX + b$ $(m, b \in F)$ or an equation $X = c$ with $c \in F$. Then $\mathrm{AG}(2, F)$ is an affine plane.

Another way of describing this affine plane is as follows. Let V be a 2-dimensional vector space over F. The points of $\mathrm{AG}(2, F)$ are all vectors of V and the lines are all cosets $v + \langle u \rangle$, where $u \in V \backslash \{(0, 0)\}$. If F is a finite field with q elements, then $\mathrm{AG}(2, F)$ is an affine plane of order q and is also denoted by $\mathrm{AG}(2, q)$.

2.18 **Remark** The finite affine planes $\mathrm{AG}(2, F)$ are precisely the finite *desarguesian* affine planes and the finite affine planes $\mathrm{AG}(2, F)$ are precisely those finite affine planes that can be embedded in a higher-dimensional affine space. See §2.4.

2.19 **Remark** The finite affine planes are classical examples of quasi-residual designs, which effectively are residual designs (§II.6.4) and are classical examples of resolvable designs (§II.7).

2.3 Projective Spaces

2.20 A *finite projective space* P is a finite incidence structure such that:

1. any two distinct points are on exactly one line;
2. (*Veblen–Young axiom*) let A, B, C, D be four distinct points of which no three are collinear. If the lines AB and CD intersect each other, then the lines AD and BC also intersect each other;
3. any line has at least three points.

2.21 **Examples** Finite projective spaces can be obtained as follows. Let V be a vector space of dimension $d+1$ over the finite field $F = \mathbb{F}_q$. The geometry $P(V)$ that has as its *points* the 1-dimensional subspaces of V and as its *lines* the 2-dimensional subspaces of V is a finite projective space.

Another way of describing the same geometry is as follows. Let $d+1$ be a positive integer and F a finite field $\mathbb{F}_q$. Let $(a_0, a_1, \ldots, a_d) \in V \setminus \{(0, 0, \ldots, 0)\}$. Define

$$(a_0 : a_1 : \cdots : a_d) = \{(fa_0, fa_1, \ldots, fa_d) | f \in F \setminus \{0\}\}.$$

The symbols $(a_0 : a_1 : \cdots : a_d)$ are considered as points and are *homogeneous coordinates*. The line through $(a_0 : a_1 : \cdots : a_d)$ and $(b_0 : b_1 : \cdots : b_d)$ is the set of points

$$\{(b_0 : b_1 : \cdots : b_d)\} \cup \{(a_0 + cb_0 : a_1 + cb_1 : \cdots : a_d + cb_d) \mid c \in F\}.$$

The projective space $P(V)$ is also denoted by $\mathrm{PG}(d, F)$. If F is a finite field with q elements, then $\mathrm{PG}(d, q)$ is often used instead of $\mathrm{PG}(d, F)$.

2.22 **Theorem** (*Representation theorem of projective geometry*) Any finite projective space that is not a projective plane is isomorphic to some $P(V)$.

2.23 Let P be a projective space. A *(linear) subspace* of P is a set U of points of P such that for any two points $P, Q \in U$, any point on the line PQ also is contained in U. Any subspace is, together with the lines contained in it, a projective space.

2.24 If S is an arbitrary set of points of P, then the *span* $\langle S \rangle$ of S is the intersection of all subspaces containing S. The span $\langle S \rangle$ is again a subspace.

2.25 A set S of points of P is *independent* if for any $x \in S$, $x \notin \langle S \setminus \{x\} \rangle$. An independent set that spans a projective space P is a *basis* of P.

2.26 **Theorem** Let U be a subspace of P, and let $Q \in P \setminus U$. Then the subspace W spanned by U and Q consists precisely of the points on the lines QX with $X \in U$.

2.27 **Remark** A set of points is a basis if and only if it is a maximal independent set if and only if it is a minimal spanning set. All bases have the same number of elements.

2.28 A projective space P has *dimension* d if a basis has $d+1$ elements. A subspace of dimension 2 is a *plane*; in a d-dimensional projective space, the *hyperplanes* are the subspaces of dimension $d-1$.

2.29 **Proposition** (*Dimension formula*) For two subspaces U_1 and U_2:

$$\dim(\langle U_1, U_2 \rangle) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2).$$

In particular, any t-dimensional subspace not contained in a hyperplane H intersects H in a subspace of dimension $t-1$.

2.30 The *quotient geometry* (or *residual geometry*) P/U of a projective space P modulo a t-dimensional subspace U has as points the $(t+1)$-dimensional subspaces through U and as lines the $(t+2)$-dimensional subspaces through U.

2.31 **Proposition** If P has dimension d and U is a t-dimensional subspace, then P/U is a projective space of dimension $d-t-1$.

2.32 If P is finite, there is an integer $n \geq 2$ such that any line has exactly $n+1$ points. This number n is the *order* of P.

2.33 **Remark** Let P be a finite d-dimensional projective space of order n. There are $n^t + \cdots + n + 1$ points in a t-dimensional subspace of P. The number of points and the number of hyperplanes of P are both equal to $n^d + \cdots + n + 1$. Any subspace and any quotient geometry of P also have order n.

2.34 **Proposition** Let q be a prime power, and d and i positive integers with $i \leq d$. The *gaussian coefficients*

$$\begin{bmatrix} d \\ i \end{bmatrix}_q = \frac{(q^d-1)(q^{d-1}-1)\cdots(q^{d-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}$$

denote the number of i-dimensional vector subspaces of a d-dimensional vector space over $\mathbb{F}_q$.

2.35 The points of $\mathrm{PG}(d,q)$ together with the i-dimensional subspaces of $\mathrm{PG}(d,q)$ as blocks and incidence by natural containment form an incidence structure denoted by $\mathrm{PG}_i(d,q)$.

2.36 **Proposition** $\mathrm{PG}_i(d,q)$ is a block design with parameters

$$v = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q = (q^{d+1}-1)/(q-1), \quad k = \begin{bmatrix} i+1 \\ 1 \end{bmatrix}_q = (q^{i+1}-1)/(q-1), \quad \lambda = \begin{bmatrix} d-1 \\ i-1 \end{bmatrix}_q$$

$$(\text{also } b = \begin{bmatrix} d+1 \\ i+1 \end{bmatrix}_q \text{ and } r = \begin{bmatrix} d \\ i \end{bmatrix}_q).$$

2.4 Affine Spaces

2.37 A *parallelism* of a geometry consisting of a set of points and a set B of blocks is an equivalence relation ("parallel") on B that satisfies the *euclidean parallel axiom*: for any point P and any block B, there is exactly one block C through P that is parallel to B. The equivalence classes of a parallelism are *parallel classes*.

2.38 A *finite affine space* is a finite incidence structure A such that:

1. any two distinct points are on exactly one line;
2. A has a parallelism;
3. (*Triangle axiom*) if A, B, C are three noncollinear points and A', B' are two distinct points such that the line $A'B'$ is parallel to AB, then the line on A' parallel to AC and the line on B' parallel to BC intersect in some point C';
4. there exist three points not on a common line.

2.39 **Remark** Most properties of affine spaces follow from the fact that they have a *projective closure*: for any affine space A there exists a projective space P and a hyperplane H of P such that A consists precisely of the points and lines not contained in H. Also, two lines of A are parallel if and only if they meet in the same point of H. The hyperplane H is the *hyperplane at infinity* of A.

2.40 For a finite affine space A, there is a positive integer n such that any line of A has exactly n points. This number n is the *order* of A. The *dimension* of an affine space is the dimension of the corresponding projective space.

2.41 **Theorem** Let A be a finite affine space of dimension d and order n.

1. The number of points of A is n^d.
2. If U is a t-dimensional subspace of A, then the quotient geometry A/U is a projective space of dimension $d-t-1$ and order n.

2.42 $\mathrm{AG}(d,q)$ denotes the affine space of dimension d and order q with projective closure equal to $\mathrm{PG}(d,q)$.

2.43 In $\mathrm{AG}(d,q)$ the cosets of $\{\bar{0}\}$ are *points*, those of 1-dimensional spaces *lines*, those of $(d-1)$-dimensional spaces *hyperplanes*; in general, the cosets of i-dimensional subspaces are *i-flats*. The points of $\mathrm{AG}(d,q)$ together with the i-dimensional flats of $\mathrm{AG}(d,q)$ as blocks and incidence by natural containment form an incidence structure denoted by $\mathrm{AG}_i(d,q)$.

2.44 **Proposition** $\mathrm{AG}_i(d,q)$ is a block design with parameters $v=q^d$, $k=q^i$ and $\lambda=\begin{bmatrix} d-1 \\ i-1 \end{bmatrix}_q$ (also $b=q^{d-i}\begin{bmatrix} d \\ i \end{bmatrix}_q$ and $r=\begin{bmatrix} d \\ i \end{bmatrix}_q$).

2.45 **Theorem** (Buekenhout) Let A be a linear space that contains at least one line with at least four points. If any three noncollinear points generate an affine plane, then A is an affine space.

2.46 **Remark** Theorem 2.45 is false if one drops the hypothesis that there is a line with at least four points. Hall triple systems (§VI.28) give examples in which all lines have size three.

2.5 Subplanes

2.47 Let P be a projective plane with point set $\mathcal{P}$ and line set $\mathcal{L}$. A projective plane P' with point set $\mathcal{P}'$ and line set $\mathcal{L}'$ is a *subplane* of P if $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{L}' \subseteq \mathcal{L}$, and P' inherits the incidence relation from P.

2.48 Theorem (Bruck) Let P be a finite projective plane of order n, and let P' be a subplane of order $m < n$ of P. Then $n = m^2$ or $m^2 + m \leq n$.

2.49 A subplane of order m of a projective plane of order $n = m^2$ is a *Baer subplane*.

2.50 Theorem Let P be a finite projective plane of order n, and let P' be a subplane of order $m < n$ of P. Then these assertions are equivalent:

1. P' is a Baer subplane of P;
2. any point outside P' is on exactly one line of P';
3. any line not in P' has exactly one point in common with P'.

2.51 Remarks Let $P = \mathrm{PG}(2, F)$, with F the field $\mathbb{F}_q$. Let K be a subfield of F and consider the geometry P' consisting of the homogeneous coordinates for points and lines whose entries are in K. Then P' is a subplane of P.

The subfields of a finite field $\mathbb{F}_{p^a}$, where p is a prime, are precisely those fields $\mathbb{F}_{p^b}$ where b divides a. The subplanes of a projective plane $\mathrm{PG}(2, p^a)$, with p a prime, are exactly the projective planes $\mathrm{PG}(2, p^b)$ where b divides a.

2.52 Proposition A projective plane $\mathrm{PG}(2, q)$ has a Baer subplane if and only if q is a square.

2.6 Baer Subgeometries

2.53 Let P be a projective space with point set $\mathcal{P}$ and line set $\mathcal{L}$. A projective space P' with point set $\mathcal{P}'$ and line set $\mathcal{L}'$ is a *subgeometry* of P if $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{L}' \subseteq \mathcal{L}$, and $\mathcal{P}'$ inherits the incidence relation of $\mathcal{P}$.

2.54 Proposition (Bruck) Let P be a finite projective space of dimension d and order q. Let P' be a subgeometry of P of order q'. If $q' < q$, then $q' \leq \sqrt{q}$.

2.55 A d-dimensional subgeometry of $\mathrm{PG}(d, q)$, whose order is $\sqrt{q}$, is a *Baer subgeometry* of $\mathrm{PG}(d, q)$.

2.56 Theorem If $P = P(V)$ is a finite desarguesian projective space of order $q = p^n$, p prime, then P has a subgeometry of order q' if and only if $q' = p^m$ with $m \mid n$. In particular, P has a Baer subgeometry if and only if q is a square.

2.57 Theorem Let B be a Baer subgeometry of $P = \mathrm{PG}(d, q)$.

1. If U is an i-dimensional subspace of P that intersects B in a j-dimensional subspace, then there is precisely one subspace of dimension $2i-j$ of B containing U. In particular, if U has no point in common with B, then U is contained in a unique $(2i+1)$-dimensional subspace of B. So, any point of $P \setminus B$ lies on a unique line of B.
2. Any subspace of dimension $d-i$ of P contains at least one subspace of dimension $d-2i$ of B; this bound is sharp.

2.7 Collineations

2.58 Let P be a projective space of dimension at least two. A *collineation* (*automorphism*) of P is a bijective map α on the point set of P that preserves collinearity; that is, P, Q, R collinear implies $\alpha(P)$, $\alpha(Q)$, $\alpha(R)$ collinear. All collineations of P form the *full collineation group* $\mathrm{Aut}P$ of P. A *collineation group* of P is a subgroup of $\mathrm{Aut}P$.

2.59 Let $P = P(V)$ be a projective space defined over the F-vector space V. A *semilinear map* of V is a map $f : V \to V$ together with an automorphism σ of F such that $f(v + w) = f(v) + f(w)$ for all $v, w \in V$, and $f(a \cdot v) = \sigma(a) \cdot f(v)$ for all $a \in F$, $v \in V$.

2.60 **Theorem** (*Fundamental theorem of projective geometry*) Any invertible semilinear map of V induces a collineation of $P(V)$. Conversely, any collineation of $P(V)$, $\dim V \geq 3$, is induced by an invertible semilinear map.

2.61 The group of all collineations of the d-dimensional projective space $P(V) = \mathrm{PG}(d, F)$, $d \geq 2$, is denoted by $\mathrm{P\Gamma L}(d+1, F)$. The set $\mathrm{PGL}(d+1, F)$ of collineations that are induced by invertible linear maps of V is a normal subgroup of $\mathrm{P\Gamma L}(d+1, F)$. The set of collineations $\mathrm{PSL}(d+1, F)$ induced by linear maps with determinant 1 is a group of collineations, the *little projective group* of $P(V)$.

2.62 Let P be a projective space. A collineation α of P is a *central collineation* if there exists a point C (the *center*) and a hyperplane H (the *axis*) such that α fixes any line on C and any point on H. If α is a central collineation different from the identity, its center and axis are uniquely determined. A central collineation different from the identity, with center C and axis H, is an *elation* if $C \in H$ and a *homology* otherwise.

2.63 A *Baer collineation* is a collineation that fixes a Baer subgeometry pointwise.

2.64 **Theorem** (Baer) A collineation of order 2 of a projective space is either a central collineation or a Baer collineation.

2.65 **Theorem** The number of fixed points of a collineation of P equals the number of fixed hyperplanes of P.

2.66 **Theorem** Let G be an arbitrary automorphism group of a finite projective space P.

1. The number of point orbits of P equals the number of hyperplane orbits.
2. The group G is point-transitive if and only if it is transitive on the hyperplanes.
3. The group G is 2-fold transitive on the points of P if and only if it is 2-fold transitive on the hyperplanes of P.

2.8 Spreads

2.67 Let t and d be positive integers with $t < d$. A *t-spread* in a d-dimensional projective space P is a set S of t-dimensional subspaces such that any point of P is on exactly one element of S.

2.68 **Theorem** A finite projective space $P = \mathrm{PG}(d, q)$ contains a t-spread if and only if $(t+1)|(d+1)$. In particular, $\mathrm{PG}(d, q)$ contains a spread of lines if and only if d is odd.

2.69 **Construction** One construction for t-spreads is as follows. Let t and d be positive integers such that $(t + 1)|(d + 1)$. Let q be a prime power. Then the field $F^\star = \mathbb{F}_{q^{d+1}}$ of order q^{d+1} contains $F = \mathbb{F}_{q^{t+1}}$ as a subfield. Consider $F^\star$ as an F-vector space.

Then the set of 1-dimensional subspaces of $F^\star$ over F forms a t-spread in the d-dimensional projective space associated to the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^{d+1}}$. The t-spreads obtained in this way are *regular* (see Definition 2.73).

2.70 A *t-regulus* of $\mathrm{PG}(2t+1,q)$ is a set R of $q+1$ mutually skew t-dimensional subspaces such that any line intersecting three elements of R intersects all elements of R. These lines are *transversals* of R.

2.71 Proposition Any three mutually skew t-dimensional subspaces of $\mathrm{PG}(2t+1,q)$ determine a unique t-regulus containing them.

2.72 Remark The points covered by a 1-regulus in $\mathrm{PG}(3,q)$ are the points of a hyperbolic quadric.

2.73 A t-spread S in $\mathrm{PG}(2t+1,q)$ is *regular* if for any three elements of S, the t-regulus determined by them is also contained in S. In general, a t-spread S of $P=\mathrm{PG}(d,q)$ is *regular*, if for any two elements, U, W of S, S induces a regular t-spread in $\langle U,W\rangle$.

2.74 Theorem A finite projective space $P=\mathrm{PG}(d,q)$ contains a regular t-spread if and only if $t+1$ divides $d+1$.

2.75 Remark There are many spreads that are not regular. One class of examples is obtained as follows. Let $t=1$. First of all, the set of transversals of a 1-regulus R is again a 1-regulus, the *opposite* 1-regulus of R. Start with a regular 1-spread S_0. Replace one 1-regulus of S_0 by its opposite 1-regulus to obtain a 1-spread S_1. If S_1 contains a 1-regulus, replace this 1-regulus by its opposite 1-regulus to obtain S_2. Continue in this manner. Any 1-spread so obtained is *subregular*.

2.9 Arcs, Ovals, Hyperovals, and Normal Rational Curves

2.76 A *k-arc* in a projective plane is a set of k points, no three collinear.

2.77 Theorem If a projective plane of order q has a k-arc, then $k\leq q+2$. If $k=q+2$, then q is even.

2.78 Let P be a projective plane of order q. An *oval* of P is a $(q+1)$-arc, and a *hyperoval* is a $(q+2)$-arc.

2.79 Examples The *conics* are examples of ovals in $\mathrm{PG}(2,q)$. Let $\mathrm{PG}(2,q)$ be described by homogeneous coordinates. Then a conic is the set of points $(x:y:z)$ satisfying a quadratic equation equivalent to $x^2=yz$.

2.80 Theorem (Segre) In $\mathrm{PG}(2,q)$, q odd, every oval is a conic.

2.81 Proposition Any oval in a projective plane of even order q can uniquely be extended to a hyperoval. The reason for this is that for q even all tangents to a $(q+1)$-arc pass through a common point, the *nucleus* of the $(q+1)$-arc.

2.82 Examples The *regular* hyperovals that consist of the union of a conic and its nucleus are the classical examples of hyperovals in $\mathrm{PG}(2,q)$, q even. In $\mathrm{PG}(2,q)$, q even, $q\geq 16$, infinite classes of *nonregular hyperovals* are known. Every hyperoval in $\mathrm{PG}(2,q)$, q even, is projectively equivalent to a hyperoval $\{(1:x:F(x))|x\in\mathbb{F}_q\}\cup\{(0:1:0),(0:0:1)\}$, for some polynomial F with $F(0)=0$ and $F(1)=1$. Next to the infinite classes of hyperovals presented in the next table, there also exists a sporadic hyperoval in $\mathrm{PG}(2,32)$.

2.83 **Table** [1106] Infinite classes of hyperovals.

Name	$q=2^h$	$F(X)$	Conditions
Regular		X^2	
Translation		X^{2^i}	$(h,i)=1$
Segre	h odd	X^6	
Glynn I	h odd	$X^{3\sigma+4}$	$\sigma=2^{(h+1)/2}$
Glynn II	h odd	$X^{\sigma+\lambda}$	$\sigma=2^{(h+1)/2}$; $\lambda=2^m$ if $h=4m-1$; $\lambda=2^{3m+1}$ if $h=4m+1$
Payne	h odd	$P(X)$	
Cherowitzo	h odd	$C(X)$	$\sigma=2^{(h+1)/2}$
Subiaco	$h=4r+2$	$S_1(X)$	$\omega^2+\omega+1=0$
Subiaco	$h=4r+2$	$S_2(X)$	$\delta=\zeta^{q-1}+\zeta^{1-q}$; ζ primitive in $\mathbb{F}_{q^2}$
Subiaco	$h\neq 4r+2$	$S_3(X)$	$T_2(1/\delta)=1$
Adelaide	h even, $h\geq 4$	$S(X)$	$\beta\in\mathbb{F}_{q^2}\setminus\{1\}$, $\beta^{q+1}=1, T(x)=x+x^q$, $m\equiv\pm(q-1)/3 \pmod{q+1}$

Here $P(X)=X^{1/6}+X^{3/6}+X^{5/6}$; $C(X)=X^\sigma+X^{\sigma+2}+X^{3\sigma+4}$;
$S_1(X)=\frac{\omega^2(X^4+X)}{X^4+\omega^2X^2+1}+X^{1/2}$; $S_2(X)=\frac{\delta^2X^4+\delta^5X^3+\delta^2X^2+\delta^3X}{X^4+\delta^2X^2+1}+\left(\frac{X}{\delta}\right)^{1/2}$;
$S_3(X)=\frac{(\delta^4+\delta^2)X^3+\delta^3X^3+\delta^2X}{X^4+\delta^2X^2+1}+\left(\frac{X}{\delta}\right)^{1/2}$; and
$S(X)=\frac{T(\beta^m)(X+1)}{T(\beta)}+\frac{T((\beta X+\beta^q)^m)}{T(\beta)(X+T(\beta)X^{1/2}+1)^{m-1}}+X^{1/2}$.

The function T_2 is the *trace function* $T_2:\mathbb{F}_{2^h}\to\mathbb{F}_2: x\mapsto\sum_{i=0}^{h-1}x^{2^i}$.

2.84 **Theorem** In $\mathrm{PG}(2,2)$, $\mathrm{PG}(2,4)$, and $\mathrm{PG}(2,8)$, every hyperoval is regular. In $\mathrm{PG}(2,16)$, there exist exactly two distinct hyperovals: the regular hyperoval and the Subiaco hyperoval, also known as the *Lunelli–Sce hyperoval*. In $\mathrm{PG}(2,32)$, there exist exactly six distinct hyperovals: the regular hyperoval, the translation hyperoval defined by $F(X)=X^4$, the Segre hyperoval, the Payne hyperoval, the Cherowitzo hyperoval, and the sporadic *O'Keefe–Penttila hyperoval*.

2.85 A k-arc of $\mathrm{PG}(2,q)$ is *complete* if it is not properly contained in a $(k+1)$-arc of $\mathrm{PG}(2,q)$.

2.86 **Table** [1106] Extendability of arcs to larger arcs. Any k-arc, with $k>k_0$, in $\mathrm{PG}(2,q)$ is contained in a K_0-arc of $\mathrm{PG}(2,q)$. In the table, for $q=2^{2e}$, $e>2$, two possible values for K_0 occur since in any projective plane $\mathrm{PG}(2,q)$, $q>4$ square, there exists a complete $(q-\sqrt{q}+1)$-arc. Here, p is always a prime.

q	k_0	K_0
$q=p^{2e},\ p>2,\ e\geq 1$	$q-\sqrt{q}/4+25/16$	$q+1$
$q=p^{2e+1},\ p>2,\ e\geq 1$	$q-\sqrt{pq}/4+29p/16+1$	$q+1$
q prime, $q>2$	$44q/45+8/9$	$q+1$
$q=p^h,\ p\geq 5$	$q-\sqrt{q}/2+5$	$q+1$
$q=p^h,\ p\geq 3,\ q\geq 23^2$, $q\neq 5^5,\ 3^6,\ h$ even for $p=3$	$q-\sqrt{q}/2+3$	$q+1$
$q=2^{2e},\ e>2$	$q-2\sqrt{q}+6$	$q+2$ or $q-\sqrt{q}+1$
$q=2^{2e+1},\ e\geq 1$	$q-\sqrt{2q}+2$	$q+2$

2.87 **Table** [1106] Exact values for $m'(2,q)$, the size of the second largest complete arcs in $\mathrm{PG}(2,q)$, for small values of q.

q	7	8	9	11	13	16	17	19	23	25	27	29
$m'(2,q)$	6	6	8	10	12	13	14	14	17	21	22	24

2.88 **Theorem** In $\mathrm{PG}(2,q)$, with $q=2^h$, if $h\geq 4$ is even, then $m'(2,q)=q-\sqrt{q}+1$.

2.89 A *k-arc* in $\mathrm{PG}(d,q)$ is a set of k points, no $d+1$ dependent. A k-arc of $\mathrm{PG}(d,q)$ is *complete* if it is not properly contained in a $(k+1)$-arc of $\mathrm{PG}(d,q)$.

2.90 **Table** [1106] The value of $m(d,q)$, the size of the largest arcs in $\mathrm{PG}(d,q)$, for small dimensions d. The characterization of the $m(d,q)$-arcs L in $\mathrm{PG}(d,q)$ is given in the last column. NRC denotes a normal rational curve.

q	d	$m(d,q)$	L
q odd, $q>3$	3	$q+1$	NRC
$q=2^h,\ q>4$	3	$q+1$	$L_e,\ e=2^v,\ (v,h)=1$
q odd, $q>5$	4	$q+1$	NRC for $q>83$
$q=2^h,\ q>4$	4	$q+1$	NRC
$q=2^h,\ q\geq 8$	5	$q+1$	NRC for $q\geq 16$
$q=2^h,\ q\geq 16$	6	$q+1$	NRC for $q>64$
$q=p^h$	$d\geq q-1$	$d+2$	$\{e_0,\ldots,e_d,e\}$

Here $e_0=(1:0:\ldots:0), e_1=(0:1:0:\ldots:0),\ldots,e_d=(0:0:\ldots:0:1)$, and $e=(1:\ldots:1)$. *NRC* stands for *normal rational curve*, that is, a $(q+1)$-arc in $\mathrm{PG}(d,q)$, $2\leq d\leq q-2$, equivalent to the $(q+1)$-arc $\{(1:t:\ldots:t^d)|t\in\mathbb{F}_q^+\}$, where $\mathbb{F}_q^+=\mathbb{F}_q\cup\{\infty\}$ and where $t=\infty$ defines the point e_d. In $\mathrm{PG}(3,q)$, $q=2^h$, $h>2$, $L_e=\{(1:t:t^e:t^{e+1})|t\in\mathbb{F}_q^+\}$, with $e=2^v$, $(v,h)=1$, and with $t=\infty$ defining the point $e_3=(0:0:0:1)$.

2.91 **Table** [1106] Extendability of arcs to larger arcs in $\mathrm{PG}(d,q)$. Any k-arc in $\mathrm{PG}(d,q)$, with k larger than the value in column three is extendable to a $(q+1)$-arc L in $\mathrm{PG}(d,q)$, which is either a normal rational curve or a $(q+1)$-arc equivalent to L_e (Table 2.90). The type of the $(q+1)$-arc L is denoted in the fourth column. Here, p is a prime.

d	q	$q+1\geq k>$	L
≥ 2	$q=p^{2e},\ p$ odd, $e\geq 1$	$q-\sqrt{q}/4+d-7/16$	NRC
≥ 2	$q=p^{2e+1},\ p$ odd, $e\geq 1$	$q-\sqrt{pq}/4+29p/16+d-1$	NRC
≥ 2	q prime, $q>2$	$44q/45+d-10/9$	NRC
≥ 2	$q=p^h,\ p\geq 5$	$q-\sqrt{q}/2+d+3$	NRC
≥ 2	$q=p^h,\ p\geq 3,\ q\geq 23^2$, h even for $p=3$, $q\neq 5^5,\ 3^6$	$q-\sqrt{q}/2+d+1$	NRC
3	$q=2^h, h>1$	$q-\sqrt{q}/2+9/4$	L_e
≥ 4	$q=2^h,\ h>2$	$q-\sqrt{q}/2+d-3/4$	NRC

2.92 **Table** [1106] Values of k for which there exist complete k-arcs in the respective spaces $\mathrm{PG}(d,q)$, d large. The last column indicates when the $(q+1)$-arcs in these spaces are always normal rational curves. Here, p is a prime.

q	d	$k\in$	
$q=p^{2e},\ e\geq 1,\ p>2$	$q-2\geq d>q-\sqrt{q}/4-39/16$	$\{q+1\}$	NRC
$q=p^{2e+1},\ e\geq 1,\ p>2$	$q-2\geq d>q-\sqrt{pq}/4+29p/16-3$	$\{q+1\}$	NRC
q prime, $q>2$	$q-2\geq d>44q/45-28/9$	$\{q+1\}$	NRC
$q=p^h,\ p\geq 5$	$q-2\geq d>q-\sqrt{q}/2+1$	$\{q+1\}$	NRC
$q=p^h,\ p\geq 3,\ q\neq 5^5,\ 3^6$, $q\geq 23^2,\ h$ even for $p=3$	$q-2\geq d>q-\sqrt{q}/2-1$	$\{q+1\}$	NRC
$q=2^h,\ q\geq 32,\ q\neq 64$	$q-5\geq d>q-\sqrt{q}/2-11/4$	$\{d+4,$ $d+5,\ q+1\}$	NRC
$q=64$	$d=58$ or $d=59$	$\{d+4,\ q+1\}$	NRC
$q=2^h,\ q\geq 8$	$q-4$	$\{q,\ q+1\}$	
$q=2^h,\ q\geq 8$	$q-3$	$\{q+1\}$	
$q=2^h,\ q\geq 4$	$q-2$	$\{q+2\}$	

2.93 **Table** [1106] Value of $m'(3,q)$, the size of the second largest complete k-arcs in $\mathrm{PG}(3,q)$, for small q.

q	8	9	11	13	16	17	19	25
$m'(3,q)$	7	9	9	10	12	13	14	18

2.94 **Table** [1106] For the indicated spaces $\mathrm{PG}(d,q)$, $2 \le d \le q-2$, it is stated if every $(q+1)$-arc is a normal rational curve, the values of d for which $m(d,q) = q+1$, and if there exist $(q+2)$-arcs.

q	$(q+1)$-arc = NRC	$m(d,q) = q+1$	$(q+2)$-arcs
$5 \le q \le 27,\ q \ne 9,\ q$ odd	$d \in \{2,\dots,q-2\}$	$d \in \{2,\dots,q-2\}$	
$8, 16$	$d \in \{3,\dots,q-4\}$	$d \in \{3,\dots,q-3\}$	$d \in \{2, q-2\}$
9	$d \in \{2,3\} \cup \{5,6,7\}$	$d \in \{2,\dots,7\}$	

2.95 **Remark** Theorem 2.96 presents the only presently known $(q+1)$-arc in $\mathrm{PG}(d,q)$, $2 \le d \le q-2$, q odd, different from a normal rational curve.

2.96 **Theorem** (Glynn) In $\mathrm{PG}(4,9)$, a 10-arc is either a normal rational curve or a 10-arc projectively equivalent to the 10-arc $L = \{(1 : t : t^2 + \eta t^6 : t^3 : t^4) | t \in \mathbb{F}_9\} \cup \{(0:0:0:0:1)\}$, where $\eta^4 = -1$.

2.10 {k; r}-Arcs

2.97 A $\{k;r\}$-*arc* in a projective plane is a set K of k points such that r is the maximum number of points in K that are collinear. A $\{k;2\}$-arc is a *k-arc*.

2.98 **Theorem** (Barlotti) Let K be a $\{k;r\}$-arc in a projective plane of order q. Then $k \le (q+1)(r-1)+1$.

2.99 The $\{k;r\}$-arcs for which $k = (q+1)(r-1)+1$ are *maximal $\{k;\ r\}$-arcs*.

2.100 **Examples** The singletons ($k = r = 1$) and the whole plane ($r = q+1$) are *trivial* maximal $\{k;r\}$-arcs. The hyperovals are nontrivial maximal $\{k;r\}$-arcs.

2.101 **Lemma** (Barlotti) If a projective plane of order q contains a maximal $\{k;r\}$-arc, then r must be a divisor of q.

2.102 **Table** [1106] Known exact values for $m_r(2,q)$, the size of the largest $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$.

r	$q = p^h,\ p$ prime	$m_r(2,q)$
2	q odd	$q+1$
2^e	2^h	$(2^e-1)q + 2^e$
$\sqrt{q}+1$	q square, $q \ge 25$	$q\sqrt{q}+1$
$(q+1)/2$	q odd prime	$(q^2-q)/2+1$
$(q+3)/2$	q odd prime	$(q^2+q)/2+1$
q	q	q^2
$q-1$	q square, $q > 4$	$q^2 - q - 2\sqrt{q} - 1$
$q-2$	q odd square, $q > 121$	$q^2 - 2q - 3\sqrt{q} - 2$
$q+1-t$, $t > 1$	$q = p^{2e},\ p = 2,3,$ $t < \min(2^{-1/3}q^{1/6}, q^{1/4}/2)$	$q^2 + q + 1 - t(q + \sqrt{q} + 1)$
$q+1-t$, $t > 1$	$q = p^{2e},\ p > 3,$ $t < \min(q^{1/6}, q^{1/4}/2)$	$q^2 + q + 1 - t(q + \sqrt{q} + 1)$

2.103 Theorem (Ball, Blokhuis, and Mazzocca) If $\mathrm{PG}(2,q)$ contains a nontrivial maximal $\{k;r\}$-arc, then q is even.

2.104 Theorem (Denniston) In $\mathrm{PG}(2,q)$, $q=2^h$, for any $r=2^{h'}$ with $0\le h'\le h$, there exists a maximal $\{k;r\}$-arc.

2.105 Remark The construction method of Denniston for maximal $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$, q even, was generalized by Mathon [1542]. Hamilton and Mathon used this generalized method to construct many new maximal $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$, q even [1028].

2.106 Table [1106] Lower bounds on $m_r(2,q)$.

r	q	$m_r(2,q)\ge$
$r=3$	q exceptional	$q+\lfloor 2\sqrt{q}\rfloor$
$r=\sqrt{q}+1$	q square	$(r-1)q+1$
$r=(q+1)/2$	q odd	$(r-1)q+1$
$r=(q+3)/2$	q odd	$(r-1)q+1$
$r=q-1$	q	$(r-1)q+1$
$r=q-2$	q even	$(r-1)q+2$
r	q square	$(r-1)q+r-\sqrt{q}+\sqrt{q}(r-q)$
$r=q-\sqrt{q}$	q square	$(r-1)q+\sqrt{q}$
$(q-r)\mid q$	q	$(r-1)q+q-r$

2.107 Remark A major problem is the construction of *large* $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$. Because the union of t conics is a $\{k;2t\}$-arc, it follows that $m_r(2,q)\ge\lfloor r/2\rfloor(q+1)$. Theorem 2.108 gives an asymptotic lower bound on $m_r(2,q)$.

2.108 Theorem [1107] For every $\epsilon>0$ and $\delta>0$, there is a $q_0=q_0(\epsilon,\delta)$ such that for every $r>q^{1/2+\delta}$, $m_r(2,q)\ge(1-\epsilon)rq$ when $q>q_0$.

2.109 Table [1106] Known upper bounds on $m_r(2,q)$.

r	Conditions	$m_r(2,q)\le$
r	all q	$(r-1)q+r$
r	q odd	$(r-1)q+r-2$
r	q odd, $r\mid q$	$(r-1)q+r/2$
r	$4\le r<q$, $r\nmid q$	$(r-1)q+r-3$
r	$9\le r<q$, $r\nmid q$	$(r-1)q+r-4$
r	q prime, $r\ge(q+3)/2$	$(r-1)q+r-(q+1)/2$
r	$r\le 2q/3$	$(r-1)q+q-r$
r	$r\ge q/2$, $(r,q)>1$, K has a skew line	$(r-1)q+q-r$
r	$r>2q/3$	$(r-1)q+(q+r-r/q)/2-\sqrt{(q+r-r/q)^2/4-(r^2-r)}$
r	no skew line to K	$rq-\sqrt{(q+1-r)q}$
r	no skew line to K	$m_r(2,q)\le(r-1)q+\lfloor r^2/q\rfloor$
r	no skew line to K, $\sqrt{q}\mid r$	$m_r(2,q)<(r-1)q+\lfloor r^2/q\rfloor$
r	$(r,q)=1$, $r<\sqrt{q}+1$	$(r-1)q+1$
r	$(r,q)=1$; $6\le r\le\sqrt{2q}+1\le q-1$	$(r-1)q+1$
r	$(r,q)=p^e$, K has a skew line	$(r-1)q+p^e$
r	q prime, $r\le(q+1)/2$	$(r-1)q+1$

2.110 Table [152] The known exact values and known intervals for $m_r(2,q)$, q small.

$r\backslash q$	3	4	5	7	8	9	11	13	16	17	19
2	4	6	6	8	10	10	12	14	18	18	20
3		9	11	15	15	17	21	23	$28-33$	$28-35$	$31-39$
4			16	22	28	28	$32-34$	$38-40$	52	$48-52$	$52-58$
5				29	33	37	$43-45$	$49-53$	65	$61-69$	$68-77$
6				36	42	48	56	$64-66$	$78-82$	$78-86$	$86-96$
7					49	55	67	79	$93-97$	$94-103$	$105-115$
8						65	$77-78$	92	120	$114-120$	$124-134$
9							$89-90$	105	$128-131$	137	$147-153$
10							$100-102$	$118-119$	$142-148$	154	172
11								$132-133$	$159-164$	$166-171$	191
12								$145-147$	$180-181$	$182-189$	$204-210$
13									$195-199$	$205-207$	$225-230$
14									$210-214$	$221-225$	$242-250$
15									231	$239-243$	$265-270$
16										$256-261$	$285-290$
17											$305-310$
18											$324-330$

2.111 Remark Maximal arcs are used to construct partial geometries (see §VI.41.3).

2.11 Caps

2.112 A *k-cap* in $\mathrm{PG}(d,q)$ is a set of k points, no three collinear. A k-cap of $\mathrm{PG}(d,q)$ is *complete* when this k-cap is not contained in a $(k+1)$-cap of $\mathrm{PG}(d,q)$.

2.113 Remark In $\mathrm{PG}(2,q)$, the definitions of k-caps and of k-arcs coincide.

2.114 The maximal size of a cap in $\mathrm{PG}(d,q)$ is denoted by $m_2(d,q)$, and the size of the second largest complete cap in $\mathrm{PG}(d,q)$ is denoted by $m_2'(d,q)$.

2.115 Table [1106] The known exact values for $m_2(d,q)$, $d \geq 3$.

q	d	$m_2(d,q)$	q	d	$m_2(d,q)$	q	d	$m_2(d,q)$
q odd	3	q^2+1	$q=2$	d	2^d	$q=3$	5	56
q even, $q>2$	3	q^2+1	$q=3$	4	20	$q=4$	4	41

2.116 A *(q^2+1)-cap* in $\mathrm{PG}(3,q)$, $q>2$, is an *ovoid* of $\mathrm{PG}(3,q)$.

2.117 Examples The elliptic quadrics in $\mathrm{PG}(3,q)$, $q>2$, and the *Tits ovoids* in $\mathrm{PG}(2,2^{2e+1})$, $e \geq 1$, are the known examples of ovoids. An elliptic quadric in $\mathrm{PG}(3,q)$ is a quadric having a quadratic equation equivalent to $f(X_0,X_1)+X_2X_3=0$, where $f(X_0,X_1)$ is a homogeneous irreducible quadratic polynomial over $\mathbb{F}_q$.

The Tits ovoids are ovoids in $\mathrm{PG}(3,2^{2e+1})$, $e \geq 1$, projectively equivalent to $K = \{(0:1:0:0)\} \cup \{(1:z:y:x) | z = xy + x^{\sigma+2} + y^{\sigma},$ with $(x,y) \in \mathbb{F}_q^2$ and $\sigma = 2^{e+1}\}$. Tits ovoids are not projectively equivalent to elliptic quadrics.

2.118 Theorem In $\mathrm{PG}(2,4)$ and in $\mathrm{PG}(2,16)$, every ovoid is an elliptic quadric. In $\mathrm{PG}(2,8)$ and in $\mathrm{PG}(2,32)$, every ovoid is an elliptic quadric or a Tits ovoid.

2.119 Table [1106] Exact and upper bounds on $m_2'(d,q)$. The type of the $m_2(d,q)$-cap in $\mathrm{PG}(d,q)$ to which a k-cap of $\mathrm{PG}(d,q)$, with $k > m_2'(d,q)$, can be extended is given in the last column. The second table specializes to the case $d = 3$. Here, p is a prime.

d	q	$m_2'(d,q)$	$m_2(d,q)$-cap
3	q even, $q \geq 8$	$\leq q^2 - q + 5$	ovoid
3	3	$= 8$	elliptic quadric
3	4	$= 14$	elliptic quadric
3	5	$= 20$	elliptic quadric
3	7	$= 32$	elliptic quadric
4	3	$= 19$	20-cap
5	3	$= 48$	56-cap
d	2	$= 2^{d-1} + 2^{d-3}$	complement of a hyperplane

q odd, $q \geq 17$	$m_2'(3,q) <$	$m_2(3,q)$-cap
$q = p^{2e},\ p > 2,\ e \geq 1$	$q^2 - q^{3/2}/4 + 39q/64 + O(q^{1/2})$	elliptic quadric
$q = p^{2e+1},\ p > 2,\ e \geq 1$	$q^2 - p^{3e+2}/4 + 119p^{2e+2}/64 - O(p^{e+2})$	elliptic quadric
q prime, $q > 2$	$2641q^2/2700 - 4q/135 + 94/27$	elliptic quadric
$q = p^h,\ p \geq 5$	$q^2 - q^{3/2}/2 + 67q/16 - O(q^{1/2})$	elliptic quadric
$q \geq 23^2,\ q = p^h,\ p \geq 3,$ h even for $p = 3,\ q \neq 5^5,\ 3^6$	$q^2 - q^{3/2}/2 + 35q/16 + O(q^{1/2})$	elliptic quadric

2.120 Theorem (Davydov and Tombak) In $\mathrm{PG}(d,2)$, $d \geq 3$, a complete k-cap K, with $d \geq 2^{d-1} + 1$, has order $k = 2^{d-1} + 2^{d-1-g}$ for some $g = 0, 2, 3, \ldots, d-1$. For each $g = 0, 2, 3, \ldots, d-1$, there exists a complete $(2^{d-1} + 2^{d-1-g})$-cap in $\mathrm{PG}(d,2)$.

2.121 Table [1106] The known upper bounds on $m_2(4,q)$.

$q = p^h,\ p$ prime	$m_2(4,q)$
q even, $q \geq 8$	$\leq q^3 - q^2 + 6q - 3$
$q = p^{2e},\ p > 2,\ e \geq 1,\ q \geq 49$	$< q^3 - q^{5/2}/4 + 39q^2/64 + O(q^{3/2})$
$q = p^{2e+1},\ p > 2,\ e \geq 1$	$< q^3 - p^{e+1}q^2/4 + 119pq^2/64 - O(p^{e+2}q)$
q prime, $q \geq 37$	$< 2641q^3/2700 - 79q^2/2700 + O(q)$
$q = p^h,\ p \geq 5,\ q \geq 19$	$< q^3 - q^{5/2}/2 + 67q^2/16 - O(q^{3/2})$
$q \geq 23^2,\ q = p^h,\ p \geq 3,$ h even for $p = 3,\ q \neq 5^5,\ 3^6$	$< q^3 - q^{5/2}/2 + 35q^2/16 + O(q^{3/2})$

2.122 Table [1106] The known upper bounds on $m_2(d,q)$.

$q = p^h,\ p$ prime	$m_2(d,q)$
q even, $q \geq 16$	$m_2(5,q) < q^4 - q^3 + 5q^2 + 3q - 1$
q even, $q \geq 16,\ d \geq 6$	$< q^{d-1} - q^{d-2} + 5q^{d-3} + 2q^{d-4} + O(q^{d-5})$
$q = p^{2e},\ e \geq 1,\ q \geq 49$	$< q^{d-1} - q^{d-3/2}/4 + 39q^{d-2}/64 + O(q^{d-5/2})$
$q = p^{2e+1},\ e \geq 1$	$< q^{d-4}(q^3 - p^{e+1}q^2/4 + 119pq^2/64 - O(p^{e+2}q))$
q prime, $q \geq 37$	$< 2641q^{d-1}/2700 - 79q^{d-2}/2700 + O(q^{d-3})$
$q = p^h,\ p \geq 5,\ q \geq 19$	$< q^{d-1} - q^{d-3/2}/2 + 67q^{d-2}/16 - O(q^{d-5/2})$
$q \geq 23^2,\ q = p^h,\ p \geq 3,$ h even for $p = 3,\ q \neq 5^5,\ 3^6$	$< q^{d-1} - q^{d-3/2}/2 + 35q^{d-2}/16 + O(q^{d-5/2})$
$q > 3,\ d \geq 3$	$q^d \cdot (d+1)/(d^2) + q^{d-1} \cdot 3 \cdot d/(2(d-1)^2)$

2.123 Table [1106] The known lower bounds on $m_2(d,q)$, for small d.

q	d	$m_2(d,q) \geq$	q	d	$m_2(d,q) \geq$
q even, $q>4$	4	$2q^2+q+9$	$q \equiv 7 \pmod 8$	4	$(5q^2-4q-9)/2$
$q \equiv 1 \pmod 8$	4	$(5q^2-2q-7)/2$	q odd	5	q^3+q^2+3q+3
$3<q \equiv 3 \pmod 8$	4	$(5q^2-8q-13)/2$	q even	5	q^3+2q^2+q+2
$q \equiv 5 \pmod 8$	4	$(5q^2-6q-11)/2$	q	6	q^4+2q^2

q	d	$m_2(d,q) \geq$	Condition
$q>4$	7	$aq^4+bq^3+cq^2+1$	$m_2(4,q) \geq aq^2+bq+c$
q even	8	$q^5+2q^4+2q^3+4q^2+q+2$	
q odd	8	$q^5+q^4+3q^3+3q^2+1$	
q	9	$q^6+2q^4+q^2$	

2.124 Table [1106] The known lower bounds on $m_2(d,q)$, for large values of d.

q	d	$m_2(d,q) \geq$
3	$6l$	$32^l((3l/8)(7/2)^{l-1}+1)$
3	$6l+v$, $v=7,\ldots,12$	$112^l m_2(v,3)$
>3	$6l$	$q^{4l}+(1+l)q^{4l-2}+(l^2-2l+1)q^{4l-4}$
>3	$6l+1$	$aq^{4l}+bq^{4l-1}+(c-a+al)q^{4l-2}+(bl-l)q^{4l-3}$
>3	$6l+2$	$aq^{4l+1}+bq^{4l}+(c-a+al)q^{4l-1}+(d-b+bl)q^{4l-2}$
>3	$6l+3$	$q^{4l+2}+(l+1)q^{4l}+(l^2-2l+3)q^{4l-2}/2$
>3	$6l+4$	$aq^{4l+2}+bq^{4l+1}+(al+c)q^{4l}+blq^{4l-1}$
>3	$6l+5$	$aq^{4l+3}+bq^{4l+2}+(c+al)q^{4l+1}+(d+bl)q^{4l}$

For $q>3$, the formulas for $d=1+6l$ and $d=4+6l$ start from $m_2(4,q) \geq aq^2+bq+c$, the one for $d=2+6l$ from $m_2(8,q) \geq aq^5+bq^4+cq^3+dq^2+eq+f$, and the one for $d=5+6l$ from $m_2(5,q) \geq aq^3+bq^2+cq+d$. For exact values of the parameters a,b,c,d,e,f, see Table 2.123. In the second formula for $q=3$, the corresponding lower bounds on $m_2(v,3)$ can be found in Table 2.125.

2.125 Table [1106] The sizes of the largest known caps in $\mathrm{PG}(d,q)$, for $d \geq 4$ and q small.

$d\backslash q$	3	4	5	7	8	9	11	13
4	20	41	66	132	208	212	316	388
5	56	126	186	434	695	840		
6	112	288	675	2499	4224	6723		
7	248	756	1715	6472	13520	17220		
8	532	2110	4700	21555	45174	68070		
9	1216	4938	17124	122500	270400	544644		
10	2744	15423	43876	323318	878800	1411830		
11	6464	34566	120740	1067080	2812160	5580100		
12	13312							

2.12 Unitals

2.126 A *unital* is a 2-$(n^3+1, n+1, 1)$ design, a geometry with n^3+1 points, $n+1$ points on each line such that any two distinct points are on exactly one line.

2.127 Remark Here the interest is not in abstract unitals (see Theorem II.5.11), but in unitals embedded in a projective plane of order $q=n^2$. The classical examples of unitals are obtained as follows.

2.128 Construction Let $P = \mathrm{PG}(2, q^2)$ be represented using homogeneous coordinates. Then the points $(x : y : z)$ for which $xx^q + yy^q + zz^q = 0$ form a unital. This unital is a *hermitian curve*.

2.129 Construction Another very important class of unitals are the *Buekenhout–Metz unitals*.

First, a description of the plane. Let $P = \mathrm{PG}(4, q)$ be the 4-dimensional projective space of order q and let H be a hyperplane of P. Let S be a spread of lines of H. Then the geometry $A(S)$ has as points those in $P \backslash H$ and as lines the planes of P that intersect H just in an element of S. Then $A(S)$ is an affine plane of order q^2 (Theorem 2.170). If the spread is regular, then $A(S)$ is desarguesian. Now fix a line $s \in S$ and consider a point $Q \in s$.

Then consider an ovoid O in a 3-dimensional space π_3 not through Q such that $H \cap \pi_3$ is the tangent plane to O in π_3 in the point $s \cap \pi_3$. Let U be the set of points, not in H, of the cone U with vertex Q and base O, together with the point at infinity of $A(S)$ corresponding to s. Then U is a unital in the projective closure of $A(S)$. If $A(S)$ is desarguesian one can choose O in such a way that U is not a hermitian curve.

2.130 Theorem (Penttila and Royle) In $\mathrm{PG}(2, 9)$, every unital is a Buekenhout–Metz unital.

2.13 Blocking Sets

2.131 Let P be a projective plane. A *blocking set* is a set B of points of P such that any line contains at least one point of B and at least one point outside B. A blocking set B in $\mathrm{PG}(2, q)$ is *small* when $|B| < 3(q+1)/2$.

2.132 Proposition Any projective plane P of order $q \neq 2$ contains a blocking set.

2.133 A blocking set B is *minimal* if through any point Q of B, there is a line only intersecting B in Q.

2.134 Examples Baer subplanes and unitals in projective planes of square order are classical examples of minimal blocking sets.

2.135 Theorem (Bruen, Bruen, and Thas) Let B be a minimal blocking set in a projective plane of order q. Then $q + \sqrt{q} + 1 \leq |B| \leq q\sqrt{q} + 1$, with $|B| = q + \sqrt{q} + 1$ if and only if B is a Baer subplane and with $|B| = q\sqrt{q} + 1$ if and only if B is a unital.

2.136 Theorem (Sziklai and Szőnyi) Let B be a small minimal blocking set in $\mathrm{PG}(2, q)$, $q = p^h$, p prime, $h \geq 1$. Then every line intersects B in 1 (mod p) points. The maximal integer e for which every line intersects B in 1 (mod p^e) points is a divisor of h.

2.137 Theorem Let B be a blocking set in $\mathrm{PG}(2, q)$, $q = p^h$, p prime, $h \geq 1$. Then

1. If $h = 0$, then $|B| \geq p + (p+3)/2$.
2. If h is even, then $|B| \geq q + \sqrt{q} + 1$.
3. If $h > 1$ is odd, then $|B| \geq q + p^e \lceil \frac{q/p^e+1}{p^e+1} \rceil + 1$, where $e < h$ is the largest divisor of h.

These bounds are sharp when $h = 1$, h even, or $h \equiv 0 \pmod 3$ with h odd.

2.138 Let P be a projective plane. A *t-fold blocking set* is a set B of points of P such that any line contains at least t points of B. A t-fold blocking set B in $\mathrm{PG}(2, q)$ is *small* when $|B| < tq + (q+3)/2$.

2.139 Remark The complement of a t-fold blocking set B in a projective plane of order q is a $\{k'; q+1-t\}$-arc K, with $k' = q^2 + q + 1 - |B|$. Due to this correspondence, t-fold

blocking sets are mainly studied for small values of t. For large values of t, instead of studying the t-fold blocking set, the complementary $\{k'; q+1-t\}$-arc is studied.

2.140 Theorem (Blokhuis, Lovász, Storme, and Szőnyi) Let B be a small minimal t-fold blocking set in $\mathrm{PG}(2,q)$, $q=p^h$, p prime, $h\geq 1$. Then every line of $\mathrm{PG}(2,q)$ intersects B in $t \pmod p$ points.

2.141 Example In $\mathrm{PG}(2,q)$, q square, it is possible to construct t-fold blocking sets by taking the union of t pairwise disjoint Baer subplanes.

2.142 Table [1106] Lower bounds on the cardinalities of t-fold blocking sets in $\mathrm{PG}(2,q)$.

$q=p^h,\ p$ prime	t	$\lvert B\rvert \geq$	Sharp
$q=p$ prime, $p>3$	$t<p/2$	$(2t+1)(p+1)/2$	for $t=1,(p-1)/2$
$q=p$ prime, $p>3$	$t>p/2$	$(t+1)p$	for $t=(p+1)/2$

q	t	Condition	$\lvert B\rvert \geq$
q	t	B does not contain a line	$tq+\sqrt{tq}+1$
q	t	B contains a line and $(t-1,q)=1$	$q(t+1)$
q	t	B contains a line and $(t-1,q)>1,\ t\leq q/2+1$	$tq+q-t+2$
q	t	B contains a line and $(t-1,q)>1,\ t\geq q/2+1$	$t(q+1)$

2.143 Table [1106] Lower bounds on the cardinalities of minimal t-fold blocking sets of $\mathrm{PG}(2,q)$ and characterization results. The first two columns give the conditions on q,t, and k. The last two columns give the structure of B, plus an implied lower bound on the value k. Here, p prime, $c_2=c_3=2^{-1/3}$ and $c_p=1$ if $p>3$.

q	$t,\ k=\lvert B\rvert-t(q+1)$	implies k	B
p^{2d+1}	$1\leq t<q/2-c_pq^{2/3}/2$	$\geq c_pq^{2/3}$	
$p^{2d}>4$	$1\leq t<c_pq^{1/6},\ k<c_pq^{2/3}$	$\geq t\sqrt{q}$	union of t disjoint Baer subplanes
p^2	$1\leq t<q^{1/4}/2,\ k<p\lceil\frac{1}{4}+\sqrt{\frac{p+1}{2}}\rceil$	$\geq t\sqrt{q}$	union of t disjoint Baer subplanes

q	$t,\ k=\lvert B\rvert-t(q+1)$, other conditions	implies k	remark
p^{6m}	$2\leq t<p^{3m/2}/4,\ k<p^{4m}\sqrt{p}/2$ no Baer subplane in B	$\geq tp^{4m}-4t^2p^{2m}$	
p^{6m+1}	$2\leq t<\dfrac{p^{3m/2+1/4}}{4},\ k<p^{4m+1}-2p^{2m+1}$	$\geq\max(tp^{4m}-4t^2p^{2m-1},$ $p^{4m+1}-p^{4m}-p^{2m+1}/2)$	$m\geq 1$
p^{6m+2}	$2\leq t<p^3/(4(p+1))$ if $m=1$; $2\leq t<p^{(3m+1)/2}/4$ if $m>1$; $k<p^{4m+2}/2$, no Baer subplane in B	$\geq tp^{4m+1}-4t^2p^{2m}$	$m\geq 1$; $p\geq 5$
p^{6m+3}	$2\leq t<p^{(6m+3)/4}/4,\ k<p^{4m+2}\sqrt{p}/2$	$\geq tp^{4m+2}-4t^2p^{2m+1}$	$p\geq 23$ ($m=0$); $p\geq 3$ ($m=1$)
p^{6m+4}	$2\leq t<p^{(3m+2)/2}/4,\ k<p^{4m+3}-2p^{2m+2}$ no Baer subplane in B	$\geq\max(tp^{4m+2}-4t^2p^{2m},$ $p^{4m+3}-p^{4m+2}-p^{2m+2}/2)$	$m\geq 1$
p^{6m+5}	$k<p^{4m+4}/2$, $2\leq t<p^{3m/2+5/4}/4$ for $m>0$; $2\leq t\leq(p-3)/4$ for $m=0$	$\geq\max(tp^{4m+3}-4t^2p^{2m+1},$ $p^{4m+3}\sqrt{p}-p^{4m+3}-p^{2m+2}/2)$	$p\geq 5$

q	$t,\ k=\lvert B\rvert-t(q+1)$, other conditions	B
p^{6m}	$2\leq t<p^{3m/2}/4,\ k<\min(p^{4m}\sqrt{p}/2,$ $2p^{4m}+(t-2)p^{3m}-16p^{2m})$	$t-1$ disjoint Baer subplanes union a tth minimal blocking set
p^{6m+2}	$m\geq 1,\ 2\leq t<p^{3m/2+1/2}/4,\ k<\min(p^{4m+2}/2,$ $2p^{4m+1}+(t-2)p^{3m+1}-16p^{2m})$	union of t disjoint Baer subplanes
p^{6m+4}	$2\leq t<p^{(3m+2)/2}/4,\ k<\min(p^{4m+3}-2p^{2m+2},(t-2)p^{3m+2}$ $+\max(2p^{4m+2}-16p^{2m},p^{4m+3}-p^{4m+2}-p^{2m+2}/2))$	union of t disjoint Baer subplanes

2.144 Theorem (Bose and Burton) Let B be a set of points in $\mathrm{PG}(d,q)$. If any subspace of dimension $d-t$ has at least one point in common with B, then $\lvert B\rvert\geq q^t+\cdots+q+1$ with equality if and only if B is a t-dimensional subspace.

2.145 A *t-blocking set* B in $\mathrm{PG}(d,q)$ is a set of points such that any $(d-t)$-dimensional subspace contains a point of B and no t-dimensional subspace is contained in B. A t-blocking set B in $\mathrm{PG}(d,q)$ is *minimal* when every point Q of B belongs to at least one $(d-t)$-dimensional space only intersecting B in Q.

2.146 Theorem (Szőnyi and Weiner) Let B be a minimal t-blocking set B of $\mathrm{PG}(d,q)$, $q=p^h$, $p>2$ prime, and assume that $|B|<3(q^t+1)/2$. Then any subspace that intersects B intersects it in 1 (mod p) points.

2.147 Theorem (Beutelspacher, Heim) Let B be a t-blocking set in $\mathrm{PG}(d,q)$. Then $|B|\geq q^t+\cdots+1+q^{t-1}\epsilon$, with $q+\epsilon+1$ the size of the smallest blocking set in $\mathrm{PG}(2,q)$, and with equality if and only if B is the point set of a cone over a minimal blocking set of size $q+\epsilon+1$ in $\mathrm{PG}(2,q)$.

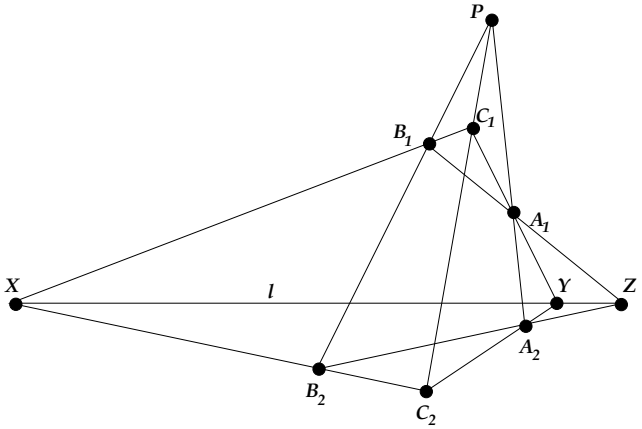
2.148 Theorem (Bokler) The minimal t-blocking sets of cardinality at most $q^t+\cdots+q+1+\sqrt{q}(q^{t-1}+\cdots+q+1)$ in $\mathrm{PG}(d,q)$, q square, $q\geq 16$, are cones with an m-dimensional vertex $\mathrm{PG}(m,q)$ and base a Baer subgeometry $\mathrm{PG}(2(t-m-1),\sqrt{q})$, for some m with $\max\{-1,2t-d-1\}\leq m\leq t-1$.

2.14 Nondesarguesian Planes

2.149 Remark The projective planes $\mathrm{PG}(2,q)$ are the classical examples of finite projective planes. Many other examples of finite projective planes exist. The projective planes $\mathrm{PG}(2,q)$ are also known as the *desarguesian* planes since they are the only finite projective planes in which the theorem of Desargues is valid (Theorem 2.152).

2.150 The *Desargues configuration* is a symmetric (10_3) configuration consisting of two triangles with vertices A_i,B_i,C_i and opposite sides a_i,b_i,c_i, $i=1,2$, such that the lines A_1A_2,B_1B_2,C_1C_2 are concurrent at a point P (the triangles are *in perspective* from P) and the points a_1a_2,b_1b_2,c_1c_2 are collinear on a line ℓ (the triangles are *in perspective* from ℓ). (If P is on ℓ, then the configuration is the *little Desargues configuration* and is not a (10_3).) (See §VI.7 for more on configurations.)

2.151 Example The Desargues configuration.



2.152 Theorem (Theorem of Desargues) In $\mathrm{PG}(2,q)$, if two triangles with vertices A_i,B_i,C_i and opposite sides a_i,b_i,c_i, $i=1,2$, are in perspective from a point P, then the corresponding intersection points a_1a_2,b_1b_2,c_1c_2 are collinear on a line ℓ.

2.153 Theorem If in a finite projective plane of order q, for every two triangles with vertices A_i,B_i,C_i and opposite sides a_i,b_i,c_i, $i=1,2$, which are in perspective from a point

P, the corresponding intersection points a_1a_2, b_1b_2, c_1c_2 are collinear on a line ℓ, then this projective plane is equal to $\mathrm{PG}(2,q)$.

2.154 Remark The preceding theorem explains why the finite projective planes, different from $\mathrm{PG}(2,q)$, are known as *nondesarguesian* planes.

2.155 Theorem (Ostrom) Any finite projective plane of order $n \geq 5$ contains a pair of triangles that are in perspective from a point and a line.

2.156 A projective plane is *pappian* if the Pappus configuration occurs for any pair of distinct lines ℓ, ℓ'. That is, given any distinct A, B, C on ℓ and any distinct A', B', C' on ℓ', the points $AB' \cap A'B$, $AC' \cap A'C$, $BC' \cap B'C$ are collinear. See Example VI.7.6.

2.157 Theorem Every pappian plane (finite or infinite) is desarguesian. Conversely, in the finite case (from Wedderburn's theorem that every finite skew field is a field), every desarguesian plane is pappian.

2.158 For any projective plane π, its *dual plane* π^* is defined as the plane whose points are the lines of π and whose lines are the points of π.

2.159 Remark Some projective planes are isomorphic to their dual plane. For instance, the dual plane of $\mathrm{PG}(2,q)$ is again isomorphic to $\mathrm{PG}(2,q)$. However, not all projective planes are isomorphic to their dual plane.

2.160 Remark If $\alpha \neq 1$ is a collineation of a projective plane π, and α fixes all lines through a point P and all points on a line ℓ, then α is a (P,ℓ)-*perspectivity*. In particular, a (P,ℓ)-*homology* if $P \notin \ell$ and a (P,ℓ)-*elation* if P is on ℓ. The point P is the *center* and ℓ is the *axis* of the perspectivity. For a given pair (P,ℓ), the (P,ℓ)-perspectivities of π form a subgroup, denoted by $\Sigma_{(P,\ell)}$, of Aut π.

2.161 π is (P,ℓ)-*transitive* if for any distinct points A, B not on ℓ and collinear with P ($A \neq P \neq B$), there is a (P,ℓ)-perspectivity α in Aut π such that $A^\alpha = B$.

2.162 Proposition If π has order n, then

1. π is (P,ℓ)-transitive for P on ℓ if and only if $|\Sigma_{(P,\ell)}| = n$.
2. π is (P,ℓ)-transitive for P not on ℓ if and only if $|\Sigma_{(P,\ell)}| = n-1$.

2.163 Proposition Let α be a (P,ℓ)-perspectivity of π. If Δ is a triangle having no vertex or side fixed by α, then Δ and Δ^α are in perspective from both P and ℓ.

2.164 A projective plane π is (P,ℓ)-*desarguesian* if for each pair of nondegenerate triangles Δ_i $(i = 1,2)$ with vertices A_i, B_i, C_i and opposite sides a_i, b_i, c_i, such that (1) Δ_1 and Δ_2 are in perspective from P, and (2) $X = a_1a_2$ and $Y = b_1b_2$ are on the line ℓ, then the point $Z = c_1c_2$ is on ℓ.

2.165 Theorem (Baer) A projective plane π is (P,ℓ)-transitive if and only if it is (P,ℓ)-desarguesian.

2.166 Remark The preceding theorem is a particular example of where properties of the automorphism group of a projective plane are sometimes equivalent to geometric properties of this plane.

Let π be a projective plane of order $n \geq 5$ and G the collineation group of π. Define $T(G) = \{(P,\ell) | G \text{ is } (P,\ell)\text{-transitive}\}$. The projective planes can be classified by looking at all possibilities for $T(G)$. This provides the *Lenz–Barlotti classification* of projective planes [679]. However, projective planes can also be classified according to the coordinatizing algebra as the properties of such an algebra translate the geometric

properties of the plane as well as those of its collineation group. This is presented in the next section.

2.167 π is (m,ℓ)-*transitive* if it is (P,ℓ)-transitive for all points P on m; dually, π is (P,Q)-*transitive* if it is (P,ℓ)-transitive for all lines ℓ on Q. If π is (ℓ,ℓ)-transitive for some line ℓ, then ℓ is a *translation line* of π and π is a *translation plane* with respect to ℓ. A *translation point* for π is a point P such that π is (P,P)-transitive; then π is a *dual translation plane* with respect to P.

2.168 Remark If π is a translation plane with respect to a line ℓ, then usually $\pi^\ell = \pi \setminus \ell$ is also known as a *translation plane*. The translation plane is considered as an affine plane, its line at infinity being the translation line. Also, the translation group of such an affine plane is the group of all (ℓ,ℓ)-elations, and acts transitively on the points of the affine plane.

2.169 Remark t-Spreads in $\mathrm{PG}(2t+1,q)$ (see §2.8) are equivalent to translation planes. Let $P = \mathrm{PG}(2t+2,q)$ and let H be a hyperplane of P. Let S be a t-spread of H. Then define the geometry $A(S)$ with points those of $P\setminus H$, and lines the $(t+1)$-dimensional subspaces of P that intersect H precisely in an element of S.

2.170 Theorem (André) $A(S)$ is a translation plane of order q^{t+1}. Conversely, for any translation plane A, there is an integer t so that a t-spread S in $H = \mathrm{PG}(2t+1,q)$ exists for which $A = A(S)$. In addition, $A(S)$ is desarguesian if and only if S is regular.

2.171 A projective plane in which every line is a translation line is a *Moufang plane*.

2.172 Proposition Finite Moufang planes are desarguesian.

2.15 Coordinatization of Arbitrary Projective Planes

2.173 Construction Let π be a projective plane of order n and R a set of n symbols with two distinguished symbols 0 and 1, $0 \neq 1$. One can coordinatize π by the set $R \cup \{\infty\}$ where ∞ is a symbol not in R, with respect to a given quadrangle.

Let P, X, Y, I be a quadrangle in π, and consider the lines $\ell_\infty = XY$, $\ell_1 = PY$, $\ell_2 = PX$ and the points $A = XI \cap \ell_1$, $B = YI \cap \ell_2$, $J = AB \cap \ell_\infty$. Assign the elements of R to the points on $\ell_1 \setminus \{Y\}$ in an arbitrary bijective manner except that 0 is assigned to P and 1 to A. If $c \in R$ is assigned to the point $C \in \ell_1$, write $(0,c)$ for C. Next, if $D \in \ell_2 \setminus \{X\}$, consider $D' = JD \cap \ell_1$; if D' is $(0,d)$, then D is $(d,0)$. For any point H not on ℓ_∞, if $XH \cap \ell_1$ is $(0,g)$ and $YH \cap \ell_2$ is $(h,0)$, then H has the coordinates (h,g). For a point $M \in \ell_\infty \setminus \{Y\}$, take the line joining M to $(1,0) = B$, and let $(0,m)$ be the point in which it meets ℓ_1; then M is given the coordinate (m). Finally, Y has coordinate (∞).

Next, coordinatize the lines. Let ℓ be a line not on Y with (m) and $(0,k)$ the points at which it meets ℓ_∞ and ℓ_1, respectively. Then ℓ has coordinates $[m,k]$. If $\ell \neq \ell_\infty$ contains Y, then ℓ is the line $[k]$ if $\ell \cap \ell_2 = (k,0)$. Finally, ℓ_∞ is the line $[\infty]$.

To determine via the coordinates when two elements are incident, one uses the incidences of π to define a ternary operation T on R. Namely, if $a,b,c \in R$, then $T(a,b,c) = k$ if and only if (b,c) is on $[a,k]$. Thus $(0,k)$ is the intersection of ℓ_1 with the line joining (a) to (b,c) so that, given a,b,c, the value of k is uniquely determined.

2.174 Proposition Let π be a projective plane coordinatized by a set R. If T is defined by $T(a,b,c) = k$ if and only if (b,c) is on $[a,k]$, then:

1. $T(a,0,c) = T(0,b,c) = c$ for all $a,b,c \in R$.
2. $T(a,1,0) = T(1,a,0) = a$ for all $a \in R$.

3. If $a, b, c, d \in R$, $a \neq c$, then there is a unique $x \in R$ such that $T(a, b, c) = T(x, c, d)$.
4. If $a, b, c \in R$, then there is a unique $x \in R$ such that $T(a, b, x) = c$.
5. If $a, b, c \in R$, $a \neq c$, then there is a unique ordered pair $x, y \in R$ such that $T(a, x, y) = b$ and $T(c, x, y) = d$.

2.175 Any ternary ring (set with a ternary operation) with two distinguished elements $0, 1$ satisfying properties (1)–(5) of Proposition 2.174 is a *planar ternary ring* (PTR).

2.176 Proposition If (R, T) is a PTR, then the structure π defined as follows is a projective plane. The points of π are ordered pairs (x, y), where $x, y \in R$, together with elements of the form (x), $x \in R$, and (∞) where ∞ is a symbol not in R. Lines are given by ordered pairs $[m, k]$, $m, k \in R$, together with elements of the form $[m]$, $m \in R$, and $[\infty]$. Incidence is

(x, y) is on $[m, k] \iff T(m, x, y) = k$,
(x, y) is on $[k] \iff x = k$,
(x) is on $[m, k] \iff x = m$, and
(x) is on $[\infty]$ for all $x \in R$ and (∞) is on $[k]$ for all $k \in R$.

Finally, (∞) is on $[\infty]$.

2.177 Remark On a PTR (R, T), for any $a, b \in R$, define $a + b = T(1, a, b)$ and for all $a, b \in R^*$, define $a \cdot b = ab = T(a, b, 0)$. Then $\langle R; + \rangle$ and $\langle R^*; \cdot \rangle$ are loops with 0 and 1 the respective identities. If (R, T) is any PTR with $T(a, b, c) = ab + c$ for all $a, b, c \in R$, then (R, T) is *linear*, and the PTR is linear. A plane coordinatized by a skewfield may be coordinatized by a linear PTR.

The algebraic properties of PTRs and/or of the associated loops are linked to the groups of perspectivities admitted by the corresponding planes; in turn, these groups reflect the geometric structure of the planes. Linearity can be characterized by the validity of a suitable little Desargues configuration.

2.178 Proposition (R, T) is linear with associative addition if and only if π is $((\infty), [\infty])$-transitive.

2.179 A *cartesian group* is a linear PTR(R, T) with associative addition.

2.180 Proposition A cartesian group (R, T) satisfies the left distributive law $a(b+c) = ab+ac$ for all a, b, c in R if and only if π is $((0), [\infty])$-transitive.

2.181 A *(left) quasifield* (R, T) is a cartesian group satisfying the left distributive law.

2.182 Corollary π is coordinatized by a quasifield with the line ℓ as $[\infty]$ if and only if ℓ is a translation line.

2.183 Proposition If (R, T) is a quasifield, then $\langle R; + \rangle$ is an abelian group.

2.184 Proposition (R, T) is linear with associative multiplication if and only if π is $((0), [0])$-transitive.

2.185 Proposition If (R, T) is linear, then (R, T) has associative multiplication and satisfies the left distributive law if and only if π is $((\infty), [0, 0])$-transitive.

2.186 A *nearfield* is a quasifield with associative multiplication.

2.187 Proposition The dual plane π^* of π can be coordinatized by dualizing the quadrangle in a natural way. Associativity of addition is preserved but the left distributive law becomes the right distributive law and yields a right quasifield.

2.188 Proposition If (R, T) is linear with associative addition then (R, T) satisfies the right distributive law if and only if π is $((\infty), [0])$-transitive.

2.189 Corollary (R, T) is a right quasifield if and only if (∞) is a translation point.

2.190 A *semifield* (or *division ring*) is a (left) quasifield satisfying the right distributive law. (So, in a semifield both distributive laws hold.)

2.191 Proposition (R, T) is a semifield if and only if π is $((\infty), [\infty])$-, $((0), [\infty])$-, and $((\infty), [0])$-transitive. Also, (R, T) is a semifield if and only if π is a translation plane with respect to $[\infty]$ and the dual of a translation plane with respect to (∞).

2.192 Table Classification of projective planes by PTR.

PTR	Geometric Properties of π	Name
Field	(P, ℓ)-transitivity, all P and ℓ, plus configuration of Pappus	Pappian plane
Skewfield	(P, ℓ)-transitivity for all P, ℓ	Desarguesian plane
Alternative division ring	(P, ℓ)-transitivity for all incident pairs P, ℓ	Moufang plane
Semifield	(ℓ, ℓ)-transitivity and (P, P)-transitivity for one incident pair P, ℓ	Semifield plane
Nearfield	(ℓ, ℓ)-transitivity and (P, m)-transitivity $P \in \ell$, $P \notin m$	Nearfield plane
Right nearfield	(P, P)-transitivity and (Q, ℓ)-transitivity, P on ℓ, Q not on ℓ	Dual nearfield plane
Quasifield	(ℓ, ℓ)-transitivity for one ℓ	Translation plane
Right quasifield	(P, P)-transitivity for one P	Dual translation plane

2.193 Construction Given a PTR (R, T) of order n with $R = \{0, 1, \ldots, n-1\}$, for any $x \in R^*$ construct an $n \times n$ matrix $\{x\}$: The entry of $\{x\}$ in position (i, j) is $T(x, i, j)$. Then $\{x\}$ is a latin square and $\{x\}$ is orthogonal to $\{y\}$ if $x \neq y$. This yields a complete set of $n-1$ MOLS. Conversely, given such a set of MOLS in normal form, $A_1, A_2, \ldots, A_{n-1}$, where A_1 has $(0, 1, \ldots, n-1)^t$ as its first column, label the squares $\{x\}$ so that $\{x\}$ is the square with x in the $(1, 0)$-position, $x = 1, 2, \ldots, n-1$. Defining $T(x, i, j) = (i, j)$th entry in $\{x\}$, and $T(0, i, j) = j$, for all i, j, yields a PTR (R, T).

2.194 Proposition There exists a finite projective plane of order n if and only if there exists a complete set of $n-1$ MOLS of order n (see §III.1 and §III.3).

2.16 Hall and André Planes

2.195 A *quasifield* Q is an algebra with two binary operations $+$ and $\cdot$ such that

1. $\langle Q; + \rangle$ is an abelian group;
2. $\langle Q^*; \cdot \rangle$ is a loop;
3. $x(y + z) = xy + xz$ for all x, y, z in Q;
4. $0x = 0$ for all $x \in Q$; and
5. $ax = bx + c$ has a unique solution for x, given $a, b, c \in Q$, $a \neq b$.

2.196 The *Hall quasifields*, which coordinatize the Hall planes, are defined as follows. Let F be a field and $f(s) = s^2 - as - b$ an irreducible quadratic polynomial over F. Let H be a two dimensional right vector space over F with basis elements 1 and λ so that $H = \{x + \lambda y | x, y \in F\}$. Take as addition in H the addition of the vector space and define a multiplication as follows: if $y = 0$, $x(z + \lambda t) = xz + \lambda(xt)$; if $y \neq 0$, $(x + \lambda y)(z + \lambda t) = xz - y^{-1}tf(x) + \lambda(yz - xt + at)$. Then $\langle H; +, \cdot \rangle$ is a Hall quasifield.

2.197 Proposition A Hall quasifield H is associative (is a nearfield) if and only if $F = \mathbb{F}_2$ (in which case $H = \mathbb{F}_4$) or $F = \mathbb{F}_3$ and $f(s) = s^2 + 1$.

2.198 Remark The Hall quasifield of order 9 (in fact, a nearfield) can also be defined as follows. Let F be $\mathbb{F}_9$ and define a new multiplication $\circ$ on F by $x \circ y = xy$ if x is a square and $x \circ y = xy^3$ if x is not a square. Then $\langle F; +, \circ\rangle$ is a quasifield; moreover, multiplication is associative. If $F = \mathbb{F}_{q^2}$, q an odd prime power, and a multiplication $\circ$ is defined by $x \circ y = xy$ if x is a square, and $x \circ y = xy^q$ if x is not a square, then $\langle F; +, \circ\rangle$ is a quasifield, actually a nearfield.

2.199 Remark The Hall planes are translation planes, so can be defined by a t-spread in $\mathrm{PG}(2t+1, q)$ (Theorem 2.170). If one replaces one 1-regulus of a regular 1-spread in $\mathrm{PG}(3, q)$, one obtains a 1-spread that is not regular. It is precisely these 1-spreads in $\mathrm{PG}(3, q)$ that define the Hall planes.

2.200 Construction Assume $F = \mathbb{F}_{q^m}$, $K = \mathbb{F}_q$ and $\mathcal{G} = \mathrm{Aut}_K(F)$ so that $\mathcal{G}$ is the cyclic group of order m and K is the subfield of F fixed by $\mathcal{G}$. The *norm function* over K of F is

$$N_{F/K} : F \to K : \alpha \mapsto N_{F/K}(\alpha) = \alpha^{(q^m-1)/(q-1)},$$

and maps F onto K. Let φ be any mapping from K into $\mathcal{G}$ that maps the identity 1 of K^* onto the identity of $\mathcal{G}$. A quasifield F_φ can then be defined. The elements of F_φ are the elements of F, addition is the same and multiplication $\circ$ is defined by

$$0 \circ y = 0 \text{ for all } y \in F, \quad x \circ y = xy^{\alpha_x} \text{ for all } x, y \in F,\ x \neq 0,$$

where $\alpha_x \in \mathcal{G}$ is the automorphism of F given by $N_{F/K}(x)^\varphi$. Then $\langle F_\varphi; +, \circ\rangle$ is an *André quasifield*. If φ is a homomorphism from K^* into $\mathcal{G}$, then the André quasifield is associative. It is an *André nearfield*.

2.201 A plane coordinatized by an André quasifield is an *André plane*.

2.17 Semifields

2.202 A *(finite) semifield* $\mathcal{S}$ is an algebra $\langle S; +, \cdot\rangle$ such that

1. $\langle S; +\rangle$ is an abelian group with identity 0;
2. $\langle S^*; \cdot\rangle$ is a loop with identity 1;
3. both left and right distributive laws hold: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ for all $a, b, c \in S$.

2.203 Proposition A proper semifield (one that is not a (skew)-field) contains three elements a, b, c such that $(ab)c \neq a(bc)$.

2.204 Theorem A finite proper semifield has order p^n, p a prime, $n \geq 3$ an integer, and $p^n \geq 16$.

2.205 For a semifield $\mathcal{S}$, define the

left nucleus of $\mathcal{S}$: $N_l = \{x \in S | x(ab) = (xa)b \text{ for all } a, b \in S\}$;
right nucleus of $\mathcal{S}$: $N_r = \{x \in S | (ab)x = a(bx) \text{ for all } a, b \in S\}$;
middle nucleus of $\mathcal{S}$: $N_m = \{x \in S | (ax)b = a(xb) \text{ for all } a, b \in S\}$.

The intersection of these three nuclei (the *semi-nuclei*) is the *nucleus* N of S.

2.206 Remarks When S is finite of characteristic p, N contains $\mathbb{F}_p$. All nuclei are (skew)-fields and S is a left (right) vector space over N_l, (N_r), N_m, and N.

2.207 Example Let $F = \mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$ be the field of four elements. The elements of the semifield V have the form $u + \lambda v$, $u, v \in F$, λ a symbol not in F.

Addition is defined componentwise, whereas multiplication is defined as follows:

$$(u+\lambda v)(x+\lambda y) = (ux+v^2y)+\lambda(vx+u^2y+v^2y^2).$$

The nucleus of V is $\mathbb{F}_2$. (In V, $(ab)c = a(bc)$ if any two of a, b, c are in $\mathbb{F}_4$.) V has six automorphisms σ_{ij}, $i = 0, 1, 2$, $j = 1, 2$, such that $(u+\lambda v)^{\sigma_{ij}} = u^j + \lambda\omega^i v^j$ and an anti-automorphism $\tau : (u+\lambda v)^\tau = u+\lambda v^2$. The plane coordinatized by V is a translation plane and a dual translation plane of order 16, namely, the so-called semifield plane with kern $\mathbb{F}_2$, or *Semi2*.

2.208 Example A semifield W has the same elements and the same addition as V in Example 2.207, but multiplication is defined as follows:

$$(u+\lambda v)(x+\lambda y) = (ux+\omega v^2y)+\lambda(vx+u^2y).$$

In W the associative law holds whenever one of a, b, c is in F. The nucleus of W is $\mathbb{F}_4$. The plane coordinatized by W is a translation plane and a dual translation plane and is the so-called semifield plane of order 16 with kern $\mathbb{F}_4$, *Semi4*. The semifields in this and Example 2.207 are essentially the only semifields of order 16.

2.209 Example *Dickson commutative semifields.* Assume $F = \mathbb{F}_{p^m}$, p odd, $m > 1$, σ a nontrivial automorphism of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and f a nonsquare in F. Then the Dickson semifield has elements $a+\lambda b$, $a, b \in F$, λ a symbol not in F, addition is componentwise and multiplication is defined as follows:

$$(a+\lambda b)(c+\lambda d) = (ac+b^\sigma d^\sigma f)+\lambda(ad+bc).$$

The planes coordinatized by the Dickson semifields have many interesting properties: They admit polarities and their full collineation groups are solvable.

2.210 Example *Albert's twisted fields.* Define a new multiplication on $F = \mathbb{F}_{p^n}$ by

$$x \circ y = xy^q - cx^q y,$$

where $q = p^m$, $1 \le m < n$, and $c \ne a^{q-1}$ for any $a \in \mathbb{F}_{p^n}$. Then $\langle F; +, \circ\rangle$ is a presemifield; that is, $\langle F^*; \circ\rangle$ is a quasigroup but not a loop. Take any $b \in F^*$ and define a new multiplication $*$ by

$$(x \circ b) * (b \circ y) = x \circ y;$$

then $\langle F; +, *\rangle$ is a semifield with multiplicative identity $b \circ b$.

2.18 The Hughes Planes

2.211 Remark Hughes planes are nondesarguesian planes of order q^2, q an odd prime power, which cannot be coordinatized by any linear PTR. They can be constructed by the nearfield $\langle N; +, \circ\rangle$, where $N = \mathbb{F}_{q^2}$, $+$ is addition in the field and the multiplication $\circ$ is defined by

$$x \circ y = \begin{cases} xy & \text{if } x \text{ is a square in } \mathbb{F}_{q^2}, \\ xy^q & \text{if } x \text{ is not a square in } \mathbb{F}_{q^2}. \end{cases}$$

The kernel of this nearfield N is the field $F = \mathbb{F}_q$ and every element of F commutes with each element of N.

2.212 Construction To construct the Hughes plane $Hu(q^2)$ of order q^2, consider the set $V = \{(x, y, z) | x, y, z \in N\}$. Define addition $+$ on V componentwise and define a left scalar multiplication by the elements of N by $k \circ (x, y, z) = (k \circ x, k \circ y, k \circ z)$. Both the points and the lines of $Hu(q^2)$ are the elements of $N^3 \setminus \{(0, 0, 0)\}$, and (x, y, z) represents $\{(k \circ x, k \circ y, k \circ z) | k \in N^*\}$. The points of $Hu(q^2)$ can be identified with the points of $\mathrm{PG}(2, q^2)$. To define the incidence, fix a basis $\{1, t\}$ for N as a vector space over F. To determine whether (x, y, z) is incident with (u, v, w), express $u = a + ta_1$, $v = b + tb_1$, $w = c + tc_1$. Then (u, v, w) and (x, y, z) are incident if

$xa + yb + zc + (xa_1 + yb_1 + zc_1) \circ t = 0$. The set π_0 of all points (x, y, z) such that $x, y, z \in F$, together with the lines joining them, forms a desarguesian Baer subplane of $Hu(q^2)$ that is left invariant by the full collineation group of $Hu(q^2)$ and is also known as the *real Baer subplane*. This full collineation group depends on q^2; namely,

If $q^2 = 3^2$, then Aut $Hu(9) = PGL(3,3) \times Sym_3$.
If $q^2 = p^2, p > 3$, then Aut $Hu(p^2) = PGL(3,p) \times C_2$.
If $q^2 = p^{2m}$, then Aut $Hu(q^2) = PGL(3,p^m) \rtimes C_{2m}$.

2.213 Proposition $Hu(q^2)$ is not (P,ℓ)-transitive for any choice of P and ℓ and, hence, is neither a translation plane nor a dual translation plane.

2.214 Remarks $Hu(q^2)$ is a *semitranslation plane*, which means the following. Let ℓ_0 be any line of π_0 (that is, ℓ_0 is a line of $Hu(q^2)$ such that $\pi_0 \cap \ell_0$ is a line of π_0), then $Hu(q^2)$ admits all elations with axis ℓ_0 and center a point on $\pi_0 \cap \ell_0$ that fix π_0.

2.19 The Figueroa Planes

2.215 Remark The *Figueroa* planes form an infinite class of nondesarguesian planes of order q^3, q a prime power, which are neither translation nor semitranslation planes.

2.216 Construction The desarguesian plane $\mathrm{PG}(2, q^3)$ over $\mathbb{F}_{q^3}$ admits a planar collineation α of order 3 ($\langle\alpha\rangle = \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^3})$). Then the points and lines of $\mathrm{PG}(2, q^3)$ fall into three disjoint classes. For a point P,

$$P \text{ is of } \begin{cases} \text{type I} & \text{if } P^\alpha = P, \\ \text{type II} & \text{if } P, P^\alpha, P^{\alpha^2} \text{ are collinear and distinct,} \\ \text{type III} & \text{if } P, P^\alpha, P^{\alpha^2} \text{ are not collinear.} \end{cases}$$

Line types are defined dually. Define as follows an involutory bijection μ between the points of type III and the lines of type III. For a point P and a line ℓ both of type III, $P^\mu = P^\alpha P^{\alpha^2}$ and $\ell^\mu = \ell^\alpha \cap \ell^{\alpha^2}$. Let $\mathcal{P}$ be the set of points and $\mathcal{L}$ the set of lines of $\mathrm{PG}(2, q^3)$. Define a new incidence structure $Fig(q^3) = (\mathcal{P}, \mathcal{L}, \mathrm{I}_F)$ in terms of the incidence I of $\mathrm{PG}(2, q^3)$:

$$P \,\mathrm{I}_F\, \ell \iff \begin{cases} P^\mu \,\mathrm{I}\, \ell^\mu & \text{if } P \text{ and } \ell \text{ are both of type III,} \\ P \,\mathrm{I}\, \ell & \text{otherwise;} \end{cases}$$

then $Fig(q^3)$ is the *Figueroa plane* of order q^3 [990].

2.217 Proposition For $q > 2$, the Figueroa plane is not desarguesian. The points and lines of type I form a desarguesian subplane of order q of both $\mathrm{PG}(2, q^3)$ and $Fig(q^3)$, and if $\mathcal{A}$ denotes its collineation group, then the collineation group of $Fig(q^3)$ is $\langle\alpha\rangle \rtimes \mathcal{A}$.

2.20 Derivation

2.218 Remark *Derivation* is a construction due to Ostrom that for $q > 2$ produces a new (nonisomorphic) plane of order q^2 from a given one of the same order.

2.219 Construction Assume π is a plane of square order q^2, and ℓ_∞ is a line of π containing a set Δ of $q+1$ points with the following property: *there exist* $q^2(q+1)$ *Baer subplanes of* π *all of which contain* Δ *such that any two of them either share the points in* Δ *only or share also one point in* π^{ℓ_∞}. Then a new affine plane $\pi^{\mathcal{D}} \setminus \ell_\infty$, the *derived* plane of π^{ℓ_∞} with respect to Δ, can be constructed:

1. the points of $\pi^{\mathcal{D}} \setminus \ell_\infty$ are the points of π^{ℓ_∞};
2. all lines of π^{ℓ_∞} that, in π, meet $\ell_\infty \setminus \Delta$ are lines of $\pi^{\mathcal{D}} \setminus \ell_\infty$;

3. each line of π^{ℓ_∞} that, in π, meets ℓ_∞ at a point of Δ is substituted by one of the Baer subplanes described above; and
4. incidence is set theoretic inclusion.

This new affine plane uniquely completes to a projective plane, the *derived plane* of π with respect to Δ.

2.220 Remarks Derivation can also be discussed from an algebraic point of view (see [1153]). By deriving the derived plane of π with respect to the same Δ, π is recovered. Not all planes are derivable. The desarguesian planes are derivable with respect to any line and any Δ. By deriving $\mathrm{PG}(2, q^2)$, one obtains the Hall plane of order q^2. Both the semifield planes of order 16 are derivable. All Hughes planes are derivable when ℓ_∞ is a line of the real Baer subplane π_0 and $\Delta = \pi_0 \cap \ell_\infty$.

The four planes of order 9 form a chain in the following sense:

$$\mathrm{PG}(2,9) \overset{\text{derive}}{\rightsquigarrow} \mathrm{Hall}(9) \overset{\text{dualize}}{\rightsquigarrow} \mathrm{Hall}(9)^* \overset{\text{derive}}{\rightsquigarrow} Hu(9),$$

and the arrows can be reversed.

2.21 Projective Planes of Small Order

2.221 Table [689, 1728] The number of distinct examples of particular substructures in the four planes of order nine.

	PG(2, 9)	Hall(9)	Hall(9)*	$Hu(9)$
Ovals	1	1	1	2
Maximal {21;3}-arcs	0	0	0	0
Unitals	2	4	4	8

2.222 Table [626, 680, 683, 1550] The number N of distinct translation planes of order q.

q	2	3	4	5	7	8	9	16	25	27	32	49
N	1	1	1	1	1	1	2	8	21	7	≥ 9	1347

2.223 Remarks The two translation planes of order nine are PG(2, 9) and Hall(9).

The eight translation planes of order sixteen are (1) PG(2, 16), (2) the semifield plane *SEMI2* with kernel $\mathbb{F}_2$, (3) the semifield plane *SEMI4* with kernel $\mathbb{F}_4$, (4) the Hall plane Hall(16), (5) the Lorimer–Rahilly plane LMRH, (6) the Johnson–Walker plane JOWK, (7) the derived semifield plane DSFP, and (8) the Dempwolff plane DEMP [683].

The seven translation planes of order 27 are (1) PG(2, 27), (2) a generalized twisted field plane, (3) a Hering plane, (4) a flag transitive plane, (5) a Sherk plane, (6) a second flag transitive plane, and (7) an André plane [680].

Mathon found by an exhaustive computer search that there are exactly nine translation planes of order 32 defined by a 4-spread in PG(9, 2) having a nontrivial stabilizer group.

2.224 Remark Twenty-two planes of order 16 are known. There are the eight translation planes, mentioned in Remark 2.223. The first three of the planes from Remark 2.223 are self-dual; the remaining five planes have duals HALL(16)*, LMRH*, JOWK*, DSFP*, and DEMP*, which are not translation planes. There are four known semitranslation planes of order 16: BBH1, BBH2, JOHN, and BBS4. The plane BBH1 is self-dual; the other three semitranslation planes have dual planes BBH2*, JOHN*, and BBS4*, which have not yet arisen. The two remaining planes MATH and MATH* are the other two known planes of order 16 [1729].

2.225 Table [1729] The number of distinct hyperovals in the known planes of order 16. The name of every plane is followed by the number of distinct hyperovals.

PG(2, 16)	2	SEMI2	17	SEMI4	3	HALL	4	HALL*	3	LMRH	6
LMRH*	1	JOWK	6	JOWK*	1	DSFP	22	DSFP*	0	DEMP	15
DEMP*	2	BBH1	3	BBH2	2	BBH2*	0	JOHN	1	JOHN*	0
BBS4	1	BBS4*	0	MATH	1	MATH*	3				

2.226 Remarks It is particularly interesting that the planes DSFP*, BBH2*, JOHN*, and BBS4* do not contain any hyperovals. Also, since the external lines to a hyperoval in a plane of order 16 define a maximal $\{120; 8\}$-arc in the dual plane, using Remark 2.224 where the relation between the planes and their dual planes is described, from Table 2.225 the number of distinct maximal $\{120; 8\}$-arcs in the planes of order 16 can also be deduced.

2.22 Substructures in Nondesarguesian Planes

2.227 Remarks A great deal of research has been done on substructures in nondesarguesian projective planes. The following list gives examples of such substructures.

1. Translation planes of order q^2 with kernel of order q have unitals [370].
2. Translation planes of order q^t, $t \geq 2$, with kernel of order q have blocking sets of size in the interval $[q^t + q^{t-1} + 1, q^t + q^{t-1} + \cdots + q + 1]$ [351].
3. Hall(q^2) has unitals [370], blocking sets [351], hyperovals if $q \geq 4$, q even [1694], and ovals if q is odd [1324].
4. *Hu*(q^2) has unitals [1826] and ovals [1818].
5. *Fig*(q^3) has unitals if q is a square, hyperovals if $q > 2$ even [661], and ovals if q is odd [492].
6. Thas proved that certain translation planes of order 2^{2m} contain maximal $\{2^{3m} - 2^{2m} + 2^m; 2^m\}$-arcs [2020]. Hamilton and Quinn constructed maximal arcs in symplectic translation planes [1029].

Some of these are *inherited substructures* from PG(2, q). Let π be an arbitrary projective plane of order q. Then π can sometimes be looked at as a modification of PG(2, q). The points of π can be identified with those of PG(2, q) and the lines of π can be regarded as point sets of PG(2, q). An oval in PG(2, q) can sometimes remain to be an oval in π. In this case this oval in π is an *inherited* oval of PG(2, q).

2.228 Remarks Of course, differences between the results on substructures in desarguesian planes and on substructures in nondesarguesian planes appear, some of which are very surprising. In particular, observe the nonexistence of hyperovals in four of the known planes of order 16 (Table 2.225). Other examples include

1. Menichetti proved that in Hall(q^2), q even, there exist complete q^2-arcs [1590]. Segre, for q odd, and Tallini, for q even, proved that complete q-arcs do not exist in PG(2, q).
2. In PG(2, q), q odd, there exist (complete) $(q+1)$-arcs and in PG(2, q), q even, there exist (complete) $(q+2)$-arcs. The existence is known of complete $(q - \sqrt{q} + 1)$-arcs in PG(2, q), $q > 4$ square (Theorem 2.88). But all the other known infinite classes of complete k-arcs in PG(2, q) have size at most $(q+1)/2 + \sqrt{q}$. In particular, there exist complete k-arcs, with $(q+1)/2 - \sqrt{q} \leq k \leq (q+1)/2 + \sqrt{q}$, consisting of half of the points of elliptic cubic curves in PG(2, q). So, an important problem in PG(2, q) is that of the existence of complete k-arcs, with $(q+1)/2 + \sqrt{q} < k < q - \sqrt{q} + 1$.

By contrast, in certain André planes of order $q = s^2$, complete k-arcs having size in this interval have been constructed by Szőnyi [1998]. Let $k|(s-1)$, then there exist in certain of these André planes complete k-arcs of size $((m-1)(q-1)/m + O(q^{1/2}))$-arcs, where $m = k$ if k is odd, and where $m = k/2$ if k is even.

3. It is known that the only subplanes of $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$, are the subplanes $\mathrm{PG}(2,p^e)$, $e|h$ (Remark 2.51). In particular, the subplanes of $\mathrm{PG}(2,q)$ have the same characteristic as $\mathrm{PG}(2,q)$. This is no longer always the case for nondesarguesian planes. De Resmini and Leone proved that the derived Hughes plane of order 25 contains desarguesian subplanes $\mathrm{PG}(2,q)$, for $q = 2, 3$ and $q = 5$ [662].

See Also

§II.5	Affine and projective spaces, together with specific substructures, give Steiner systems.
§II.6	Projective planes are symmetric designs.
§II.7	Affine planes are resolvable designs.
§IV.1, §IV.2	Finite geometries provide constructions for PBDs.
§IV.6, §VI.31	Links with linear spaces.
§VI.23, §VI.41	Related incidence structures: generalized quadrangles and partial geometries.
§VI.28	Hall triple systems generalize affine planes.
[1104, 1105, 1108]	Standard references on finite geometry.
[1106]	Recent survey article on finite geometry.
[679, 1153, 1489]	Standard references on projective planes.

References Cited: [152, 351, 370, 492, 626, 661, 662, 679, 680, 683, 689, 990, 1028, 1029, 1104, 1105, 1106, 1107, 1108, 1153, 1324, 1489, 1542, 1550, 1590, 1694, 1728, 1729, 1818, 1826, 1998, 2020]

3 Divisible Semiplanes

Rudolf Mathon

3.1 A *divisible semiplane* (or *elliptic semiplane*) $\mathcal{S}$ is a set of points $\mathcal{P}$, a set of lines $\mathcal{L}$, and an incidence relation beteween $\mathcal{P}$ and $\mathcal{L}$ such that:

1. Every line is incident with k points, and dually, every point is incident with k lines.
2. Any two distinct points are incident with at most one line, and dually, any two distinct lines have at most one point in common.
3. If a point p and a line L are not incident, then there exists at most one line incident with p and parallel to L, and dually, there exists at most one point incident with L and noncollinear with p.

3.2 **Proposition** The points and lines of a divisible semiplane $\mathcal{S}$ can be partitioned into n classes of equal size m such that any two points are collinear if they belong to different classes and noncollinear if they belong to the same class, and dually, any two lines

intersect in a point if they belong to different classes and are parallel if they are in the same class. Hence, $\mathcal{S}$ can be interpreted as a *symmetric divisible design*.

3.3 The numbers (n, k, m) are the *parameters* of a divisible semiplane.

3.4 **Theorem** $|\mathcal{P}| = |\mathcal{L}| = nm$ and $k(k+1) = m(n+1)$.

3.5 **Construction** A symmetric 2-(n, k, m) design $\mathcal{D}$ from a divisible semiplane $\mathcal{S}$. Identify the point and line classes with elements and blocks of $\mathcal{D}$, respectively. A block B contains an element x if any line in the corresponding line class is incident with a (unique) point of the corresponding point class. Then $\mathcal{D}$ has n elements and n blocks, each element is in k blocks, every block has k elements, any two distinct elements are in m blocks, and any two distinct blocks have m elements in common.

3.6 **Remark** Symmetric divisible designs have been studied by Bose and Connor [305] where the Hasse–Minkowski theory of quadratic forms is used to derive necessary conditions for their existence. Additional conditions are obtained by applying the well-known Bruck–Ryser–Chowla conditions to the symmetric design associated with a semiplane.

Divisible semiplanes were introduced by Dembowski [679] in connection with projective planes.

3.7 A *standard* semiplane is either a projective plane of order q or is obtained from it by omitting a Baer subset $\mathcal{B}$. In the first case $\mathcal{S}$ has parameters $(q^2+q+1, q+1, 1)$; in the second case there are several possibilities:

1. $\mathcal{B}$ consists of a line L together with all incident points and a point p together with all incident lines. If p is incident with L, then $n = k = m = q$ and $\mathcal{S}$ is a *symmetric net* of order q. If p is not incident with L, then $n = q+1$, $k = q$, $m = q-1$, and $\mathcal{S}$ is an *affine biplane* of order q.
2. $\mathcal{B}$ is a Baer subplane of order $\sqrt{q}$. Then $\mathcal{S}$ has parameters $(q+\sqrt{q}+1, q, q-\sqrt{q})$ and is a *Baer semiplane* of order q.

3.8 **Remark** Standard divisible semiplanes have been extensively studied [142, 145, 225, 1222]. The fact that they are embeddable in projective planes plays an important role in the analysis of their structural properties and symmetries. A semiplane that is not of standard type must have $m < q - \sqrt{q}$ and is not directly related to a projective plane. Only two nonstandard semiplanes are known.

3.9 **Example** A $(15, 7, 3)$ divisible semiplane (Baker [142]).

Let I be the 3×3 identity matrix. Let $\begin{pmatrix} 0&1&0 \\ 1&0&0 \\ 0&0&1 \end{pmatrix}$, $\begin{pmatrix} 1&0&0 \\ 0&0&1 \\ 0&1&0 \end{pmatrix}$, and $\begin{pmatrix} 0&0&1 \\ 0&1&0 \\ 1&0&0 \end{pmatrix}$ be A, B, and C, respectively. Substitute these 3×3 blocks into the matrix on the right. The result is an incidence matrix in which rows index the points, and columns the lines, of a divisible semiplane. It is a 7-GDD of type 3^{15} in which the groups are the sets of points indexed within each 3×3 block.

	I	I	I	I	I	I	I							
I		A	B		C				A	C		B		
I			A	B		C				A	C		B	
I				A	B		C				A	C		B
I	C				A	B		B				A	C	
I		C				A	B		B				A	C
I	B		C				A	C		B				A
I	A	B		C				A	C		B			
		A	C		B			A			C		C	C
			A	C		B		C	A			C		C
				A	C		B	C	C	A			C	
	B				A	C			C	C	A			C
		B				A	C	C		C	C	A		
	C		B				A		C		C	C	A	
	A	C		B						C		C	C	A

3.10 Example A $(45, 12, 3)$ divisible semiplane, given as nine base blocks to be developed mod $(-, 5, 3)$:

$\{0_{00}, 1_{01}, 2_{01}, 0_{21}, 3_{22}, 6_{22}, 0_{30}, 4_{30}, 8_{31}, 2_{41}, 4_{41}, 6_{41}\}$,
$\{0_{01}, 1_{00}, 2_{01}, 2_{20}, 5_{22}, 8_{20}, 1_{32}, 5_{31}, 6_{31}, 0_{41}, 5_{42}, 7_{40}\}$,
$\{0_{01}, 1_{01}, 2_{00}, 1_{20}, 4_{20}, 7_{22}, 2_{32}, 3_{30}, 7_{32}, 1_{40}, 3_{42}, 8_{41}\}$,
$\{3_{00}, 4_{01}, 5_{01}, 0_{22}, 3_{22}, 6_{21}, 1_{30}, 5_{30}, 6_{31}, 1_{42}, 3_{42}, 8_{42}\}$,
$\{3_{01}, 4_{00}, 5_{01}, 2_{22}, 5_{20}, 8_{20}, 2_{31}, 3_{30}, 7_{30}, 2_{42}, 4_{40}, 6_{41}\}$,
$\{3_{01}, 4_{01}, 5_{00}, 1_{20}, 4_{22}, 7_{20}, 0_{30}, 4_{31}, 8_{30}, 0_{41}, 5_{40}, 7_{42}\}$,
$\{6_{00}, 7_{01}, 8_{01}, 0_{21}, 3_{20}, 6_{21}, 2_{30}, 3_{30}, 7_{31}, 0_{40}, 5_{40}, 7_{40}\}$,
$\{6_{01}, 7_{00}, 8_{01}, 2_{22}, 5_{22}, 8_{21}, 0_{30}, 4_{32}, 8_{32}, 1_{40}, 3_{41}, 8_{42}\}$,
$\{6_{01}, 7_{01}, 8_{00}, 1_{21}, 4_{22}, 7_{22}, 1_{31}, 5_{32}, 6_{31}, 2_{42}, 4_{41}, 6_{40}\}$.

3.11 Remark This semiplane was first presented by the author at the Eleventh British Combinatorial Conference held at the University of London in 1987.

3.12 Theorem Removing the 36 points of three disjoint blocks of size 12 yields a 9-GDD of type 3^{33} having three orthogonal resolutions.

3.13 Remark Divisible semiplanes are also related to many other combinatorial configurations such as equidistant permutation arrays, generalized weighing matrices, Howell designs and Room squares [1395, 2094]. Add the groups as new blocks to an (n, k, m) divisible semiplane to obtain a $(k + 1, 1)$-design (pairwise balanced with constant $r = k+1$). From it construct a doubly resolvable $(k, 1)$-design on $v = (m+1)n-k^2-2$ elements (see [2094]). A generalized Room square $\mathrm{GRS}(k, 1; v)$ has rows and columns indexed by the parallel classes from the two orthogonal resolutions, determining the position of a block in the square. Apply Theorems VI.44.30 to obtain an $\mathrm{EPA}(k, k-1)$ of size v. This equidistant permutation array gives a nonlinear equidistant code.

See Also

§II.6	Symmetric designs underlie divisible semiplanes.
§IV.4	Symmetric group divisible designs arise from divisible semiplanes.
§V.6	Balanced generalized weighing matrices arise from divisible semiplanes.
§VI.49	Doubly resolvable (r, λ)-designs arise from divisible semiplanes.
§VI.50	Generalized Room squares arise from divisible semiplanes.
§VI.44	Generalized Room squares and equidistant permutation arrays.

References Cited: [142, 145, 225, 305, 679, 1222, 1395, 2094]

4 Graphs and Multigraphs

Gordon F. Royle

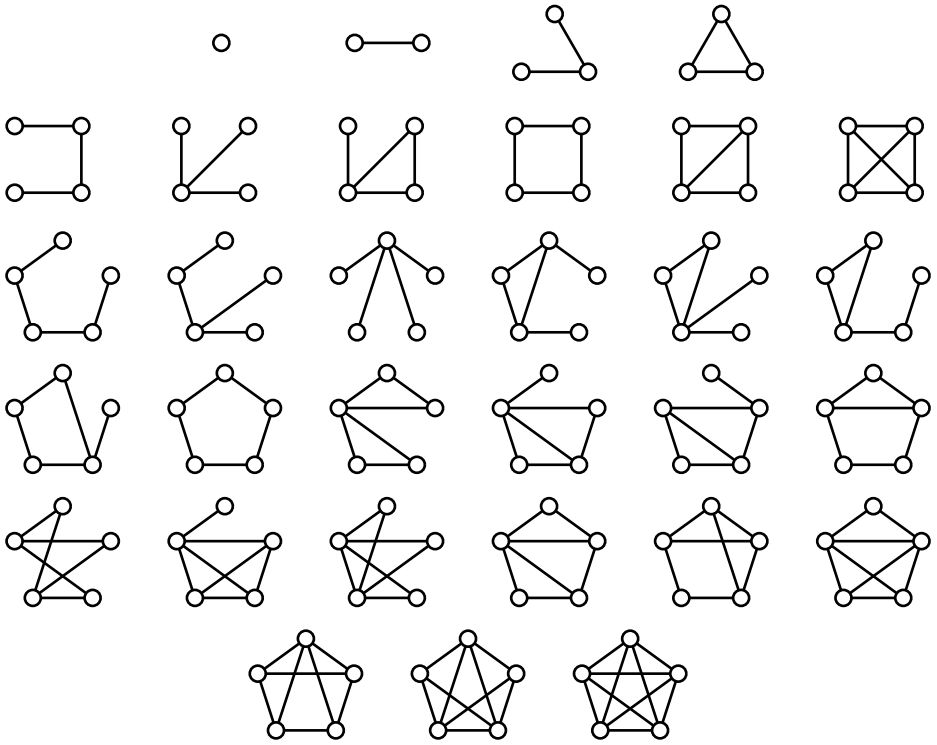
4.1 All Graphs

4.1 A finite graph G is a pair $(V(G), E(G))$ where $V(G)$ is a finite set, the *vertices* of G, and $E(G)$ is a set of unordered pairs of distinct vertices of G, the *edges* of G.

4.2 Graphs G and H are *isomorphic* if there is a bijection $\phi : V(G) \to V(H)$ such that $\{v, w\} \in E(G)$ if and only if $\{\phi(v), \phi(w)\} \in E(H)$. An *automorphism* of a graph G is an isomorphism from G to itself. The set of all automorphisms of G forms a group under composition and is denoted $\mathrm{Aut}(G)$.

4.3 If $\{v, w\} \in E(G)$, then v and w are *adjacent*, written $v \sim w$. A *path* of length n from v_0 to v_n is a sequence $v_0 \sim v_1 \sim \cdots \sim v_n$ of distinct vertices. A graph is *connected* if there is a path from any vertex to any other.

4.4 **Table** The connected graphs on up to five vertices.



4.5 **Remark** The numbers of pairwise nonisomorphic graphs can be computed exactly by using Polya's enumeration theory (see [1056]). All numbers given in this chapter refer to numbers of pairwise nonisomorphic graphs.

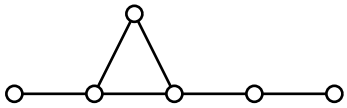
4.6 **Table** Numbers of graphs on up to 16 vertices.

n	All Graphs	Connected Graphs
1	1	1
2	2	1
3	4	2
4	11	6
5	34	21
6	156	112
7	1044	853
8	12346	11117
9	274668	261080
10	12005168	11716571
11	1018997864	1006700565
12	165091172592	164059830476
13	50502031367952	50335907869219
14	29054155657235488	29003487462848061
15	31424685969804308768	31397381142761241960
16	6400101570452755789492 8	6396956011322517617627 7

4.7 **Theorem** Every finite abstract group occurs as the automorphism group of some graph (see [1055]).

4.8 **Theorem** Almost all graphs have trivial automorphism group.

4.9 **Example** The smallest graph with trivial automorphism group has 6 vertices and 6 edges.



4.10 The *complement* of a graph G is the graph $\overline{G}$ on the same vertex set and where two vertices are adjacent in $\overline{G}$ if and only if they are not adjacent in G. A graph is *self-complementary* if it is isomorphic to its complement.

4.11 **Table** Numbers of self-complementary graphs on 5 to 17 vertices.

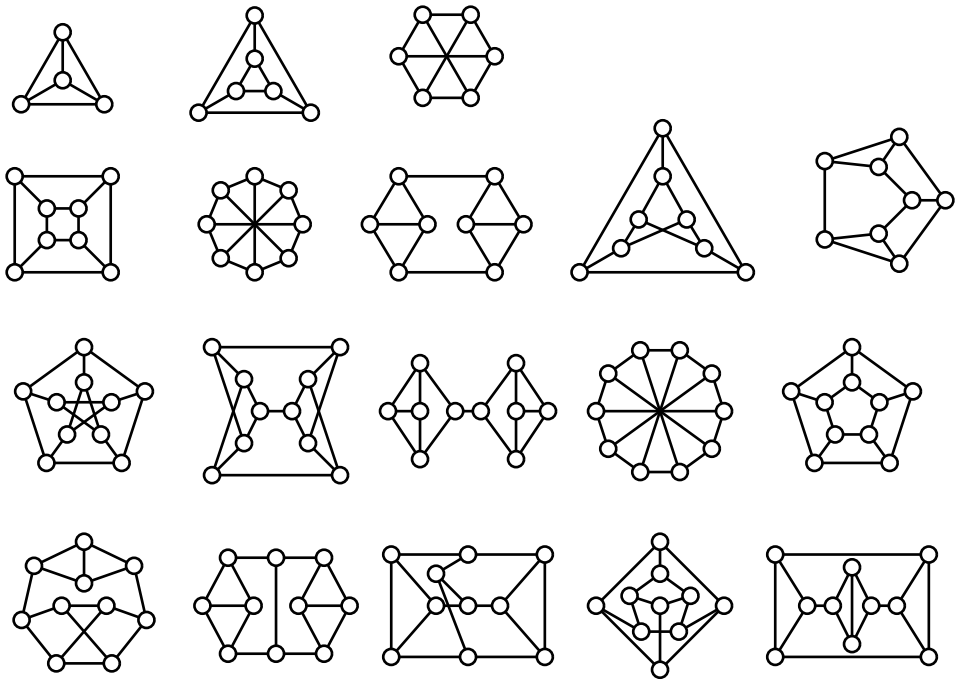
n	5	6	7	8	9	10	11	12	13	14	15	16	17
$sc(n)$	2	0	0	10	36	0	0	720	5600	0	0	703760	11220000

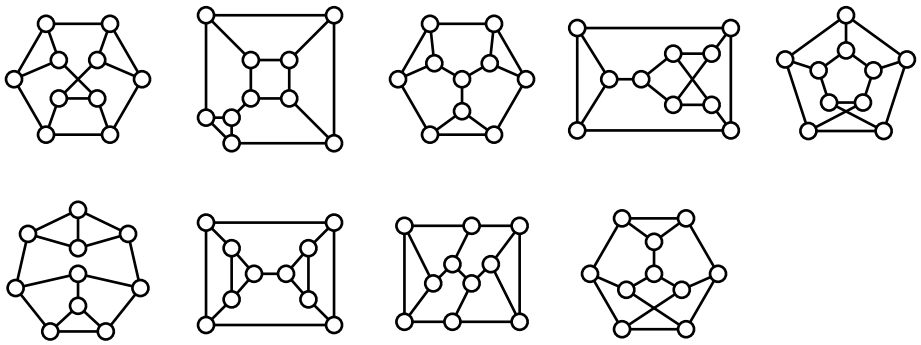
4.12 **Remark** The number of self-complementary graphs on n vertices is equal to the difference between the number of graphs on n vertices with an even number of edges and the number of graphs on n vertices with an odd number of edges.

4.2 Regular Graphs

4.13 A graph is *regular* with *degree* k if each vertex is adjacent to exactly k other vertices. A regular graph of degree 3 is a *cubic graph*.

4.14 **Table** Connected cubic graphs on up to 10 vertices.





4.15 **Remark** The smallest regular graphs with trivial automorphism group are 4-regular graphs on 10 vertices or 3-regular graphs on 12 vertices.

4.16 The *distance* between any two vertices is the length of the shortest path between them, and the *diameter* of the graph is the longest of these distances. A *cycle* of length n is a sequence $v_0 \sim v_1 \sim \cdots \sim v_{n-1} \sim v_0$ of distinct vertices (except that v_0 occurs twice), and the *girth* of a graph is the length of the shortest cycle.

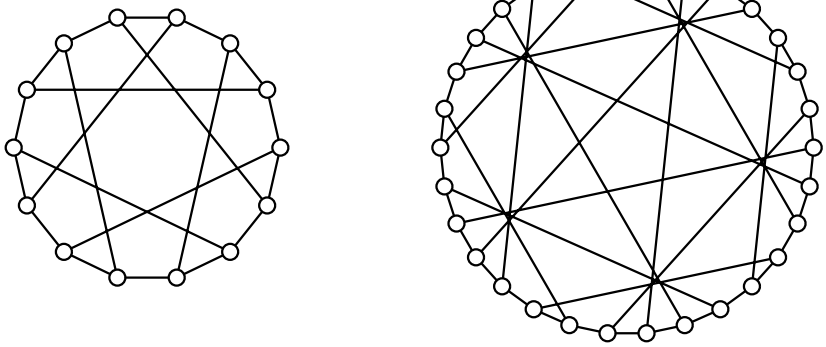
4.17 **Remarks** The exact number of cubic graphs can be computed analytically by results of Robinson and Wormald [1809]. However, the results in Table 4.18 for cubic graphs of a given girth were found by constructing all the graphs using the algorithm in [327]. An explicit listing of all cubic graphs on $2n$ vertices for $2n \leq 22$ is available from `http://www.csse.uwa.edu.au/~gordon/data.html`.

4.18 **Table** Numbers of connected cubic graphs tabulated according to girth g. Missing entries in the top right of the table are zeros, whereas missing entries at the bottom are unknown values.

n	$g \geq 3$	$g \geq 4$	$g \geq 5$	$g \geq 6$	$g \geq 7$	$g \geq 8$
4	1					
6	2	1				
8	5	2				
10	19	6	1			
12	85	22	2			
14	509	110	9	1		
16	4060	792	49	1		
18	41301	7805	455	5		
20	510489	97546	5783	32		
22	7319447	1435720	90938	385		
24	117940535	23780814	1620479	7574	1	
26	2094480864	432757568	31478584	181227	3	
28	40497138011		656783890	4624501	21	
30	845480228069			122090544	546	1
32	18941522184590				30368	0
34	453090162062723					1
36	11523392072541432					3
38	310467244165539782					13
40	8832736318937756165					155

4.19 A graph is *bipartite* if the vertex set can be partitioned into two sets $V(G) = X \cup Y$ such that every edge has one vertex in X and the other in Y.

4.20 Example The point/block incidence graph of an incidence structure is a bipartite graph. The projective plane $PG(2,2)$ yields a 14-vertex cubic bipartite graph with girth 6, *Heawood's graph*, and the generalized quadrangle $W(2)$ (Example VI.23.7) yields a 30-vertex cubic bipartite graph with girth 8, *Tutte's 8-cage*.



4.21 A k-regular graph of girth g is a (k,g)-*cage* if it has the minimum number of vertices among all k-regular graphs of girth g.

4.22 Remark The $(3,g)$-cages are known for $g \leq 12$ and are listed in Table 4.23; the smallest *known* cubic graph with girth 13 has 272 vertices, but it is unknown if there is a smaller one.

4.23 Table Cubic cages of girth $g \leq 12$.

Girth g	Size	Cages	Girth g	Size	Cages
3	4	K_4	4	6	$K_{3,3}$
5	10	Petersen graph	6	14	Heawood graph
7	24	McGee graph	8	30	Tutte's 8-cage
9	58	18 different graphs	10	70	3 different graphs
11	112	Balaban graph	12	126	Generalized hexagon $H(2)$

4.24 Remark Although there are results on the enumeration of *labeled* regular graphs of degree four and five, there are no currently available theoretical tools for counting pairwise nonisomorphic regular graphs of degree higher than three. Therefore, all of the remaining results are obtained by direct computer enumeration, with the larger numbers in Table 4.25 from Markus Meringer's program **genreg** [1592].

4.25 Table Numbers of connected k-regular graphs on up to 16 vertices.

$n\backslash k$	4	5	6	7	8	9	10
5	1						
6	1	1					
7	2		1				
8	6	3	1	1			
9	16		4		1		
10	59	60	21	5	1	1	
11	265		266		6		1
12	1544	7848	7849	1547	94	9	1
13	10778		367860		10786		
14	88168	3459383	21609300	21609301	3459386	88193	540
15	805491		1470293675		1470293676		805579
16	8037418	2585136675	?	?	?	?	?

4.26 **Table** Numbers of connected k-regular bipartite graphs on up to 20 vertices.

$n\backslash k$	2	3	4	5	6	7	8	9	10
6	1	1							
8	1	1	1						
10	1	2	1	1					
12	1	5	4	1	1				
14	1	13	14	4	1	1			
16	1	38	129	41	7	1	1		
18	1	149	1980	1981	157	8	1	1	
20	1	703	62611	304495	62616	725	12	1	1

4.3 Planar Graphs

4.27 A graph G is *planar* if it can be drawn in the plane with no crossing edges. A planar graph with n vertices has at most $3n - 6$ edges and is a *planar triangulation* if it meets this bound. A 3-connected planar graph is a *polytope*.

4.28 **Remark** One of the most famous results in graph theory is the *Four Color Theorem*: Any planar graph can be colored with 4 colors: Each vertex can be assigned a color from a collection of 4 colors in such a way that every edge joins two vertices of different colors.

4.29 **Table** Numbers of 3-connected planar graphs and planar triangulations on 4-18 vertices. These numbers were computed by the program *plantri* written by Gunnar Brinkmann and Brendan McKay (see `http://cs.anu.edu.au/~bdm/plantri`).

n	Polytopes	Triangulations
4	1	1
5	2	1
6	7	2
7	34	5
8	257	14
9	2606	50
10	32300	233
11	440564	1249
12	6384634	7595
13	96262938	49566
14	1496225352	339722
15	23833988129	2406841
16	387591510244	17490241
17	6415851530241	129664753
18	107854282197058	977526957

4.4 Transitive Graphs

4.30 A graph G is *vertex-transitive* if for any two vertices v and w there is an automorphism $\sigma \in \mathrm{Aut}(G)$ such that $\sigma(v) = w$. (Equivalently, $\mathrm{Aut}(G)$ is transitive on $V(G)$.) A vertex-transitive graph is necessarily regular.

4.31 A graph G is a *Cayley graph* if there is a subgroup $A \leq \mathrm{Aut}(G)$ such that for any two vertices v and w, there is *exactly one* automorphism $\sigma \in A$ such that $\sigma(v) = w$. (Equivalently, A acts regularly on $V(G)$.)

4.32 **Table** Numbers of vertex-transitive graphs on up to 26 vertices tabulated by degree k [1576]. Totals include the degrees not tabulated.

$n\backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	12	Total
1	1													1
2	1	1												2
3	1		1											2
4	1	1	1	1										4
5	1		1		1									3
6	1	1	2	2	1	1								8
7	1		1		1		1							4
8	1	1	2	3	3	2	1	1						14
9	1		2		3		2		1					9
10	1	1	2	3	4	4	3	2	1	1				22
11	1		1		2		2		1		1			8
12	1	1	4	7	11	13	13	11	7	4	1	1		74
13	1		1		3		4		3		1		1	14
14	1	1	2	3	6	6	9	9	6	6	3	2	1	56
15	1		3		8		12		12		8		3	48
16	1	1	3	7	16	27	40	48	48	40	27	16	7	286
17	1		1		4		7		10		7		4	36
18	1	1	4	7	16	24	38	45	54	54	45	38	24	380
19	1		1		4		10		14		14		10	60
20	1	1	4	11	28	47	83	115	149	168	168	149	115	1214
21	1		3		11		29		48		56		48	240
22	1	1	2	3	11	18	38	52	79	94	109	109	94	816
23	1		1		5		15		30		42		42	188
24	1	1	6	20	74	167	373	652	1064	1473	1858	2064	2064	15506
25	1		2		9		25		57		86		104	464
26	1	1	2	5	16	29	71	117	204	286	397	466	523	4236

4.33 **Remark** The vast majority of the small vertex-transitive graphs are Cayley graphs, but it is not known if this situation continues for higher orders.

4.34 **Table** Numbers of vertex-transitive graphs that are not Cayley graphs.

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	Total
10	1			1							2
15		1		1		1		1			4
16		1	1	1	1	1	1	1	1		8
18			1			1	1			1	4
20	3	4	4	7	8	7	8	8	7	8	82
24			1	5	7	9	11	11	12	12	112
26	1		2	3	7	6	8	13	14	12	132

4.5 Multigraphs and Digraphs

4.35 A *multigraph* G is a pair $(V(G), E(G))$ where $V(G)$ is a finite set, the *vertices* of G, and $E(G)$ is a multiset of unordered pairs of distinct vertices (*edges*).

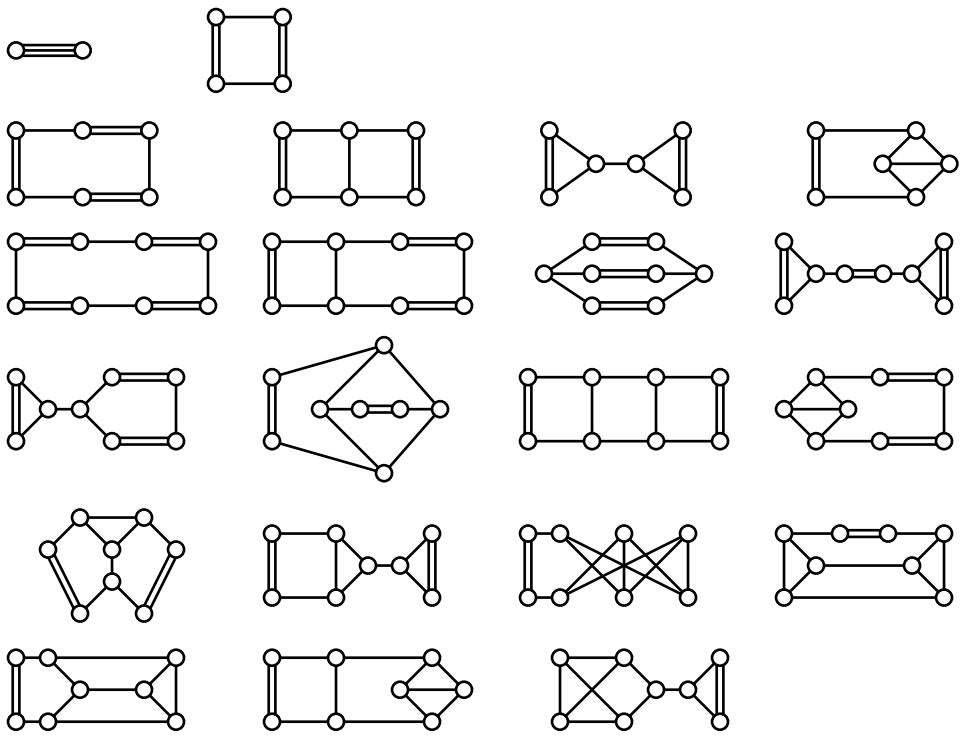
4.36 A *directed graph* or *digraph* D is a pair $(V(D), A(D))$ where $V(D)$ is a finite set, the *vertices* of D, and $A(D)$ is a set of ordered pairs of distinct vertices (*arcs*). A *tournament* is a digraph where for every pair of distinct vertices $v, w \in V(D)$, exactly one of (v, w) and (w, v) is an arc.

4.37 **Remark** Both multigraphs with a given number of edges and digraphs with a given number of arcs can be counted by applications of Polya's enumeration theory.

4.38 **Table** Multigraphs on up to eight vertices, tabulated by number of edges e.

e	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$
0	1	1	1	1	1	1
1	1	1	1	1	1	1
2	2	3	3	3	3	3
3	3	6	7	8	8	8
4	4	11	17	21	22	23
5	5	18	35	52	60	64
6	7	32	76	132	173	197
7	8	48	149	313	471	588
8	10	75	291	741	1303	1806
9	12	111	539	1684	3510	5509
10	14	160	974	3711	9234	16677
11	16	224	1691	7895	23574	49505
12	19	313	2874	16310	58464	143761
13	21	420	4730	32604	140340	406091
14	24	562	7620	63363	326792	1114890
15	27	738	11986	119745	738090	2970964
16	30	956	18485	220546	1619321	7685972
17	33	1221	27944	396428	3455129	19311709
18	37	1550	41550	696750	7180856	47170674
19	40	1936	60744	1198812	14555856	112123118

4.39 **Table** Connected cubic multigraphs on up to eight vertices (excluding the cubic graphs in Table 4.14).



4.40 Table The number N_c of connected cubic multigraphs on up to 18 vertices (including the cubic graphs).

n	2	4	6	8	10	12	14	16	18
N_c	1	2	6	20	91	509	3608	31856	340416

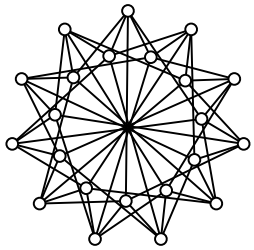
4.41 Table Numbers of digraphs on up to 10 vertices.

n	Digraphs	Tournaments
1	1	1
2	3	1
3	16	2
4	218	4
5	9608	12
6	1540944	56
7	882033440	456
8	1793359192848	6880
9	13027956824399552	191536
10	341260431952972580352	9733056

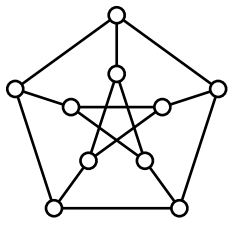
4.6 Some Graphs from Designs

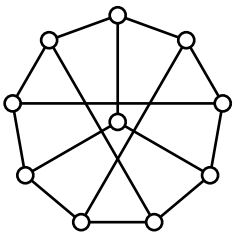
4.42 Remarks Graphs are constructed from designs in a variety of different ways. In particular many examples of strongly regular or distance-regular graphs come from designs.

4.43 Example The point/block incidence graph of a design often leads to interesting graphs, as already seen with Heawood's graph. The point/block incidence graph of the unique 2-(11,5,2) design (the biplane of order 3, Example II.1.26) is a bipartite distance-regular graph of diameter 3. In fact, symmetric designs are equivalent to bipartite distance-regular graphs of diameter 3.



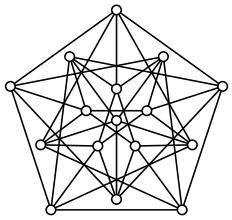
4.44 Example There are several ways to define a graph on the blocks of a design. The following graph is defined on the blocks of the unique 2-(6,3,2) design (Example II.1.18) where two vertices are adjacent if the corresponding blocks meet in exactly two points. This graph is a strongly regular graph, *Petersen's graph*; two of the many possible drawings are given.





4.45 Remark This construction always results in a strongly regular graph if the design is quasi-symmetric.

4.46 **Example** A (16,5,0,2) strongly regular graph, the *Clebsch graph*. If A is the adjacency matrix of this graph, then $A + I$ is a point/block incidence matrix for a 2-(16,6,2) design, namely, the biplane of order 4 with a doubly transitive automorphism group. (See Example II.1.32.)



4.47 **Remark** If a symmetric design has a polarity, then its point/block incidence matrix A can be chosen to be symmetric. If the polarity has the property that no point lies on its polar block, then the diagonal of the matrix is 0 and the matrix is the adjacency matrix of a strongly regular graph. If, as in Example 4.46, every point lies on its polar block then $A - I$ is the adjacency matrix of a strongly regular graph.

4.48 **Remark** The 2-(16,6,2) design mentioned in Example 4.46 has two further polarities with no absolute points; the corresponding graphs are (16,6,2,2) strongly regular graphs: the *Shrikhande graph* and the lattice graph $L_2(4)$.

See Also

[1056]	Many enumeration techniques related to graphs and other combinatorial structures.
[1785]	Very comprehensive listings of data relating to graphs, including thousands of pictures of graphs and hundreds of tables.
[293, 1055]	Two of the standard references in graph theory.
[989]	*The CRC Handbook of Graph Theory*.

References Cited: [293, 327, 989, 1055, 1056, 1576, 1592, 1785, 1809]

5 Factorizations of Graphs

Lars D. Andersen

5.1 Definitions and Examples

5.1 A *factor* of a multigraph G is a submultigraph of G including all vertices of G (a *spanning* submultigraph). For a nonnegative integer r, an *r-factor* is a factor that is regular of degree r.

5.2 A *factorization* of a multigraph G is a set $\mathcal{F} = \{F_1, \ldots, F_k\}$ of edge-disjoint factors of G whose edge-sets partition the edge-set of G. A factorization into r-factors for some nonnegative integer r is an *r-factorization*.

5.3 **Remark** As the factors in a factorization of a multigraph are permitted to have isolated vertices, almost any graph decomposition problem is a factorization problem. The focus here is on r-factorizations. Only regular multigraphs can have r-factorizations.

5.4 Two factorizations $\mathcal{F} = \{F_1, \ldots, F_k\}$ and $\mathcal{G} = \{G_1, \ldots, G_\ell\}$ of a multigraph are *orthogonal* if any factor of $\mathcal{F}$ and any factor of $\mathcal{G}$ have at most one edge in common.

5.5 **Remark** In [84] two factorizations satisfying the definition above are *suborthogonal*. If each factor of $\mathcal{F}$ has *exactly* one edge in common with each factor of $\mathcal{G}$, then $\mathcal{F}$ and $\mathcal{G}$ are *orthogonal*. This notation, although useful, is not adopted here.

5.6 **Remark** Two r-factorizations of a (simple) graph G of order n cannot be orthogonal unless $r = 1$, and then only if G is regular of degree at least $\frac{n}{2}$.

5.7 **Example** A 2-factorization and three pairwise orthogonal 1-factorizations of $K_{4,4}$. The vertices $\{1, 2, 3, 4\}$ are completely joined to $\{A, B, C, D\}$. Each factorization is a line, factors are separated by semicolons, and only edge-sets are shown.

1A A2 2B B1 3D D4 4C C3; 1C C2 2D D1 3A A4 4B B3
1A 2B 3C 4D; 1B 2A 3D 4C; 1C 2D 3A 4B; 1D 2C 3B 4A
1A 2D 3B 4C; 1B 2C 3A 4D; 1C 2B 3D 4A; 1D 2A 3C 4B
1A 2C 3D 4B; 1B 2D 3C 4A; 1C 2A 3B 4D; 1D 2B 3A 4C

5.2 Existence Results for Factorizations

5.8 **Remarks** Deciding whether a cubic graph has a 1-factorization is NP-complete [1123]. It follows that the 1-factorization problem is NP-complete in general, and that the problem of deciding whether a graph has two edge-disjoint 1-factors is also NP-complete. See §VII.6 for a discussion of NP-completeness in design theory; see [860] for a general discussion. Deciding whether a graph has a 1-factor is polynomial, and there is a good characterization of graphs having a 1-factor [293].

5.9 **Theorem** The following multigraphs have 1-factorizations; therefore, they have r-factorizations for any r dividing their degree:

1. Regular bipartite multigraphs—in particular, $K_{n,n}$ and the hypercube Q^n.
2. Regular graphs of order $2n$ and degree $d \geq (\sqrt{7} - 1)n$—in particular, K_{2n} [494].
3. Planar cubic multigraphs without bridges [105].

5.10 **Remark** Many other classes of multigraphs are known to have 1-factorizations. Petersen's graph is a notable example of a cubic graph *not* having a 1-factorization. *Snarks* are cubic graphs that do not have a 1-factorization (and satisfy some connectivity condition that varies in the literature) (see [2125]).

5.11 **Conjecture** Any regular graph of order $2n$ and degree at least n has a 1-factorization.

5.12 **Theorem** A multigraph has a 2-factorization if and only if it is regular of even degree.

5.13 **Remark** It follows from Theorem 5.12 that a regular multigraph has r-factorizations for all even r dividing the degree. Theorem 5.14, about graphs only, allows r to be odd. Theorem 5.15 is about factorizations into *semiregular* factors.

5.14 **Theorem** [1100] Let G be a graph of order $2n$ that is regular of degree at least n, and let $r \geq 2$. Then G has an r-factorization if and only if r divides the degree of G.

5.15 **Theorem** [1102] For nonnegative integers d, s, and r, any graph for which each vertex has degree in the interval $[d, d + s]$ has a factorization in which each vertex of each factor has degree r or $r + 1$ if $d \geq \varphi(r, s)$, where

$$\varphi(r,s) = \begin{cases} r(r+s) & \text{if } s \in \{0,1\} \text{ and } r \text{ is even,} \\ r(r+s)+1 & \text{if } s \in \{0,1\} \text{ and } r \text{ is odd,} \\ r(r+s+1)+1 & \text{if } s \geq 2, \end{cases}$$

and these values are best possible.

5.3 Equivalent Combinatorial Objects

5.16 Theorem The existence of the following are equivalent:

1. A 1-factorization of K_n.
2. A symmetric latin square of order $n-1$.
3. A unipotent (*constant diagonal*) symmetric latin square of order n.
4. A resolution of a BIBD$(n, 2, 1)$.
5. A round robin tournament with n players played in $n-1$ rounds (see §VI.51.1).

5.17 Theorem The existence of the following are equivalent:

1. Two orthogonal 1-factorizations of K_n.
2. Two orthogonal-symmetric latin squares of order $n-1$ (see [725]).
3. Two orthogonal resolutions of a BIBD$(n, 2, 1)$.
4. A Room square of side $n-1$ (see §VI.50).
5. A Room frame of type 1^{n-1} (see §VI.50).
6. A Howell design $H(n-1, n)$ (see §VI.29).

5.18 Theorem For any integer $d \geq 2$, the existence of the following are equivalent:

1. d pairwise orthogonal 1-factorizations of K_n.
2. d pairwise orthogonal-symmetric latin squares of order $n-1$.
3. d pairwise orthogonal resolutions of a BIBD$(n, 2, 1)$.
4. A Room d-cube of side $n-1$ (see §VI.50).

5.19 Theorem For any positive integer d, the existence of the following are equivalent:

1. d pairwise orthogonal 1-factorizations of $K_{n,n}$.
2. d pairwise orthogonal latin squares of order n.
3. A transversal design TD$(d+2, n)$ (see §III.3).
4. An orthogonal array OA$(d+2, n)$ (see §III.6).

5.20 Remark For $d = 1$, Theorem 5.19 states that the existence of a 1-factorization of $K_{n,n}$ is equivalent to the existence of a latin square of order n (see Theorem III.1.11 for other equivalences).

5.21 Remark Just as a 1-factorization of K_n models a round robin tournament played in rounds (Theorem 5.16), a 1-factorization of $K_{n,n}$ is a simple model of a tournament where each player from one team plays each player from another team, with the tournament partitioned into rounds. (See also Example VI.51.47.)

5.22 Remark See Theorem VI.29.11 for the connection between orthogonal 1-factorizations and Howell designs.

5.4 Enumeration and Tables

5.23 LF$(2n)$ is the number of 1-factorizations of a labeled K_{2n}.

5.24 Two 1-factorizations $F = \{f_1, f_2, \ldots, f_k\}$ and $H = \{h_1, h_2, \ldots, h_k\}$ of G are *isomorphic* if there exists a map ϕ from the vertex-set of G onto itself such that $\{f_1\phi, f_2\phi, \ldots, f_k\phi\} = \{h_1, h_2, \ldots, h_k\}$. Here, $f_i\phi$ is the graph (1-factor) with edges $\{x\phi, y\phi\}$ where $\{x, y\}$ is an edge in f_i.

5.25 NF$(2n)$ is the number of pairwise nonisomorphic 1-factorizations of K_{2n}.

5.26 Table The known values for the number of distinct and the number of nonisomorphic 1-factorizations of K_{2n} [715, 2107].

$2n$	2	4	6	8	10	12
LF($2n$)	1	1	6	6,240	1,225,566,720	252,282,619,805,368,320
NF($2n$)	1	1	1	6	396	526,915,620

5.27 Remark A discussion of the computer algorithm used to obtain the results on K_{12} in Table 5.26 can be found in Example VII.6.26.

5.28 Remark In [715] the following estimates are given for the number of distinct 1-factorizations of K_{14}, K_{16} and K_{18}. Assuming that most distinct OFs have only trivial automorphisms, an estimate for the number of nonisomorphic 1-factorizations is obtained by dividing the number of distinct 1-factorizations of K_n by $n!$.

$2n$	14	16	18
estimated LF($2n$)	9.876×10^{28}	1.48×10^{44}	1.52×10^{63}
estimated NF($2n$)	1.132×10^{18}	7.07×10^{30}	2.37×10^{47}

5.29 Theorem

1. $\mathrm{NF}(2n) \leq ((2n-1)!)^{n-1}$;
2. $\lim_{n\to\infty} \log(\mathrm{NF}(2n))/(2n^2 \log(2n)) = 1$ [415].

5.30 Table The six nonisomorphic factorizations of K_8. Each line is a factorization, with the number at the end. Each block of digits is a 1-factor, with 0 omitted, so that, for example, 1234567 denotes the 1-factor with edges 01, 23, 45, and 67.

1234567 2134657 3124756 4152637 5142736 6172435 7162534 1
1234567 2134657 3124756 4152637 5142736 6172534 7162435 2
1234567 2134657 3124756 4162537 5172634 6142735 7152436 3
1234567 2134657 3124756 4162735 5172634 6142537 7152436 4
1234567 2134657 3142756 4162537 5172634 6123547 7152436 5
1234567 2143657 3162547 4172635 5123746 6152734 7132456 6

5.31 Table The 396 nonisomorphic factorizations of K_{10}. Notation as in Table 5.30.

123456789 213465879 312495768 415263978 514283769 617243859 716293548 819253647 918273456 1
123456789 213465879 312495768 415263978 514283769 617243859 716293548 819273456 918253647 2
123456789 213465879 312475968 415263978 514283769 617253849 716293548 819243657 918273456 3
123456789 213465879 312475968 415263978 514283769 617253849 716293548 819273456 918243657 4
123456789 213465879 312495768 415263978 514283769 617293548 716243859 819273456 918253647 5
123456789 213465879 312475968 415263978 514283769 619273548 716253849 817293456 918243657 6
123456789 213465879 312475968 415263978 514283769 617253849 718293456 819243657 916273548 7
123456789 213465879 312495768 415263978 516293847 619253748 714283659 817243569 918273456 8
123456789 213465879 312495768 415263978 516293748 617243859 714283569 819273456 918253647 9
123456789 213465879 312475968 416283957 518263749 617293548 715243869 819273456 914253678 10
123456789 213465879 312495768 416273859 518293647 614253978 719283456 815243769 917263548 11
123456789 213465879 312495768 415283769 514263978 618293547 719243856 816273459 917253648 12
123456789 213465879 312495768 415283769 516293478 614273859 719263548 817243956 918253647 13
123456789 213465879 312475968 415263978 516283749 614293857 719253648 817243569 918273456 14
123456789 213465879 312475968 415263978 516283749 617293548 714253869 819243657 918273456 15
123456789 213465879 312475968 415263978 516283749 619273548 714293856 817253469 918243657 16
123456789 213465879 312475968 415263978 518273469 617293548 716253849 819243756 914283657 17
123456789 213465879 312495768 415263978 516293847 614283759 719253648 817243569 918273456 18
123456789 213465879 312495768 415263978 514283769 617293548 718243659 819273456 916253847 19
123456789 213465879 312475968 415263978 516293748 617253849 714283569 819243657 918273456 20
123456789 213465879 312475968 415263978 514283769 618293457 719253648 816273549 917243856 21
123456789 214365879 315264978 412375968 513274869 618293457 719243856 817253946 916283547 22
123456789 213465879 312475968 415263978 514283769 619273548 718253649 817293456 916243857 23
123456789 213465879 312475968 416253978 518243769 617293548 715263849 819273456 914283657 24
123456789 214365879 315264978 412375968 513284769 619243857 718293456 817253946 916273548 25
123456789 213465879 312475968 415263978 514273869 617283549 718293456 819243657 916253748 26
123456789 213465879 312475968 415263978 518273649 617293548 714253869 819243756 916283457 27
123456789 213465879 314256978 412395768 518273649 615293847 716283459 819243756 917263548 28
123456789 213465879 312475968 415263978 516283749 617293548 714253869 819273456 918243657 29
123456789 213465879 312475968 416253978 518273469 617283549 714293856 819243657 915263748 30
123456789 213465879 314256978 412395768 516293847 617283459 718263549 819243756 915273648 31
123456789 213465879 314265978 412385769 516283947 619253748 718293456 815273649 917243568 32
123456789 214365879 315264978 412375968 513274869 618243957 719253846 816293547 917283456 33
123456789 213465879 312495768 415263978 517243869 618293547 719283456 814273659 916253748 34
123456789 213465879 312475968 416253978 518273469 617293548 715263849 819243756 914283657 35

123456789	213465879	312495768	416253978	517283469	618243759	719263548	815293647	914273856	36
123456789	213465879	312495768	415263978	516293748	619283547	718253469	817243659	914273856	37
123456789	213465879	312495768	415263978	517283469	614273859	719253648	816293547	918243756	38
123456789	213465879	314256978	412375968	516283947	619243857	718293456	815273649	917263548	39
123456789	213465879	312495768	415263978	516293847	614283759	718243569	819273456	917253648	40
123456789	213465879	312475968	415263978	516283749	614293857	718243569	819273456	917253648	41
123456789	213465879	312475968	415263978	516293748	617283549	718253469	819243657	914273856	42
123456789	214365879	315264978	412375968	513284769	618293457	719243856	817253946	916273548	43
123456789	213465879	312495768	415263978	517243869	614283759	716293548	819273456	918253647	44
123456789	213465879	314256978	412375968	516283947	617293548	719243856	815273649	918263457	45
123456789	213465879	314256978	415273968	516283749	617293548	718263459	819243657	912384756	46
123456789	213465879	312475968	415263978	518273469	617283549	714293856	819243657	916253748	47
123456789	213465879	312475968	415263978	518243769	617293548	716253849	819273456	914283657	48
123456789	214365879	315264978	412375968	513274869	618243957	719283456	817293546	916253847	49
123456789	213465879	314256978	412375968	516293847	618243957	719283456	817263549	915273648	50
123456789	213465879	312475968	416253978	518243769	617293548	715283649	819273456	914263857	51
123456789	213465879	312475968	415263978	514283769	618273549	719253648	817293456	916243857	52
123456789	213465879	314265978	415273968	516293748	617283549	719243856	812345769	918253647	53
123456789	213465879	314256978	415273968	516293748	619283457	712384956	817243659	918263547	54
123456789	213465879	312475968	416293857	519273648	615243978	718263549	814253769	917283456	55
123456789	213465879	314256978	412375968	516283947	619273548	715263849	817293456	918243657	56
123456789	213465879	314256978	412375968	517263948	615293847	719283456	816273549	918243657	57
123456789	213465879	312475968	415263978	514283769	618293457	719243856	816273549	917253648	58
123456789	213465879	314256978	412375968	518273649	615293847	719263548	817243956	916283457	59
123456789	213465879	314256978	412395768	516283749	617243859	719263548	815293647	918273456	60
123456789	213465879	312475968	415263978	519273648	614293857	716283549	817253469	918243756	61
123456789	213465879	312475968	415263978	516293748	617253849	718243569	819273456	914283657	62
123456789	213465879	312475968	415263978	516273849	617293548	718253469	819243756	914283657	63
123456789	213465879	312475968	415263978	517283649	614293857	718243569	819273456	916253748	64
123456789	214365879	315264978	412395768	517283469	619253847	718293546	816243759	913274856	65
123456789	214365879	315264978	412395768	518243769	619283547	713294856	816273459	917253846	66
123456789	213465879	312475968	415263978	519273648	617253849	714283569	816293457	918243756	67
123456789	213465879	314256978	415273968	516293748	617283549	718243659	819263457	912384756	68
123456789	213465879	312475968	415263978	516273849	617293548	718253469	819243657	914283756	69
123456789	213465879	314256978	415273968	516283749	617293548	718243659	819263457	912384756	70
123456789	213465879	312495768	415263978	516293748	619283547	718243659	817253469	914273856	71
123456789	214365879	315264978	412385769	519243768	618273459	713294856	816253947	917283546	72
123456789	213465879	312495768	415263978	517293648	619283547	714253869	816273459	918243756	73
123456789	213465879	314256978	412375968	516283947	618293457	719243856	815273649	917263548	74
123456789	213465879	314256978	412375968	518273649	615293847	719263548	816243957	917283456	75
123456789	213465879	314256978	412375968	516273849	615283947	718293456	819243657	917263548	76
123456789	213465879	314256978	417283956	518263749	619243857	715293468	812364759	916273548	77
123456789	213465879	314256978	412395768	516293847	618243759	719283456	815273649	917263548	78
123456789	214365879	315264978	412375968	513284769	618243957	719253846	817293456	916273548	79
123456789	213465879	314256978	412375968	518263947	619243857	716293548	815273649	917283456	80
123456789	213465879	312475968	415263978	516273849	618293457	719253648	817243569	914283756	81
123456789	213465879	314256978	412395768	518263749	619273548	716243859	817293456	915283647	82
123456789	213465879	314256978	412395768	518293647	617243859	719283456	816273549	915263748	83
123456789	213465879	312495768	415283769	516243978	614273859	718293456	819263547	917253648	84
123456789	213465879	314256978	412395768	516293847	618243759	719263548	815273649	917283456	85
123456789	213465879	314256978	412395768	519283647	617243859	718293456	816273549	915263748	86
123456789	213465879	312475968	415263978	516283749	619273548	714253869	817293456	918243657	87
123456789	213465879	312475968	416253978	518273469	617293548	715283649	819243756	914263857	88
123456789	213465879	314256978	412395768	519273648	618243759	716283549	817293456	915263847	89
123456789	213465879	314256978	416273859	518293647	617283549	715243968	819263457	912374856	90
123456789	214365879	315264978	412395768	513284769	618243759	719253846	817293456	916273548	91
123456789	213465879	314256978	415273968	519263748	612384759	716283549	817293456	918243657	92
123456789	213465879	314256978	415273968	516293847	617283459	719263548	812364957	918243756	93
123456789	214365879	315264978	412395768	517243869	619253748	718293456	813274659	916283547	94
123456789	213465879	312475968	416253978	518243769	617283549	714293856	819263457	915273648	95
123456789	213465879	312475968	415263978	519273648	617283549	714253869	816293457	918243756	96
123456789	213465879	314256978	415273968	516293847	617283459	719263548	812374956	918243657	97
123456789	213465879	312475968	415263978	514283769	617293548	718253649	819273456	916243857	98
123456789	213465879	312495768	415263978	516293847	617283459	719253648	814273569	918243756	99
123456789	213465879	312475968	415263978	516293748	617283549	714253869	819273456	918243657	100
123456789	213465879	314256978	415273968	516293748	617283549	718263459	819243657	912384756	101
123456789	213465879	314295678	417253869	518273649	619283547	715263948	816243759	912345768	102
123456789	214365879	315284769	419253768	516243978	618293457	712384659	817263549	913274856	103
123456789	214365879	315284769	417293568	519263478	618243957	712384956	813274659	916253748	104
123456789	213465879	314256978	412395768	519263748	618273549	716283459	815293647	917243856	105
123456789	213465879	312475968	415263978	518243769	617283549	719253648	816293457	914273856	106
123456789	213465879	314256978	412375968	516283947	618293457	719243856	817263549	915273648	107
123456789	213465879	314256978	412395768	518263749	617243859	719283456	815293647	916273548	108
123456789	214365879	315284769	417293568	518273946	612345978	719243856	816253749	913264857	109
123456789	214365879	315264978	412395768	518273469	619283547	713294856	816243759	917253846	110
123456789	214365879	315284769	416293578	519243768	612384957	718263459	817253946	913274856	111
123456789	214365879	315274968	412385769	516293748	619283547	718243956	817263459	913254678	112
123456789	213465879	312475968	416253978	518273469	617293548	719243856	815263749	914283657	113
123456789	213465879	314256978	415293768	518263947	617283459	719243856	816273549	912364857	114
123456789	213465879	312475968	416283957	518273649	615293478	719263548	814253769	917243856	115
123456789	213465879	314256978	412395768	517283649	618243759	716293548	819273456	915263847	116
123456789	213465879	312475968	416283957	518273649	615293478	719243856	814253769	917263548	117
123456789	213465879	314275968	415283769	516243978	617253849	718293456	819263547	912364857	118
123456789	213465879	314256978	412395768	518273649	617293548	719283456	816243759	915263847	119
123456789	213465879	314265978	412385769	517243968	615293748	718253649	819273456	916283547	120
123456789	214365879	315264978	412375968	513284769	619273548	718293456	816243957	917253846	121
123456789	213465879	312475968	415263978	519273648	618293457	714283569	816253749	917243856	122
123456789	213465879	312475968	415263978	518273469	617283549	719243856	814293657	916253748	123
123456789	214365879	315264978	412395768	517283469	618243759	719253846	816293547	913274856	124

123456789	213465879	314256978	415273968	517293648	618243759	712384956	819263547	916283457	125
123456789	214365879	315284769	418293756	516273948	612345978	719253846	817263549	913245768	126
123456789	214365879	315284769	418293756	516273948	619243857	712354968	817263459	913254678	127
123456789	214365879	315264978	412395768	517283469	618293547	719253846	816243759	913274856	128
123456789	213465879	314256978	412395768	518293647	617283459	719243856	816273549	915263748	129
123456789	213465879	312475968	415263978	518243769	619273548	716253849	817293456	914283657	130
123456789	213465879	314256978	416273859	517293648	615283947	718263549	819243756	912345768	131
123456789	213465879	312475968	416293857	518273649	615243978	719283456	814253769	917263548	132
123456789	214365879	315284769	417293568	518273946	612345978	719243856	813264957	916253748	133
123456789	214365879	315264978	412395768	518273469	619253847	713294856	816243759	917283546	134
123456789	213465879	312495768	415283769	514263978	618273459	719243856	816293547	917253648	135
123456789	213465879	312495768	415283769	516243978	614273859	719263548	817293456	918253647	136
123456789	213465879	312475968	416253978	518273469	617293548	715263849	819243657	914283756	137
123456789	213465879	314256978	412395768	518263749	619273548	716243859	815293647	917283456	138
123456789	213465879	314256978	412395768	517263849	618243759	716293548	819273456	915283647	139
123456789	213465879	312475968	416253978	518243769	617283549	715293648	819273456	914263857	140
123456789	213465879	314256978	412395768	518293647	617283549	719243856	816273459	915263748	141
123456789	213465879	314256978	412395768	518273649	615293847	719283456	816243759	917263548	142
123456789	213465879	314256978	412375968	518273649	615283947	719263548	816293457	917243856	143
123456789	213465879	314256978	412395768	519263847	617293548	715283649	816273459	918243756	144
123456789	213465879	314256978	412395768	518273649	615293847	719263548	816243759	917283456	145
123456789	213465879	314256978	415293768	518263947	617243859	719283456	812364957	916273548	146
123456789	213465879	314265978	415273968	512374869	617283549	718293456	819243657	916253847	147
123456789	213465879	312495768	415283769	516243978	619273548	714263859	817293456	918253647	148
123456789	213465879	314256978	412395768	519283647	615293748	716243859	817263549	918273456	149
123456789	214365879	315274968	412385769	513294678	618243759	719263548	816253947	917283456	150
123456789	213465879	314256978	415273968	516293847	612374859	718263549	819243657	917283456	151
123456789	213465879	314256978	412395768	516293847	617283459	719263548	815273649	918243756	152
123456789	214365879	315264978	412395768	518243769	619253847	713294856	816273459	917283546	153
123456789	213465879	314256978	415273968	516293847	619283457	712364859	817263549	918243756	154
123456789	214365879	315284769	418293756	517263948	619243857	712354968	816273459	913254678	155
123456789	214365879	315264978	412375968	513284769	619273548	718253946	816293457	917243856	156
123456789	214365879	315264978	412385769	519243768	613284759	718293456	817253946	916273548	157
123456789	213465879	314256978	412395768	517283649	615293847	718263459	819243756	916273548	158
123456789	213465879	314265978	412395768	519273648	615293847	718243569	816253749	917283456	159
123456789	214365879	315264978	412385769	517243968	619283547	718293456	813274659	916253748	160
123456789	213465879	314265978	415273869	512374968	617293548	718243956	819253647	916283457	161
123456789	213465879	312495768	416253978	517243869	618273459	719263548	814293756	915283647	162
123456789	213465879	314256978	412375968	516273948	619243857	718293456	817263549	915283647	163
123456789	213465879	315264978	413295768	517243869	618273459	719283546	816253947	912374856	164
123456789	214365879	315294768	416273859	518243769	619283457	712394856	817263549	913254678	165
123456789	214365879	315264978	412395768	518243769	613284759	719253846	817293456	916273548	166
123456789	214365879	315264978	412375968	513284769	619243857	718253946	817293456	916273548	167
123456789	213465879	314256978	415273968	516293748	619283547	712384956	817243659	918263457	168
123456789	214365879	315264978	412385769	519243768	613284759	718253946	817293456	916273548	169
123456789	213465879	314256978	412375968	516283947	615273849	719263548	817293456	918243657	170
123456789	213465879	314256978	415273968	516293748	619283547	712384956	817263459	918243657	171
123456789	214365879	315264978	412375968	513274869	618243957	719283456	816293547	917253846	172
123456789	214365879	315264978	412375968	513284769	618293457	719253846	817243956	916273548	173
123456789	213465879	314256978	412395768	519283647	618273549	716243859	817293456	915263748	174
123456789	213465879	314256978	417293856	516283749	612394857	718243659	819263547	915273468	175
123456789	213465879	314256978	412375968	518273649	615283947	719263548	817293456	916243857	176
123456789	213465879	314265978	415273968	512374869	617283549	719243856	816293457	918253647	177
123456789	213465879	314256978	412395768	519263847	617283549	715293648	816273459	918243756	178
123456789	213465879	314256978	412395768	518263749	617293548	719243856	816273459	915283647	179
123456789	213465879	314256978	412395768	516293847	618243759	715283649	819273456	917263548	180
123456789	213465879	312475968	416253978	518273469	617283549	719243856	814293657	915263748	181
123456789	214365879	315294768	416273859	518243769	612394857	719283456	817263549	913254678	182
123456789	213465879	314256978	412375968	518263947	619283457	716293548	815273649	917243856	183
123456789	213465879	314256978	412395768	519273648	617283549	718293456	816243759	915263847	184
123456789	213465879	312475968	416253978	517283649	614293857	719263548	815273469	918243756	185
123456789	213465879	314256978	415273968	516293748	612384759	718263549	819243657	917283456	186
123456789	213465879	314256978	415273968	516293748	612384957	719283456	817243659	918263547	187
123456789	213465879	314256978	415293768	516273948	619283457	718263549	817243659	912384756	188
123456789	213465879	314275968	416293578	519263748	615283947	718253469	812364957	917243856	189
123456789	213465879	314265978	415293768	516273948	619283457	718253649	812354769	917243856	190
123456789	213465879	314256978	412395768	516293847	617283549	718243659	819273456	915263748	191
123456789	213465879	314256978	415293768	516273948	617283549	718243659	819263457	912384756	192
123456789	214365879	315264978	412395768	518243769	619253847	713284659	817293456	916273548	193
123456789	213465879	314256978	415273968	518293647	612374859	716283549	819263457	917243856	194
123456789	214365879	315264978	412395768	517283469	618293547	719243856	813274659	916253748	195
123456789	214365879	315294768	418253769	517263849	612394857	719283546	816273459	913245678	196
123456789	214365879	315274968	412385769	516293748	619283547	718263459	817253946	913245678	197
123456789	214365879	315264978	412375968	516273948	618293547	719253846	813245769	917283456	198
123456789	214365879	315274968	416253978	518293746	613284759	719263548	812345769	917243856	199
123456789	214365879	315284769	416253978	519243768	618293457	712384956	813274659	917263548	200
123456789	214365879	315264978	417253869	519283746	618243957	713294856	816273459	912354768	201
123456789	213465879	314265978	418293657	512384769	615283749	719253468	817243956	916273548	202
123456789	213465879	314265978	415293768	512384769	619283457	718253649	817243956	916273548	203
123456789	213465879	314265978	415293768	512384769	619273548	718243956	817253649	916283457	204
123456789	214365879	315264978	413285769	517243968	619253847	718293456	812374659	916273548	205
123456789	214365879	315294768	416253978	518243769	612384957	719263548	813274659	917283456	206
123456789	213465879	314256978	417283956	516293748	612384957	718243659	819263547	915273468	207
123456789	214365879	315264978	412385769	517293468	619283547	718243956	813274659	916253748	208
123456789	214365879	315264978	412385769	517243968	619253748	718293456	813274659	916283547	209
123456789	214365879	315264978	412375968	516273948	618293457	719243856	813254769	917283546	210
123456789	214365879	315264978	412385769	519243768	618273459	713294856	817253946	916283547	211
123456789	213465879	314256978	412395768	516293847	615283749	718243659	819273456	917263548	212
123456789	213465879	314256978	412395768	516293748	617243859	718263549	819273456	915283647	213

123456789	214365879	315274968	416253978	517283469	619243857	718293546	813264759	912374856	214
123456789	213465879	314256978	412395768	519283647	615273849	716293548	817263459	918243756	215
123456789	213465879	314256978	412375968	516273948	615293847	719283456	817263549	918243657	216
123456789	213465879	314256978	415273968	516293847	619283457	718243659	812374956	917263548	217
123456789	214365879	315264978	413295768	517283469	619273548	718243956	812374659	916253847	218
123456789	214365879	315284769	417293568	519263478	618243957	712384659	816253749	913274856	219
123456789	214365879	315294768	418253769	517263948	612384957	719283546	816273459	913245678	220
123456789	213465879	314256978	412375968	519263847	617293548	718243956	815273649	916283457	221
123456789	213465879	314256978	415273968	517283649	612384759	719263548	816293457	918243756	222
123456789	213465879	314256978	415293768	516273948	612384759	718263549	819243657	917283456	223
123456789	213465879	314256978	416273859	512374968	617293548	719283456	815263947	918243657	224
123456789	214365879	315274968	413285769	516243978	619253847	718293456	812374659	917263548	225
123456789	213465879	314256978	412375968	516293847	618243957	719263548	815273649	917283456	226
123456789	213465879	314256978	416293857	517243968	618273459	715283649	819263547	912374856	227
123456789	213465879	314256978	417293856	516273948	615283749	718243659	819263547	912345768	228
123456789	213465879	312495768	415283769	516243978	618293547	714263859	819273456	917253648	229
123456789	213465879	314256978	415293768	516273849	619283547	712394856	817243659	918263457	230
123456789	213465879	314256978	415273968	519263748	612384957	718243659	817293456	916283547	231
123456789	213465879	314256978	412395768	518263749	617283459	719243856	815293647	916273548	232
123456789	213465879	314256978	415273968	516293748	619283457	718243659	817263549	912384756	233
123456789	213465879	312495768	415283769	514263978	618273459	719253648	816293547	917243856	234
123456789	214365879	315284769	417293568	519263478	618253749	712384659	816243957	913274856	235
123456789	213465879	314265978	417283569	516273948	618293457	712384956	819253647	915243768	236
123456789	213465879	314275968	416253978	519263748	618293547	715283649	812345769	917243856	237
123456789	213465879	314265978	412395768	518273469	619253748	716283549	815293647	917243856	238
123456789	213465879	314256978	412395768	516283749	619273548	718243659	817293456	915263847	239
123456789	213465879	314265978	415293768	518273469	612394857	719243856	817253649	916283547	240
123456789	213465879	314265978	412385769	518293647	615273948	719243568	816253749	917283456	241
123456789	213465879	314256978	412375968	517263948	618273549	719283456	815293647	916243857	242
123456789	214365879	315284769	419263857	517243968	612345978	718293546	816253749	913274856	243
123456789	213465879	314256978	412375968	517293648	615283947	719243856	816273549	918263457	244
123456789	213465879	314256978	416283957	517293648	618273459	712384956	819263547	915243768	245
123456789	214365879	315264978	412395768	518293746	619283547	713254869	816273459	917243856	246
123456789	214365879	315284769	416253978	519243768	612384957	718293546	817263459	913274856	247
123456789	214365879	315264978	412395768	518273469	613284759	719243856	817293546	916253748	248
123456789	214365879	315264978	412385769	519243768	618253947	713294856	816273459	917283546	249
123456789	214365879	315264978	412385769	519243768	618253947	713284659	817293456	916273548	250
123456789	214365879	315274968	412385769	516293748	619283547	718263459	817243956	913254678	251
123456789	214365879	315264978	412395768	519273846	618293547	713254869	816243759	917283456	252
123456789	214365879	315284769	419263857	516293478	618243759	712354968	817253946	913274856	253
123456789	214365879	315264978	417253968	518293746	612384759	719283456	813245769	916273548	254
123456789	214365879	315284769	418263957	516293478	619253748	712354968	813274659	917243856	255
123456789	214365879	315264978	417253968	519273846	618243759	713294856	812354769	916283457	256
123456789	214365879	315274968	412385769	519263478	618293547	713284659	817243956	916253748	257
123456789	214365879	315264978	413285769	517293468	619273548	718243956	812374659	916253847	258
123456789	214365879	315284769	417293568	519273846	612345978	718243956	816253749	913264857	259
123456789	214365879	315274968	416253978	519283746	618293457	712354869	813264759	917243856	260
123456789	214365879	315284769	418293756	517263948	612345978	719253846	816273549	913245768	261
123456789	214365879	315264978	417253968	518293746	613284759	719243856	812345769	916273548	262
123456789	213465879	314256978	412395768	516293847	619273548	718243659	815263749	917283456	263
123456789	213465879	314256978	416273859	512374968	617293548	718243956	819263457	915283647	264
123456789	213465879	314256978	412375968	516273948	617283549	718293456	819243657	915263847	265
123456789	214365879	315264978	412375968	513284769	619273548	718243956	816293457	917253846	266
123456789	214365879	315264978	412385769	519273468	613284759	718243956	817293546	916253748	267
123456789	214365879	315264978	412395768	519283746	618273459	713254869	816293547	917243856	268
123456789	214365879	315284769	417293568	519273846	612345978	718243956	813264957	916253748	269
123456789	214365879	315264978	412395768	519273846	618243759	713254869	817293456	916283547	270
123456789	213465879	314256978	412395768	519283647	618273459	716293548	815263749	917243856	271
123456789	213465879	314256978	415273968	517293648	618243759	712384956	819263457	916283547	272
123456789	213465879	314256978	415273968	516293847	618243759	719283456	812364957	917263548	273
123456789	214365879	315264978	417253869	518273946	619283547	713294856	816243759	912345768	274
123456789	214365879	315264978	417283569	518273946	619253847	713294856	816243759	912345768	275
123456789	213465879	314275968	412395678	516283749	619243857	718253469	815293647	917263548	276
123456789	213465879	314265978	415293768	517283649	619273548	718243956	812345769	916253847	277
123456789	213465879	314256978	412395768	517293648	618243759	719283456	816273549	915263847	278
123456789	214365879	315264978	413295768	517243869	619283547	718253946	816273459	912374856	279
123456789	214365879	315284769	419253768	516293478	618243957	712384659	817263549	913274856	280
123456789	214365879	315274968	416253978	519283746	612384759	718293456	813245769	917263548	281
123456789	213465879	314265978	412395768	518273649	619283547	715243869	817293456	916253748	282
123456789	213465879	314275968	412385769	518293647	619253748	716283549	817243956	915263478	283
123456789	213465879	314256978	412395768	516273849	618243759	719283456	815293647	917263548	284
123456789	214365879	315264978	413295768	518273469	619253847	712394856	816243759	917283546	285
123456789	213465879	314256978	416273859	512374968	618293457	719263548	817243956	915283647	286
123456789	213465879	314256978	416273859	519243768	618293457	712394856	817263549	915283647	287
123456789	213465879	314256978	416273859	512374968	618243957	719263548	815293647	917283456	288
123456789	213465879	314256978	412375968	517293648	618273549	719283456	815263947	916243857	289
123456789	213465879	312495768	416273859	517293648	618253947	719283456	815243769	914263578	290
123456789	213465879	314295678	415273869	518263947	619283457	712354968	817243659	916253748	291
123456789	214365879	315264978	412375968	518273946	619283547	713254869	816293457	917243856	292
123456789	214365879	315264978	412395768	519283746	618293547	713254869	816273459	917243856	293
123456789	214365879	315284769	418293756	516273948	612354978	719253846	817263459	913245768	294
123456789	214365879	315274968	412385769	516293478	619253748	718243956	813264759	917283546	295
123456789	214365879	315294768	418253769	516273849	612394857	719283546	817263459	913245678	296
123456789	214365879	315264978	413285769	517243968	619253847	718293546	816273459	912374856	297
123456789	214365879	315264978	413295768	519273846	618243759	712354869	816253947	917283456	298
123456789	214365879	315274968	417253869	516293748	618243957	719283546	813264759	912345678	299
123456789	214365879	315264978	412395768	516293748	618273459	719243856	813254769	917283546	300
123456789	214365879	315264978	413285769	517293468	618253947	719243856	812374659	916273548	301
123456789	214365879	315264978	416273859	519283746	618253947	712354869	817293456	913245768	302

123456789	214365879	315264978	416273859	518293746	619283457	712354869	817243956	913254768	303
123456789	214365879	315284769	419263857	517293468	612354978	718253946	816243759	913274856	304
123456789	213465879	314256978	415293768	517283649	612384759	718243956	819263457	916273548	305
123456789	214365879	315264978	416283759	517243968	618293457	719253846	812354769	913274856	306
123456789	214365879	315274968	412385769	519263478	618253947	713294856	816243759	917283546	307
123456789	214365879	315274968	416293578	519283746	612394857	718263459	813254769	917243856	308
123456789	214365879	315264978	412395768	516293748	618273459	719283546	813254769	917243856	309
123456789	214365879	315264978	413295768	519283746	618253947	712354869	816273459	917243856	310
123456789	214365879	315284769	417293568	519263478	612384957	718243956	813274659	916253748	311
123456789	214365879	315264978	412375968	516273948	618293457	719283546	813254769	917243856	312
123456789	214365879	315294768	416253978	518243769	612384957	719283456	813274659	917263548	313
123456789	213465879	314256978	416283759	519263847	617293548	718243956	815273649	912345768	314
123456789	213465879	314275968	415283769	518293647	612354978	716253948	819263457	917243856	315
123456789	213465879	314256978	415293768	519263847	617283459	718243956	812364957	916273548	316
123456789	214365879	315264978	417253869	518273946	619283457	713294856	816243759	912354768	317
123456789	214365879	315264978	412385769	519273468	618253947	713294856	816243759	917283546	318
123456789	214365879	315284769	417293568	519263478	618243957	712384659	813274956	916253748	319
123456789	214365879	315264978	413285769	518293746	619253847	712345968	817243956	916273548	320
123456789	214365879	315264978	412385769	518273946	619283547	713245968	817293456	916253748	321
123456789	214365879	315284769	416293578	519243768	612384957	718253946	817263459	913274856	322
123456789	214365879	315264978	417283569	518293746	619243857	712394856	816273459	913254768	323
123456789	214365879	315274968	416253978	517283469	618293547	719243856	812374659	913264857	324
123456789	214365879	315284769	416253978	519243768	612384957	718263459	817293546	913274856	325
123456789	214365879	315274968	412385769	513294678	618243759	719283456	816253947	917263548	326
123456789	214365879	315284769	419263857	516293748	618273459	712354968	817253946	913245678	327
123456789	214365879	315264978	412375968	513274869	618253947	719283546	817293456	916243857	328
123456789	214365879	315274968	412385769	513294678	618253947	719283456	816243759	917263548	329
123456789	214365879	315274968	413285769	512394678	619253847	718293456	816243759	917263548	330
123456789	214365879	315264978	413285769	516293748	618273459	719243856	817253946	912354768	331
123456789	214365879	315284769	419263857	516243978	618253749	712345968	817293546	913274856	332
123456789	214365879	315264978	412385769	513294768	618243759	719283456	817253946	916273548	333
123456789	214365879	315264978	412385769	517293468	619283547	718253946	816243759	913274856	334
123456789	214365879	315274968	417253869	518263947	613294857	719283456	816243759	912354678	335
123456789	214365879	315264978	412385769	518293746	619273548	713245968	816253947	917283456	336
123456789	214365879	315264978	417253869	519283746	613294857	718243956	816273459	912354768	337
123456789	214365879	315264978	416273859	518293746	619283457	713254869	817243956	912354768	338
123456789	214365879	315264978	413285769	512394768	618273459	719243856	817293546	916253748	339
123456789	214365879	315284769	418263957	517293468	612354978	719243856	813274659	916253748	340
123456789	214365879	315284769	418293756	516273849	612345978	719263548	817253946	913245768	341
123456789	214365879	315274968	417253869	518263947	619283457	713294856	816243759	912354678	342
123456789	214365879	315284769	417253968	519263478	612384957	718293546	816243759	913274856	343
123456789	214365879	315264978	417253968	519283746	618273459	713294856	812354769	916243857	344
123456789	214365879	315284769	416253978	519243768	612384957	718293456	813274659	917263548	345
123456789	214365879	315284769	418293756	517243968	612345978	719253846	816273549	913264857	346
123456789	213465879	312495768	416253978	518293647	619273548	715243869	817263459	914283756	347
123456789	213465879	314275968	412385769	516243978	619283547	718253649	817293456	915263748	348
123456789	214365879	315264978	413285769	517243968	619273548	718293456	812374659	916253847	349
123456789	214365879	315274968	412385769	518293746	613245978	719283456	816253947	917263548	350
123456789	214365879	315264978	412375968	516273948	618293547	719283456	813245769	917253846	351
123456789	214365879	315284769	416273859	519243768	612394857	718263549	817293456	913254678	352
123456789	214365879	315274968	416283759	519263478	618243957	713294856	812354769	917253846	353
123456789	214365879	315264978	412385769	517243968	618293547	719283456	813274659	916253748	354
123456789	214365879	315264978	413295768	518273469	619283547	712394856	816243759	917253846	355
123456789	214365879	315284769	418273956	516293748	619243857	712345968	817263549	913254678	356
123456789	213465879	314275968	412385769	519243678	615283947	718263549	817293456	916253748	357
123456789	213465879	314256978	412395768	519263847	615283749	718243659	817293456	916273548	358
123456789	214365879	315284769	416253978	519243768	618293457	712384659	817263549	913274856	359
123456789	214365879	315264978	412385769	519283746	618253947	713245968	817293456	916273548	360
123456789	214365879	315264978	413295768	518273469	612384759	719283546	817243956	916253748	361
123456789	214365879	315284769	416253978	519243768	618293457	712384659	813274956	917263548	362
123456789	214365879	315264978	413295768	516273948	618243759	719253846	812354769	917283456	363
123456789	214365879	315264978	413295768	518273469	619283547	712384659	817243956	916253748	364
123456789	214365879	315264978	412385769	518273946	619253748	713245968	816293547	917283456	365
123456789	214365879	315264978	413285769	516293748	618273459	719253846	817243956	912354768	366
123456789	214365879	315264978	413295768	517243869	618253947	719283456	812374659	916273548	367
123456789	214365879	315274968	416283759	518263947	619243857	713254869	817293546	912345678	368
123456789	214365879	315264978	412385769	517293468	618253947	719283546	816243759	913274856	369
123456789	214365879	315264978	412385769	517293468	619253748	718243956	813274659	916283547	370
123456789	214365879	315274968	413285769	516243978	619253847	718263459	817293546	912374856	371
123456789	214365879	315264978	413285769	519243768	618253947	712384659	817293456	916273548	372
123456789	214365879	315284769	416273859	517243968	618293457	719263548	812374956	913254678	373
123456789	213465879	314275968	416293857	518243769	612354978	719283456	815263947	917253648	374
123456789	214365879	315264978	417253968	519273846	618243759	713294856	812345769	916283547	375
123456789	214365879	315274968	416253978	519263847	618243759	713294856	812345769	917283546	376
123456789	214365879	315264978	417253869	518273946	613294857	719283456	816243759	912354768	377
123456789	214365879	315284769	412395678	513274968	618243759	719253846	816293457	917263548	378
123456789	214365879	315274968	416253978	519283746	613294857	718263459	812354769	917243856	379
123456789	213465879	312475968	416253978	518243769	619273548	715283649	817293456	914263857	380
123456789	213465879	314275968	416253978	519263847	615293748	718243569	812364957	917283456	381
123456789	213465879	314275968	412395678	518293647	615283749	719263548	817253469	916243857	382
123456789	214365879	315264978	412385769	516273948	618243759	719283546	817293456	913254768	383
123456789	214365879	315264978	412385769	516293748	618273459	719283546	817243956	913254768	384
123456789	214365879	315264978	416283759	518273946	619243857	712354869	817293456	913254768	385
123456789	214365879	315264978	412385769	516273948	618243759	719283456	817293546	913254768	386
123456789	214365879	315274968	417263859	518243769	613294857	719283456	816253947	912354678	387
123456789	214365879	315284769	416253978	519243768	618273549	712384659	817293456	913264857	388
123456789	214365879	315264978	416283759	518273946	619253847	712354869	817293456	913245768	389
123456789	214365879	315274968	413285769	516293478	618253947	719263548	812374659	917243856	390
123456789	214365879	315274968	416253978	518293746	613284759	719243856	812345769	917263548	391

123456789	214365879	315264978	413285769	519273846	618293547	712345968	817243956	916253748	392
123456789	214365879	315264978	413285769	518273946	619253748	712345968	816293547	917243856	393
123456789	214365879	315274968	416283759	517263948	618293457	719253846	812354769	913245678	394
123456789	214365879	315274968	413285769	512394678	618293547	719243856	817263459	916253748	395
123456789	214365879	315274968	413285769	512394678	618243759	719263548	817293456	916253847	396

5.32 **Remark** See Remark VII.6.117 for a discussion of the invariants used to differentiate nonisomorphic 1-factorizations of K_{2n}.

5.33 **Remark** From Theorem 5.18, the existence of k pairwise orthogonal 1-factorizations of K_{2n} is equivalent to the existence of a Room k-cube of side $2n-1$ (see §VI.50). In particular, $\nu(2n-1)$ denotes the maximum number of pairwise orthogonal 1-factorizations of K_{2n}. Table VI.50.51 gives lower bounds on $\nu(n)$ for $n \leq 103$.

5.34 LB(n) denotes the number of 1-factorizations of a labeled $K_{n,n}$.

5.35 NB(n) denotes the number of pairwise nonisomorphic 1-factorizations of $K_{n,n}$.

5.36 **Remark** The number of latin squares of order n is $n!\,\mathrm{LB}(n)$, and NB(n) is greater than the number of main classes of latin squares of order n and smaller than the number of isotopy classes of latin squares of order n. It is in fact greater than half the latter number. Compare with Table III.1.16.

5.37 **Table** Some known values for the number of distinct and the number of nonisomorphic 1-factorizations of $K_{n,n}$ [684, 1573, 1579].

n	1	2	3	4	5	6	7	8
LB(n)	1	1	2	24	1344	1,128,960	12,198,297,600	2,697,818,265,354,240
NB(n)	1	1	1	2	2	17	324	842,227

Furthermore, $\mathrm{LB}(9) = 8! \cdot 377,597,570,964,258,816$;
$\mathrm{LB}(10) = 9! \cdot 7,580,721,483,160,132,811,489,280$; and
$\mathrm{LB}(11) = 10! \cdot 5,363,937,773,277,371,298,119,673,540,771,840$.

5.38 **Remark** In principle, formulae exist for the calculation of LB(n), but they are impractical for large n [686, 1579, 1894].

5.39 **Theorems**

1. $\mathrm{LB}(n) \geq (n!)^{2n-1}/n^{n^2}$;
2. $\mathrm{NB}(n) \geq (n!)^{2n-3}/(2n^{n^2})$;
3. $\lim_{n\to\infty}(\mathrm{LB}(n))^{1/n^2}/(e^{-2}n) = \lim_{n\to\infty}(\mathrm{NB}(n))^{1/n^2}/(e^{-2}n) = 1$. [2091]

5.40 **Remark** From Theorem 5.39(3), a weaker statement follows:

$$\lim_{n\to\infty}(\log(\mathrm{LB}(n))/(n^2\log n) = \lim_{n\to\infty}(\log \mathrm{NB}(n))/(n^2\log n) = 1.$$

5.41 **Remarks** MOLS correspond to pairwise orthogonal 1-factorizations of $K_{n,n}$, and hence, $N(n)$ (defined in §III.3) denotes the maximum number of pairwise orthogonal 1-factorizations of $K_{n,n}$. Bounds on $N(n)$ can be found in §III.3.4 and §III.3.6.

5.42 **Table** [1270, 1823, 1862] The number of nonisomorphic 1-factorizations of $r-$regular graphs of order $2n \leq 12$. N denotes the number of regular graphs while OF denotes the number of 1-factorizations (that is, the sum of the number of nonisomorphic 1-factorizations of each). When $r = 2n-1$, these values are in Table 5.26.

r	2	3	4	2	3	4	5	6	2	3	4	5	6	7	8
$2n$	4	6	6	8	8	8	8	8	10	10	10	10	10	10	10
N	1	2	1	3	6	6	3	1	5	21	60	60	21	5	1
OF	1	2	1	2	8	16	19	13	2	23	310	3,468	13,277	14,241	3,192

r	2	3	4	5	6	7	8	9	10
$2n$	12	12	12	12	12	12	12	12	12
N	9	94	1547	7,849	7,849	1547	94	9	1
OF	9	157	32,714	5,122,910	298,222,859	?	?	?	5,794,885,778

5.43 **Table** All nonisomorphic 2-factorizations of all regular graphs of even degree at least 4 and order at most 8. Each line is a 2-factorization; 2-factors are given by their cycles.

Graph	2-Factorizations
K_5	01234; 02413
$K_6 - \{03, 14, 25\}$	012 345; 042315 012354; 024315
$K_7 - \{01, 12, 23, 34, 45, 56, 60\}$	024 1536; 0314625 0241635; 0315264 0246135; 0362514
$K_7 - \{01, 12, 20, 34, 45, 56, 63\}$	0315 246; 0416 235 0314625; 0423516
K_7	012 3456; 0315 246; 0416 235 012 3456; 0314625; 0423516 0123456; 0241635; 0315264 0123456; 0246135; 0362514
$K_8 - \{01, 03, 04, 12, 15, 23, 26, 37, 45, 47, 56, 67\}$	0246 1357; 0527 1436 02417536; 0527 1346 02416357; 05271346 02461357; 05271436
$K_8 - \{01, 04, 07, 12, 15, 23, 26, 34, 37, 45, 56, 67\}$	02471635; 03146 257 0246 1357; 03614725 0253 1647; 05724136 02417536; 03164725
$K_8 - \{01, 02, 04, 12, 13, 23, 37, 45, 46, 56, 57, 67\}$	035 14726; 06342517 0347 1526; 0536 1427 03517426; 0527 1436 03471526; 05361427 03514726; 05243617
$K_8 - \{01, 02, 03, 12, 15, 26, 34, 37, 45, 46, 57, 67\}$	0417 2365; 05316 247 04163527; 056 13247 04136527; 05324716
$K_8 - \{01, 02, 03, 12, 13, 23, 45, 46, 47, 56, 57, 67\}$ $(= K_{4,4})$	0415 2637; 0617 2435 04152637 05342716

For the graph $K_8 - \{01, 02, 05, 13, 16, 23, 24, 34, 47, 56, 57, 67\}$ the 10 nonisomorphic 2-factorizations are

03627 145; 046 12537	03541726; 04637 125	03546 127; 04152637
03517264; 0637 1254	03721546; 0417 2536	03514627; 04521736
03526417; 04512736	03527146; 04512637	03546217; 04152736
03627154; 06412537		

For the graph $K_8 - \{01, 23, 45, 67\}$, the 49 nonisomorphic 2-factorizations are

02146 357; 034 15627; 05247 136	02146 357; 03615 247; 04317 256
02143657; 035 16247; 046 13725	02146 357; 03165 247; 04362517
0214 3657; 03461725; 06247 135	02146 357; 0347 1526; 04271365
02134657; 035 14726; 04251736	02134657; 035 16247; 04152736
02143657; 035 16427; 04731526	02143657; 03516274; 05246 137
02146 357; 03156247; 04361725	02146 357; 03174265; 04361527

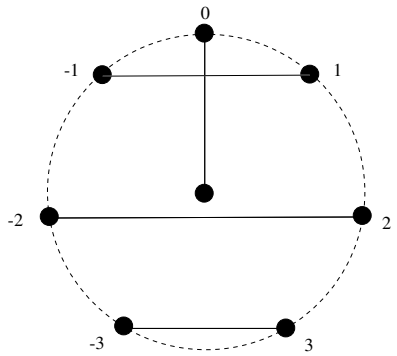
02146 357; 03472615; 04256317	02146 357; 03625174; 05613427
02146 357; 03651724; 05261347	0213 4657; 0415 2637; 0617 2435
0213 4657; 0416 2537; 0517 2436	0213 4657; 0426 1537; 0527 1436
0246 1357; 0365 1274; 0437 1526	02134657; 0374 1526; 0536 1427
0214 3657; 0346 1527; 05316247	02416537; 0364 1275; 0526 1347
0213 4657; 04152637; 05342716	0213 4657; 04162537; 05172436
0213 4657; 04261537; 05271436	02134657; 03514726; 0425 1637
02134657; 03614725; 0426 1537	0214 3657; 03461527; 05317426
02143657; 03164725; 0426 1537	02143657; 0374 1526; 05317246
02146375; 0347 1526; 04271356	02416357; 0374 1265; 05271346
0246 1357; 03651274; 05261437	02134657; 03516274; 05241736
02134657; 03517426; 04163725	02134657; 03526174; 05142736
02134657; 03615274; 05371426	02134657; 03627415; 04253716
02143657; 03152746; 04261735	02143657; 03517246; 04731625
02143657; 03517264; 05247316	02143657; 03517426; 04613725
02143657; 03526174; 05137246	02146357; 03165274; 05173426
02146357; 03427156; 04731625	02146357; 03715624; 05274316
02146375; 03165247; 04351726	02146375; 03516247; 04317256
02416537; 03462175; 04725136	

5.44 **Remark** [520] There are precisely 122 nonisomorphic 2-factorizations of K_9 with the property that each factor is a Hamilton cycle.

5.5 Some 1-Factorizations of Complete Graphs

5.45 **Construction** If $S = \{\{s_i, t_i\} : 1 \le i \le n-1\}$ is a starter in an abelian group G of order $2n-1$, then $\{\{\infty, g\} \cup (S+g) : g \in G\}$ are the edge-sets of a 1-factorization of K_{2n} (with vertex set $G \cup \{\infty\}$) (see §VI.55)

5.46 **Example** If S is the patterned starter $\{\{g, -g\} : g \in G \setminus \{0\}\}$ in the cyclic group of order $2n-1$, the resulting 1-factorization of K_{2n} is known as GK_{2n}. It can be obtained by rotating the diagram to the right (shown here for GK_8). In Table 5.30, factorization #6 is isomorphic to GK_8, and in Table 5.31, factorization #290 is isomorphic to GK_{10} (see §VI.55).



5.47 **Construction** Let E be an even starter (see §VI.55.5) written multiplicatively in an abelian group G of order $2n$. Label the vertices of K_{2n+2} by the elements of G and two infinity elements ∞_1 and ∞_2 and define $x\infty_1 = \infty_1$ and $x\infty_2 = \infty_2$ for all $x \in G$. Let $E^* = E \cup \{\{e, \infty_1\}, \{m_E, \infty_2\}\}$ and $Q^* = \{\{x, xg^*\} | x \in G\} \cup \{\{\infty_1, \infty_2\}\}$. Then $F_E = \{xE^* | x \in G\} \cup Q^*$ (where $xE^* = \{\{xa, xb\} | \{a, b\} \in E^*\}$ for $x \in G$) is a 1-factorization of K_{2n+2}.

5.48 **Construction**

1. For even n, a 1-factorization $\mathcal{F}$ of K_{2n} can be obtained by letting $\{F_1, \ldots, F_{n-1}\}$ and $\{G_1, \ldots, G_{n-1}\}$ be 1-factorizations of two disjoint K_ns, letting $\{H_1, \ldots, H_n\}$ be a 1-factorization of the $K_{n,n}$ with all edges joining a vertex of one K_n to a vertex of the other, and putting $\mathcal{F} = \{F_1 \cup G_1, \ldots, F_{n-1} \cup G_{n-1}, H_1, \ldots, H_n\}$.
2. For odd n there is a similar construction; a specific example is given in Construction 5.49.

5.49 Construction A 1-factorization of K_{2n} known as GA_{2n} (best known when n is odd):

***n* even.** Let $\{F_1, \ldots, F_{n-1}\}$ be a GK_n on the vertex set $C_1 \cup \{\infty_1\}$, where C_1 is the group with elements $1_1, \ldots, (n-1)_1$ and addition modulo $n-1$. Let $n_1 = \infty_1$ and choose notation such that the edge $i_1\infty_1$ is in F_i. Similarly, let $\{G_1, \ldots, G_{n-1}\}$ be a GK_n on $C_2 \cup \{\infty_2\}$, where $n_2 = \infty_2$ and the elements of C_2 are $1_2, \ldots, (n-1)_2$, and where the edge $i_2\infty_2$ is in G_i. Further, let $\{H_1, \ldots, H_n\}$ be the 1-factorization of $K_{n,n}$ where H_i has edge-set $\{j_1(j+i)_2 : 1 \le j \le n\}$, numbers reduced modulo n. Then GA_{2n} is the 1-factorization $\{F_1 \cup G_1, \ldots, F_{n-1} \cup G_{n-1}, H_1, \ldots, H_n\}$ of K_{2n}. In Table 5.30, factorization #2 is isomorphic to GA_8.

***n* odd.** Let $\{F_1, \ldots, F_n\}$ be a GK_{n+1} defined on the vertex set $\{1_1, \ldots, n_1\} \cup \{\infty_1\}$, addition modulo n, with the edge $i_1\infty_1$ in F_i, and let $\{G_1, \ldots, G_n\}$ be a GK_{n+1} on the vertex set $\{1_2, \ldots, n_2, \infty_2\}$ defined in the same way. Let $\{H_1, \ldots, H_n\}$ be as above. Then GA_{2n} is the 1-factorization on the vertex set $\{1_1, \ldots, n_1, 1_2, \ldots n_2\}$ with factors $(F_1 - 1_1\infty_1) \cup (G_1 - 1_2\infty_2) + 1_1 1_2$, $\ldots$, $(F_n - n_1\infty_1) \cup (G_n - n_2\infty_2) + n_1 n_2$, $H_1, \ldots, H_{n-1}$. In Table 5.31, factorization #396 is isomorphic to GA_{10}.

5.50 An *automorphism* of a factorization of a graph G is a mapping of the vertices of G to themselves that also maps factors to factors. The *automorphism group* of a factorization F is the group of all automorphisms of F. Any subgroup of the automorphism group is *a group of automorphisms* of the factorization.

5.51 A 1-factorization of K_{2n} is

1. *1-rotational* (or *vertex-1-rotational*, or *factor-cyclic*) if it has an automorphism that fixes one vertex and is cyclic on the remaining vertices;
2. *cyclic* if it has an automorphism that is cyclic on the vertices; and
3. *rigid* if the identity is the only automorphism.

5.52 Remark GK_{2n} is 1-rotational for all $n \ge 1$.

5.53 Theorem The order of the automorphism group for the 1-factorizations of K_8 (see Table 5.30).

Factorization Number	1	2	3	4	5	6
Group Order	1,344	64	16	96	24	42

5.54 Table The number $f_n(t)$ of nonisomorphic 1-factorizations of K_n for $n = 10$ and 12 with automorphism group of order t [715].

t	1	2	3	4	5	6	8	9	10	11
$f_{10}(t)$	298	69	5	7	0	6	3	1	0	0
$f_{12}(t)$	526,461,499	437,436	669	14,801	92	245	610	0	10	2

t	12	16	18	20	24	32	40	48	54	55	110	240	432	660
$f_{10}(t)$	2	1	1	0	0	0	1	0	1	0	0	0	1	0
$f_{12}(t)$	138	76	0	2	25	4	0	6	0	1	1	2	0	1

5.55 Theorems

1. If n is prime, GA_{2n} is cyclic.
2. [385] For any abelian group G of even order, $G \ne \mathbb{Z}_{2^t}, t \ge 3$, there exists a factorization of $K_{|G|}$ admitting G as a (necessarily sharply) vertex-transitive group of automorphisms—in particular, a cyclic 1-factorization of K_{2n} exists if and only if $2n \ne 2^t, t \ge 3$.
3. A rigid 1-factorization of K_{2n} exists if and only if $2n \ge 10$.

4. The number of nonisomorphic rigid 1-factorizations of K_{2n} tends to infinity with n.
5. If $2n-1 \geq 7$ is a prime, the automorphism group of GK_{2n} is the Frobenius group F_{2n-1} of order $(2n-1)(2n-2)$.
6. The order of the automorphism group of GK_{2n}, $2n \geq 8$, is $(2n-1)\phi(2n-1)$.
7. If $n \geq 5$ is a prime, the automorphism group of GA_{2n} is the group $F_n \times \mathbb{Z}_2$ of order $2n(n-1)$.

5.56 **Remark** It has been conjectured [385] that Theorem 5.55.2 holds without the assumption that the group be abelian. For some evidence for this, see [1805].

5.57 **Construction** Let S be a Steiner triple system of order v on the vertices of K_v, and for each vertex x take the 1-factor F_x of K_{v+1} with edge-set $\{\infty x\} \cup \{yz : \{x,y,z\} \in S\}$. This is a 1-factorization of K_{v+1} (a *Steiner 1-factorization*).

5.58 A *near 1-factorization* of a graph is a factorization where each factor has one vertex of degree zero, all other vertices having degree 1.

5.59 **Remark** A near 1-factorization of K_{2n-1} can be constructed from a 1-factorizations of K_{2n} by deleting a single vertex; thus they always exist.

5.60 **Theorem** [2166] Given any 1-factorization $\mathcal{F}$ of K_{2n}, there exists a further 1-factor F with the property that no two edges of F are in the same 1-factor of $\mathcal{F}$. Such a 1-factor is a *rainbow* 1-factor.

5.6 Perfect and Uniform 1-Factorizations

5.61 A 1-factorization $\mathcal{F} = \{F_1, \ldots, F_k\}$ of a graph G is *perfect* if $F_i \cup F_j$ is a Hamilton cycle of G for all $i \neq j$.

5.62 **Theorem** [2121] Perfect 1-factorizations of K_{2n} exist when $2n-1$ or n is a prime, and for the following values of $2n$: 16, 28, 36, 40, 50, 126, 170, 244, 344, 530, 730, 1332, 1370, 1850, 2198, 2810, 3126, 4490, 6860, 6890, 11450, 11882, 12168, 15626, 16808, 22202, 24390, 24650, 26570, 29792, 29930, 32042, 38810, 44522, 50654, 51530, 52442, 63002, 72362, 76730, 78126, 79508, 103824, 148878, 161052, 205380, 226982, 300764, 357912, 371294, 493040, 571788, 1092728, and 1225044.

5.63 **Remarks**

1. It is conjectured that a perfect 1-factorization of K_{2n} exists for all n.
2. When $2n-1$ is prime, GK_{2n} is perfect.
3. When n is a prime, GA_{2n} is perfect.
4. The smallest number $2n$ for which the existence of a perfect 1-factorization of K_{2n} is in doubt is 52.
5. All of the "sporadic" perfect 1-factorizations given in Theorem 5.62 for K_{2n} when $2n > 40$ were found via the use of starters in the finite field $\mathbb{F}_{2n-1}$.
6. The existence of a perfect 1-factorization of K_{2n} implies the existence of a symmetric latin square of order $2n-1$ with no proper subsquare (see Remark III.1.56).
7. The study of general graphs that possess a perfect 1-factorization was first done in [1327]. A graph is *strongly hamiltonian* if it possesses a perfect 1-factorization.

5.64 **Construction** Let $p \geq 11$ be a prime. Construction 5.47 applied to the even starter $S = \{\{x,y\} : x,y \in \mathbb{F}_p^* \setminus \{1, \frac{1}{2}\}, x+y=1\}$ in the multiplicative group $\mathbb{F}_p^*$ yields a (perfect) 1-factorization isomorphic to GK_{p+1}. If instead, the even starter $S' =$

$S \setminus \{\{-1,2\}\} \cup \{\{-1,\frac{1}{2}\}\}$ is used, a perfect 1-factorization *not* isomorphic to GK_{p+1} is obtained [365].

5.65 Theorem There is a cyclic perfect 1-factorization of K_{2n} if and only if n is prime.

5.66 Theorems In a series of four papers from 1986 to 1989, Ihrig studied the structure of the automorphism group of a perfect 1-factorization F of K_{2n}. Four of his theorems:

1. If $\alpha \in Aut(F)$, then α has order dividing either $2n, 2n-1$, or $2n-2$.
2. If F contains no automorphism of order 2 having fixed points, then $|Aut(F)| = a \times b \times c$ where $a|2n$, $b|(2n-1)$ and $c|(n-1)$. Also, c is odd and at least one of a, b, or c is 1.
3. $|Aut(F)|$ must divide one of $2n(2n-1)$, $2n(n-1)$ or $(2n-1)(2n-2)$.
4. If F has at least two automorphisms of order 2 having fixed points, then F is isomorphic to either GK_{2n} or GA_{2n}

5.67 $\mathrm{NP}(2n)$ is the number of pairwise nonisomorphic perfect 1-factorizations of K_{2n}.

5.68 Theorems

1. $\mathrm{NP}(p+1) \geq 2$ for all primes $p \geq 11$ (see Construction 5.64).
2. $\mathrm{NP}(4) = \mathrm{NP}(6) = \mathrm{NP}(8) = \mathrm{NP}(10) = 1$; $\mathrm{NP}(12) = 5$; $\mathrm{NP}(14) = 23$; (see [714])
3. The unique perfect 1-factorization of K_8 is #6 in Table 5.30.
4. The unique perfect 1-factorization of K_{10} is #396 in Table 5.31.
5. [1594] There are precisely 88 nonisomorphic perfect one factorizations of K_{16} with a nontrivial automorphism group. (None yet found with a trivial automorphism group).

5.69 Table Lower bounds for $\mathrm{NP}(2n)$, $16 \leq 2n \leq 40$ (see [1745]).

$2n$	16	18	20	22	24	26	28	30	32	34	36	38	40
$\mathrm{NP}(2n) \geq$	88	6	16	20	30	59	134	284	890	165	352	2	4

5.70 $\nu_P(2n)$ denotes the maximum number of pairwise orthogonal perfect 1-factorizations of K_{2n}.

5.71 Theorem $\nu_P(4) = \nu_P(6) = \nu_P(8) = \nu_P(10) = 1$.

5.72 Table Lower bounds for $\nu_P(2n)$ (see [1745]).

$2n$	12	18	20	22	24	26	28	30	32	34	36	38	44	48	54	60	68	72	80	84	126
$\nu_P(2n) \geq$	3	3	5	3	9	2	3	5	5	2	2	7	3	5	8	5	7	7	9	17	9

5.73 A 1-factorization $\mathcal{F} = \{F_1, \ldots, F_k\}$ of K_{2n} is *uniform* if $F_i \cup F_j$ is isomorphic to $F_k \cup F_\ell$ for all $i \neq j$ and $k \neq \ell$. $\mathcal{F}$ has *type* $(t_1, t_2, \ldots t_s)$ if $F_i \cup F_j$ is the disjoint union of cycles of lengths $t_1, t_2, \ldots t_s$.

5.74 Remark Any perfect 1-factorization of K_{2n} is uniform.

5.75 Theorems Other than perfect 1-factorizations, the following infinite classes of uniform 1-factorizations of K_{v+1} are known:

1. Type $(4, 4, \ldots, 4)$ if v is a power of 2 (the Steiner 1-factorization from the projective triple system of order $v-1$; see Constructions 5.57 and II.2.8);
2. Type $(4, 6, \ldots, 6)$ if v is a power of 3 (the Steiner 1-factorizations from a Hall triple system (§VI.28));
3. Type $(p+1, 2p, 2p, \ldots, 2p)$ if $v = p^k$ with $p > 2$ and $k > 1$; and
4. The 1-factorization generated by any S_a from Theorem VI.55.22 when $v \equiv 3 \pmod 4$ is a prime power (in general, the type is not known).

5.76 Theorem (see [1594]) If $\mathcal{F}$ is a uniform 1-factorization of K_{2n} with $2n \leq 16$, then $\mathcal{F}$ is one of the following: (1) a perfect 1-factorization, (2) type (4,4) (#1 in Table 5.30), (3) type (4,6) (#1 in Table 5.31), (4) type (6,6), or (5) type (4,4,4,4).

5.7 Maximal Sets of 1-Factors

5.77 Two s-factors are *compatible* (or *edge-disjoint*) if they contain no edge in common. If S is a set of pairwise compatible s-factors that cannot be extended to an s-factorization, then S is a *premature set* of s-factors. If there is no s-factor compatible with all the members of S, then S is *maximal*.

5.78 Theorem [609] If n is odd, then a maximal set of 1-factors in K_{2n} contains at least n 1-factors. If n is even, then a maximal set in K_{2n} contains at least $n+1$ 1-factors.

5.79 Theorem [609] If d is even and $d < n$ then K_{2n} contains a maximal set of $2n-d-1$ 1-factors.

5.80 Theorems

1. If there is a maximal set of k 1-factors in K_{2n}, and k is even, then $k \geq (4n+4)/3$.
2. [1796] There is a maximal set of k 1-factors in K_{2n} whenever $(4n+4)/3 \leq k \leq 2n-3$.

5.81 Theorem There is a premature set of k 1-factors in K_{2n} whenever k is even and $n < k < 2n-4$, or when $k = 2n-4$, $n \geq 5$ and n is odd.

5.82 Theorem For every order $2n$ greater than 8 there is a premature set of $2n-4$ 1-factors in K_{2n} that is not maximal.

5.83 Proposition The question of deciding whether a set S of 1-factors of a graph G is premature is NP-complete [522].

5.8 Some 2-Factorizations of Complete Graphs

5.84 Theorem For any $m \geq 3$, K_n has a 2-factorization where each factor consists of disjoint m-cycles if and only if m is odd and $n \equiv m \pmod{2m}$ (see §VI.12.3).

5.85 Remarks

1. The case $n = m$ of Theorem 5.84 states that for odd n, K_n has a *hamiltonian decomposition*.
2. The general problem of finding a factorization of K_{2n-1} into *given, isomorphic* 2-factors is known as the *Oberwolfach problem* (see §VI.12.3).

5.86 Theorem [1119] When n is even there exists a maximal set of k pairwise compatible 2-factors of K_n if and only if $k \in \{\lceil \frac{n-\sqrt{n}}{2} \rceil, \lceil \frac{n-\sqrt{n}}{2} + 1 \rceil, \ldots, \frac{n-2}{2}\}$. When n is odd, there exists a maximal set of k pairwise compatible 2-factors of K_n if and only if $k = (n-1)/2$.

5.87 Theorem [1119] There exists a maximal set of k pairwise compatible hamiltonian cycles in K_n if and only if $k \in \{\lfloor \frac{n+3}{4} \rfloor, \lfloor \frac{n+3}{4} + 1 \rfloor, \ldots, \lfloor \frac{n-1}{2} \rfloor\}$.

5.88 A *Kotzig factorization* of K_{2n-1} is a hamiltonian decomposition together with an orthogonal near 1-factorization.

5.89 Theorem For all $n \geq 2$, K_{2n-1} has a Kotzig factorization.

See Also

§II.7	An RBIBD(v, k, λ) is a $(k-1)$-factorization of λK_v.
§III.1	Latin squares are 1-factorizations of $K_{n,n}$.
§VI.12	Resolvable cycle systems are 2-factorizations of complete graphs. Oberwolfach designs are 2-factorizations of complete graphs.
§VI.24	Graph decompositions.
§VI.29	Howell designs are equivalent to orthogonal 1-factorizations of regular graphs.
§VI.50	Room squares (and Room d-cubes) are related to orthogonal 1-factorizations of K_{2n}.
§VI.55	Starters are used to construct 1-rotational 1-factorizations of K_{2n}.
[1271]	Contains the 1-factorizations of complete graphs up to order 10 in electronic form.
[2107]	A survey of 1-factorizations of complete graphs including most of the material of this chapter.
[2108]	A book on 1-factorizations of graphs.
[84]	A survey of orthogonal factorizations.
[725]	Contains, among many other subjects related to factorization, a fast algorithm for finding 1-factorizations of K_{2n}.
[299]	A monograph on general factorizations of graphs.
[1860]	A survey on perfect 1-factorizations of K_{2n}.
[1823, 1861]	Together enumerate all nonisomorphic 1-factorizations of simple graphs of order at most 10.
[81]	Hamiltonian decompositions in general.
[2122]	Discusses the automorphism group of 1-factorizations obtained from the K-construction.

References Cited: [81, 84, 105, 293, 299, 365, 385, 415, 494, 520, 522, 609, 684, 686, 714, 715, 725, 860, 1100, 1102, 1119, 1123, 1270, 1271, 1327, 1573, 1579, 1594, 1745, 1796, 1805, 1823, 1860, 1861, 1862, 1894, 2091, 2107, 2108, 2121, 2122, 2125, 2166]

6 Computational Methods in Design Theory

Peter B. Gibbons
Patric R. J. Östergård

6.1 Introduction

6.1 **Remarks** For more than three decades now the computer has been an indispensable ally in the search for combinatorial designs of many types. The use of clever computational techniques has not only enabled many existence and enumeration questions to be settled, but has also allowed larger classes of designs to be analyzed, often leading to the formulation of conjectures that have been subsequently proved for infinite families of designs. This interaction between the fields of design theory and computer science is genuinely two-way, with designs having a variety of applications in computer science (see [546, 584] and many of the chapters in this present volume).

This chapter outlines some of the main computational methods that have been successful in solving existence and enumeration problems in combinatorial design theory. Issues related to the validation of search results are also discussed.

6.2 **Remarks** The construction of a combinatorial design can be formulated as a special type of combinatorial optimization problem. With such problems there is a set Σ of *feasible solutions* (or states) together with an objective function (*cost*) $c(S)$ associated with each feasible solution S. The task is to find an optimal solution, corresponding to a feasible solution with overall (global) minimum cost. In some cases the objective function can be viewed as being a *profit*, in which case the task is to find a feasible solution with maximum profit. Throughout this chapter we cast optimization problems and methods in terms of minimizing cost. One feature of design problems, unlike many other optimization problems, is that an optimal solution is easily certified as being optimal. On the other hand, approximations to an optimal solution are generally of little use in design construction.

6.3 **Remarks** Optimization problems, even with similar descriptions, can vary greatly in difficulty. For example, a minimum spanning tree of a weighted graph $G = (V, E)$ can be found by a worst-case $O(|E| + |V| \log |V|)$-time greedy algorithm, whereas the current best algorithm for obtaining a minimum cost Hamilton circuit of G runs in worst-case exponential time. The current belief is that the second problem (the well-known traveling salesman problem, TSP) cannot be solved by a worst-case polynomial-time algorithm. This belief is based on knowledge of the theory of *NP-completeness* (see [860]). The set *NP* consists of all decision problems (problems with *yes/no* answers) where a *yes*-instance can be verified in polynomial time. A problem A is *NP-hard* if a worst-case polynomial-time algorithm for A can be used to produce a worst-case polynomial-time algorithm for any problem $B \in NP$ (that is, B is reducible to A). An *NP*-hard problem in *NP* is *NP-complete*. The enormous amount of effort spent in attempting, without success, to find polynomial-time algorithms for a large variety of *NP*-hard problems (of which TSP is one) has led many researchers to conjecture that such algorithms do not exist.

6.4 **Table** The following design construction and analysis problems have been shown to be *NP*-hard.

NP-Hard Problems	References
Completion of partial latin squares	Colbourn [522]
Deciding the decomposability of Kirkman systems	Colbourn and Colbourn [536]
Embedding of partial triple systems	Colbourn [521]
Is a block design t-colorable for all $t \geq 9$?	Colbourn et al. [539]
Is a partial SQS 2-colorable?	Colbourn et al. [540]
Is a partial STS t-colorable for any fixed $t \geq 3$?	Colbourn et al. [539]
Is an STS 14-colorable?	Phelps and Rödl [1738]
Is an STS k-chromatic?	Phelps and Rödl [1738]
Orienting triple systems	Colbourn [523]

6.5 **Remarks** Most design construction problems appear to be *intractable*, that is, they appear not to have polynomial-time algorithms. This extends to enumeration, where in general it is unlikely that a block design enumeration can be performed by a *polynomial delay* algorithm, that is, an algorithm that constructs the first design in polynomial-time, and each of the remaining designs within polynomial time of completing the previous design. It is therefore acceptable to use methods that run in worst-case exponential time. The goal of the methods described is to minimize the average time

for a single design construction or overall time for a complete enumeration of a family of designs.

6.6 Remark Problems related to enumeration can also be difficult to solve. For example, block design isomorphism is graph isomorphism-complete, implying that a polynomial-time algorithm is unlikely to exist. The related problem of determining the automorphism group of a design is also difficult, because computing the automorphism group order for a graph is graph isomorphism-complete (see [1536]).

6.7 Table Major topics covered in this chapter.

Topic	Section
Complexity issues	6.1
Backtracking	6.2
Orderly algorithms	6.2
Isomorph rejection	6.2
A_{tk}-matrices and basis reduction	6.3
Tactical decompositions	6.3
Counting techniques	6.4
Local search	6.5
Hill-climbing	6.5
Simulated annealing	6.5
Tabu search	6.5
Evolutionary algorithms	6.5
Validating computational results	6.6
Isomorphism	6.7
Group maintenance	6.7
Distributed search	6.7
Fine tuning	6.7

6.2 Exhaustive Search

6.8 Remarks Backtracking is one of the oldest methods for design construction. It works by building up feasible solutions one step at a time, exhaustively covering all possibilities in a systematic fashion. It is guaranteed to find an optimal solution if allowed to run long enough (which, of course, is the catch). However, by the use of clever pruning techniques, such as rejecting partial feasible solutions that either cannot lead to a complete solution or are equivalent to partial solutions already generated earlier in the search, substantial improvements in execution time can be made.

Backtracking may be formulated as a search of the product space $X^n = X_1 \times X_2 \times \cdots \times X_n$, where the component selection spaces X_1, X_2, ..., X_n may or may not be the same. For any $i \in \{1, 2, \ldots, n\}$, define a boolean-valued *feasibility property* $\Pi_i : X_1 \times X_2 \times \cdots \times X_i \to \{\texttt{true}, \texttt{false}\}$ such that for any $(x_1, x_2, \ldots, x_i) \in X_1 \times X_2 \times \cdots \times X_i$, the implication

$$\Pi_i(x_1, x_2, \ldots, x_i) = \texttt{true} \Rightarrow \forall\ 1 \le j < i,\ \Pi_j(x_1, x_2, \ldots, x_j) = \texttt{true}$$

holds. With an *existence* problem, the task is to find one $(x_1, x_2, \ldots, x_n)$ such that $\Pi_n(x_1, x_2, \ldots, x_n) = \texttt{true}$; with an *enumeration* (or *classification*) problem, the task is to find all such $(x_1, x_2, \ldots, x_n)$; and with a *counting* problem, the task is to find the number of such solutions.

The key to the efficiency of a backtrack algorithm lies in the choice of an appropriate feasibility property. Suppose that a partial solution $(x_1, x_2, \ldots, x_i)$ has been constructed, for some $1 \le i < n$, and that $\Pi_i(x_1, x_2, \ldots, x_i) = \texttt{false}$. Since

$\Pi_j(x_1, x_2, \ldots, x_j) =$ `false` for all $j > i$, there is no point in extending this partial solution, and so in one stroke $|X_{i+1}| \times |X_{i+2}| \times \cdots \times |X_n|$ infeasible solutions are eliminated.

In general, only n, X_1, X_2, ..., X_n and Π_n are given (but see Remarks 6.11), and the task is to find appropriate feasibility properties $\Pi_1, \Pi_2, \ldots, \Pi_{n-1}$. Good feasibility properties should often have $\Pi_i(x_1, x_2, \ldots, x_i) =$ `false`, particularly for small values of i.

6.9 Algorithm The general backtrack algorithm for enumeration is

{Find all $(x_1, x_2, \ldots, x_n) \in X_1 \times X_2 \times \cdots \times X_n$ such that $\Pi_n(x_1, x_2, \ldots, x_n) =$ `true`}
procedure Search($(x_1, x_2, \ldots, x_i), i$);
begin
if $i = n$
then record $(x_1, x_2, \ldots, x_n)$ as a solution
else for each $x_{i+1} \in X_{i+1}$ **do**
if $\Pi_{i+1}(x_1, x_2, \ldots, x_{i+1})$
then Search($(x_1, x_2, \ldots, x_{i+1}), i+1$)
end
Search($(), 0$)

An execution of this algorithm can be modelled by a *search tree*, with one node for each recursive call.

6.10 Remarks The backtrack algorithm can be used to construct BIBDs in either a block-by-block or a point-by-point manner. Let the point set of a BIBD(v, b, r, k, λ) be $P = \{1, 2, \ldots, v\}$, and let $B = \{1, 2, \ldots, b\}$ be the set of indices of the blocks. In this chapter the designs are not necessarily simple, so that collections of blocks should be viewed as multisets.

In a block-by-block construction, define $X_i = \{S \subseteq P : |S| = k\}$ for $1 \le i \le b$, and let the feasibility property be

$$\Pi_i(x_1, x_2, \ldots, x_i) = |\{x_j : \{c, d\} \subseteq x_j,\ j \le i\}| \le \lambda \ \forall\ \ \{c, d\} \subseteq P, c \ne d.$$

Moreover, to avoid duplication of work, assume that $x_i \le x_j$ when $i < j$, for some total order (such as lexicographic) defined on the subsets.

In a point-by-point, construction one determines, for each point i, $1 \le i \le v$, the set of blocks containing i. So, in terms of the backtracking framework, $X_i = \{S \subseteq B : |S| = r\}$ and the feasibility property is

$$\Pi_i(x_1, x_2, \ldots, x_i) = |\{\{j, i\} : |x_j \cap x_i| \ne \lambda,\ j < i\}| = 0,$$

assuming, for efficiency reasons, that $x_i < x_j$ when $i < j$. For an introduction to general incidence structure construction methods see [696, 1271, 1360].

6.11 Remarks In constructing BIBDs in a block-by-block manner, the feasibility property in Remarks 6.10 is generally bad when $\lambda > 1$. For $\lambda = 1$, one may use the fact that every pair of distinct points must occur in exactly one block of a completed design, and define $X_i = \{S \subseteq P : |S| = k,\ \{e, f\} \subseteq S\}$, where the pair $\{e, f\} \not\subseteq x_j\ \forall\ j < i$ is fixed using some heuristic that aims to optimize the performance of the algorithm. (In this case the blocks are not necessarily constructed in lexicographical order.) A promising heuristic is to minimize $|X_i|$. This *minimum degree heuristic* has been used to great effect in the construction of many types of combinatorial designs, including Steiner triple systems (see Example 6.14) and cyclic Steiner quadruple systems (see [538]). The definition of X_i also shows that a component selection space may depend on the current partial solution.

6.12 Remarks The block-by-block approach in Remarks 6.10 leads to instances of the *exact cover problem*, where one is given a set S of elements and a collection $\mathcal{S}$ of subsets of

S, and the problem is to find one or all partitions of S using sets from $\mathcal{S}$. Backtrack search using the minimum degree heuristic and a dedicated data structure produces a state-of-the-art algorithm for many such instances (see [1315]).

The point-by-point approach in Remarks 6.10, on the other hand, can be viewed as a problem of finding cliques in graphs. In this setting, since X_i does not depend on i, a graph can be constructed with one vertex for each element of X_i and with edges between vertices whose corresponding sets intersect in exactly λ elements. Then the cliques of size v, which are maximum cliques if they exist, are in one-to-one correspondence with the complete solutions of the search problem.

6.13 Remarks The implementation of strong feasibility conditions can considerably reduce the size of the search tree traversed by the algorithm. To cite a simple example, when incidence matrices are built up point by point, one may prune the search if one block contains more than k points.

Proper feasibility conditions are often problem-dependent and the value of mathematics in saving computing time cannot be overstated. For example, in searching for resolutions of BIBDs, Morales and Velarde [1632] precompute possible intersection patterns between the parallel classes and use this information to effectively guide the search and prune the tree. Another example is Dinitz and Stinson's search [723] for perfect 1-factorizations of K_{n+1}. They constructed starters by the use of cosets in the multiplicative group of $\mathbb{F}_n$ (n a prime power). Search feasibility was achieved by a theorem that allowed them to check only a few (fewer than eight) pairs for hamiltonicity to deduce that all pairs formed hamiltonian circuits (see §VII.5.6).

There is also a great variety of problem-independent techniques for improving on the general backtrack algorithm. Such techniques have been thoroughly studied in the field of constraint programming. Here there is room for only a glimpse of some of these. Whereas the minimum degree heuristic allows a choice based on local information, one may instead make a choice based on looking ahead at the implications of the alternative choices. Gibbons and Mathon [902] have found that in signing GDDs such *look-ahead* techniques are useful, particularly if the check is "turned on" only at some of the levels of the search tree. (Backtrack search with some of the studied look-ahead techniques is subtly different from general backtrack search.)

The technique of *branch and bound* is a variation of backtracking that has been successful in solving optimization problems. With this method, given a partial solution $(x_1, x_2, \ldots, x_i)$, where $i < n$, one calculates a *lower bound* $B(x_1, x_2, \ldots, x_i)$ on the cost of any solution obtained by extending $(x_1, x_2, \ldots, x_i)$. If this bound is at least as high as the cost of the best solution found so far, then the partial solution can immediately be rejected as any extension cannot provide a better solution. Look-ahead techniques can further be used to direct the search towards solutions with good cost. Whenever a search or optimization problem can be formulated as an instance of integer linear programming, a particular bound for a branch and bound approach is obtained by solving the linear programming relaxation. Margot [1522] studies enumeration of covering designs in this setting.

6.14 Example Kaski and Östergård [1268] devised a backtracking method to enumerate the $11,084,874,829$ nonisomorphic Steiner triple systems of order 19 (BIBD$(19, 3, 1)$s). The approach consists of the following three main parts:

1. Enumerating particular partial STS(19) (sets of blocks);
2. Completing the partial STS(19) using the approach of Remarks 6.11; and
3. Rejecting some of the STS(19) obtained so that exactly one object from each isomorphism class remains.

6.15 The *seeds* of an enumeration of objects are partial objects that form the starting point for completing the search.

6.16 **Remarks** As mentioned in Remarks 6.8, for efficiency reasons, partial solutions (objects) should be rejected if they are equivalent (isomorphic) to solutions (objects) encountered earlier in the search. However, such a test is often rather expensive compared with the other computations in the search. In these situations, it is advisable to carry out exhaustive tests only up to a certain level of the search tree (the level corresponding to the seeds) and from then on to perform only partial isomorph rejection checks, or no such checks at all. It is desirable that the seeds be rather large partial objects, yet small in number. A good sign is when many of these objects have only trivial automorphisms.

For STS(v), where blocks cannot intersect in more than one point, the seeds can be defined as sets of blocks of size 3, out of a v-set V of points, consisting of one block and the $3(r-1)$ blocks that intersect that block in one point. For STS(19) the seeds contain as many as 25 out of a total of 57 blocks. There are several ways of viewing such seeds. One may think of constructing a Steiner triple system by completing one point at a time, with the seeds having three points completed. An alternative way of looking at them is to ignore the three points of the first block and to consider only the remaining $v-3$ points. If one forms a graph with one vertex for each of these points and one edge for each occurrence of a point pair in a block, then the seeds correspond to three edge-disjoint 1-factors of K_{v-3}, the complete graph of order $v-3$ (or, alternatively, a 1-factorization of a 3-regular graph of order $v-3$). A set of i edge-disjoint 1-factors is a *partial* 1-factorization of rank i.

6.17 **Example** The unique seed for an STS(7) and the two seeds for an STS(9). (In these matrices the columns correspond to vertices and the rows to 1-factors. For each 1-factor, the edges consist of pairs of vertices with the same number.)

0011	001122	001122
0101	010212	010212
0110	012021	012120

6.18 **Remark** For STS(19) there are 14,648 seeds.

6.19 **Remarks** The general backtrack algorithm can be tuned to search for seeds for an STS(v). To enumerate all nonisomorphic seeds, *isomorph rejection* is introduced by strengthening the feasibility properties so as to reject partial seeds that are isomorphic to partial seeds that have been generated earlier in the search. More specifically, one tries to extend a partial seed if and only if it is the lexicographically lowest (or *canonical*) representative of its isomorphism class. Some details of how this is done are now provided.

An enumeration of seeds can be obtained by constructing one 1-factor at a time in the framework of 1-factorizations of a complete graph. An ordering of objects with an increasing amount of structure—edges, 1-factors, and partial 1-factorizations—is first defined. The vertices of a graph of order n are numbered $0, 1, \ldots, n-1$.

1. An edge e is written as an ordered pair (i, j) with $0 \le i < j \le n-1$. For any two edges $e = (i, j)$ and $e' = (i', j')$, define $e < e'$ if either $i < i'$ or $i = i'$ and $j < j'$.
2. A 1-factor f is written as an ordered list of edges $f = (e_1, e_2, \ldots)$ where $e_i < e_j$ whenever $i < j$. For two 1-factors $f = (e_1, e_2, \ldots)$ and $f' = (e'_1, e'_2, \ldots)$, define $f < f'$ if there exists a k such that $e_l = e'_l$ for all $l < k$, and $e_k < e'_k$.

3. For a partial 1-factorization $F = (f_1, f_2, \ldots)$, it is required that $f_i < f_j$ whenever $i < j$. For two partial 1-factorizations $F = (f_1, f_2, \ldots)$ and $F' = (f'_1, f'_2, \ldots)$, define $F < F'$ if there exists some k such that $f_l = f'_l$ for all $l < k$, and $f_k < f'_k$.

The automorphism group of the complete graph K_n is S_n, the symmetric group on n elements. Thus given a partial 1-factorization F, one can rename the n points using a permutation $\alpha \in S_n$, and obtain another partial 1-factorization of the same graph, denoted F^α. Then F is *canonical* if $F \leq F^\alpha$ for all permutations $\alpha \in S_n$. A canonical object forms a complete invariant for the objects in its isomorphism class and can thereby be used to decide whether two objects are isomorphic. Unfortunately, transforming an object into canonical form is generally a hard problem.

6.20 Proposition If two distinct partial 1-factorizations are both canonical, then they are nonisomorphic. If a partial 1-factorization $F_i = (f_1, f_2, \ldots, f_i)$ is canonical, then $F_j = (f_1, f_2, \ldots, f_j)$, for $1 \leq j \leq i$, is also canonical. If a partial 1-factorization F is not canonical, then a partial 1-factorization extended from F is also not canonical.

6.21 Remark Utilizing Proposition 6.20, the backtrack search can now be altered so that, on each level, partial 1-factorizations that are not canonical are rejected. A backtrack search that uses such an isomorph rejection technique is an *orderly algorithm* [808, 1784].

6.22 Proposition A partial 1-factorization of rank i of K_n is equivalent to an $(i, n, i-1; n/2)$ equireplicate error-correcting code, that is, one having an even distribution of the coordinate values in every coordinate.

6.23 Remarks Isomorph rejection must also be carried out among the Steiner triple systems obtained by completing the seeds. Unfortunately, orderly algorithms that are based on testing whether objects are in canonical form tend to become expensive when the sizes of the objects grow. Instead one may use an isomorph-rejection framework developed by McKay [1571], where canonicity of an augmentation rather than of the object itself is tested.

Isomorphic copies of a (complete or partial) object may appear in several nodes of a search tree (that is, may be constructed in several ways). In the *canonical augmentation* framework exactly one of the possible parents of an object is defined to be the right one. Every object that passes this canonical augmentation test and has the same parent object should be compared pairwise in a second test. However, the automorphisms of the parent may commonly be utilized in deciding whether an object should be accepted (thereby replacing the second test). In particular, all objects that pass the canonical augmentation test and whose parent has no nontrivial automorphisms are accepted.

6.24 Remarks Within a complete STS(v) reside b subobjects, some isomorphic and each consisting of one of the blocks together with the blocks that intersect it in one point. These objects are isomorphic to the seeds defined in Remarks 6.16. For the canonical augmentation test, one of these should be defined to be the designated parent in the search. The observation that there is a one-to-one correspondence between these seed objects and the blocks of the completed STS(v) makes it possible to consider a designated block instead.

The designated block can be defined to be the first block in a given ordering of blocks that should not depend on the labeling of the STS. If the STS has nontrivial automorphisms, some of the blocks are indistinguishable (as they lie in the same orbit of blocks of the automorphism group) so that the test should rather be based on whether the block lies in the first orbit in an ordering of orbits. For example, after encoding the incidence matrix as a Levi graph, the program `nauty` can produce a

desired ordering (see §6.7).

The canonical augmentation test can be sped up with the help of *invariants*. The number of Pasch configurations (see Example 6.116) in which a block lies does not depend on the labeling and this value can be taken into account in forming an ordering of the (orbits of) blocks. If one requires that the designated block be the one occurring in the largest number of Pasch configurations, then complete objects that fail the test can be rather quickly detected even without having to call `nauty`. Further speed-up of the enumeration of STS(19) can be achieved by considering the block intersection graph (see Remarks 6.108) rather than the Levi graph of the complete design.

6.25 Remarks The described algorithm generates one representative of each isomorphism class and therefore employs a *total isomorph rejection* strategy. Sometimes it is not possible to use the full automorphism group at intermediate levels (due to its size or difficulty of calculation). Using subgroups results in a *partial isomorph rejection* scheme, allowing the possibility of generating solutions that are isomorphic. In an enumeration, total isomorph rejection must always be employed among the complete objects. Isomorph rejection is also important in an existence search since isomorphic partial solutions that cannot lead to complete solutions are culled out in the search process.

6.26 Remark Dinitz, Garnick, and McKay [715] enumerated the $526,915,620$ nonisomorphic 1-factorizations of K_{12} via an orderly algorithm. By viewing a 1-factorization of K_{2n} as a 3-GDD of type $(2n-1)^1 1^{2n}$, an approach analogous to the one for Steiner triple systems can also be employed [1270].

6.27 Remarks Arguably the most famous backtracking search conducted to date was that by Lam, Thiel, and Swiercz [1378] in 1989 to show that a projective plane of order 10 (see §VII.2) does not exist. Their search took approximately 800 days of CPU time on a VAX-11/780 plus about $3,000$ hours on a supercomputer, the CRAY-1S.

The method relies on results obtained from studying the binary error-correcting code (see §VII.1) associated with a putative projective plane of order 10. Let A be the line-point incidence matrix of such a plane, and let S be the vector space generated by the rows of A over $\mathbb{F}_2$. A vector in S is a *codeword*, and the number of ones is its *weight*. The *weight enumerator* of S is defined to be $\sum_{i=0}^{111} w_i x^i$, where w_i is the number of codewords of weight i. Each codeword of weight i corresponds to a configuration with i points.

The weight enumerator of S is uniquely determined by the values of w_{12}, w_{15}, and w_{16}. By 1985, Lam and others had shown that these three values were all zero, allowing them to compute the weight enumerator and, in particular, to show that if a projective plane of order 10 exists, then its code must contain $24,675$ codewords of weight 19. Therefore, 19-point starting configurations were used as the basis for the search. For further details, see [1378] or the survey in Chapter 12 of [1271].

Despite the care taken in this search, the time is approaching when an independent verification of this result is warranted. Given the huge improvements in computing power over the past decades, this should be a less daunting task.

6.28 Table Further examples of the application of backtracking to existence and enumeration problems.

Configurations	References
Association schemes	Degraer and Coolsaet [664]
Balanced incomplete block designs	Lam et al. [1372]
Balanced tournament designs	Dinitz and Dinitz [711]
Bhaskar Rao designs	Gibbons and Mathon [899]
Biplanes	Salwach and Mezzaroba [1838]

Covering designs	Applegate, Rains, and Sloane [106]
Group divisible designs	Gibbons and Mathon [902]
Hadamard matrices	Kharaghani and Tayfeh-Rezaie [1287]
Linear spaces	Betten and Betten [227]
Mendelsohn triple systems	Denny and Mathon [697]
Perfect 1-factorizations	Dinitz and Garnick [714]
Projective planes	Gibbons and Mathon [902]
Resolutions of designs	Kaski and Östergård [1265]
Steiner systems	Spence [1945]
Strong starters	Kocay, Stinson, and Vanstone [1318]
Symmetric designs	Spence [1941]
t-designs	McKay and Radziszowski [1574]

6.3 Restrictive Search Assuming Automorphisms

6.29 **Remark** Various specialized techniques have been successful in constructing large designs by assuming an underlying group structure for the target design. The most important of these techniques are discussed in this section. The methods in §6.5 also examine only part of the search space, but differ from the methods of this section in that they cannot be extended to an exhaustive search of the whole space.

6.30 Given a t-(v,k,λ) design $(V,\mathcal{B})$, let V_h $(0<h<v)$ be the set of all h-subsets of V. Let $V_t=\{x_1,x_2,\ldots,x_m\}$ and $V_k=\{y_1,y_2,\ldots,y_n\}$, where $m=\binom{v}{t}$ and $n=\binom{v}{k}$. The A_{tk}-matrix $A_{tk}=(a_{ij})$ is the $m\times n$ (0,1)-matrix where $a_{ij}=1$ if and only if $x_i\subseteq y_j$.

6.31 **Proposition** A t-(v,k,λ) design exists if and only if there is a solution z to the matrix equation $A_{tk}z=\lambda J$, a Diophantine linear system of equations, where z is an n-dimensional vector with nonnegative integer entries, and J is the m-dimensional all-ones vector.

6.32 **Remark** A solution, in theory, can be obtained using integer programming techniques. For most designs of interest, however, A_{tk} is prohibitively large. To reduce the size, one assumes the action of a group G on the set V.

6.33 Let ρ_t and ρ_k be the number of orbits under the induced action of a group G on V_t and V_k, respectively. Denote by $A_{tk}(G)=(a_{ij})$ a $\rho_t\times\rho_k$ matrix where a_{ij} is the number of k-sets in the jth orbit of V_k containing a representative t-set in the ith orbit of V_t. $A_{tk}(G)$ can be obtained from A_{tk} by adding the columns in each orbit of V_k and keeping one representative row from each orbit of V_t.

6.34 **Proposition** A t-design with G as a subgroup of its automorphism group exists if and only if there is a solution z to the matrix equation $A_{tk}(G)z=\lambda J$, where z is a ρ_k-dimensional vector with nonnegative integer entries, and J is the ρ_t-dimensional all-ones vector.

6.35 **Remarks** Kramer and Mesner [1343] first suggested using the A_{tk}-matrix equation to find t-designs. Since then the method has led directly to the discovery of many new t-designs (see Remarks 6.45).

To use this equation to find a t-design effectively, three problems must be solved:

1. Find a group G that is likely to be a subgroup of the automorphism group of some design with the given parameters;
2. Find an efficient algorithm for constructing the $A_{tk}(G)$-matrix; and

3. Find an effective procedure for solving the equation $A_{tk}(G)z = \lambda J$.

Groups that have been used to solve Problem 1 are in particular various kinds of linear groups, including ASL, PGL, PΓL, PSL, and PΣL. See VII.9.2 and [599] for useful collections of permutation groups. There is a trade-off relating to the size of the group used. The larger the group, the greater the achieved "fusion" of the t-sets and k-sets into a smaller number of (larger) orbits. This reduces the size of the matrix A_{tk} and hence the size of the equation $A_{tk}(G)z = \lambda J$ to be solved. On the other hand, existence is less likely because one is fusing larger segments that must fit precisely to form the design. Put another way, smaller groups are more likely to be subgroups of the automorphism group of the putative design.

The efficient computation of A_{tk} (Problem 2) is achieved by solving two subproblems:

2.1. Design an algorithm and a data structure for computing and representing G-orbits of V_k and V_t.

2.2. Develop a method to decide which G-orbit of V_k contains a given orbit of V_t.

Algorithms for solving Problem 2 are described in Chapter 6 of Kreher and Stinson [1360]. For computing orbit representatives, an orderly algorithm (see Remark 6.21) can be employed. Consider the action of G on the set $V = \{1, 2, \ldots, n\}$, with the usual lexicographical ordering on V. Define the orbit representative for any subset S of V as the lexicographically first subset in the orbit of S, and construct the following data structure inductively. At level 0 take the empty set. For $m \geq 0$, the orbit representatives of V_m are extended in all possible ways by adding one element and removing sets that are not lexicographically minimal under the action of G. The remaining subsets form orbit representatives for V_{m+1}. (It turns out that, when adding elements to a set S, it suffices to consider elements that are greater than all elements of S.)

For small groups, the outlined approach for solving Problem 2 is straightforward and fast, but for large groups more advanced group-theoretic methods are indispensable. See [1399] for examples of such techniques. There are several approaches for solving Problem 3; some of the most useful are now discussed.

6.36 Example (Kreher and Radziszowski [1353]) Suppose that $(V = \{1, 2, 3, 4, 5, 6, 7\}, \mathcal{B})$, a 2-$(7, 3, 1)$ design, is to be constructed, with a subgroup $G = \langle (145)(276), (26)(45) \rangle \cong S_3$ of its automorphism group. Then $A_{23}(G)$ is the following matrix:

	123 347 136 356 357 234		125 147 146 456 157 245		127 467 167 256 257 246					
		124 457 156		126 247 567		134 345 135	137 346 235		236 237 367	
								145		267
{12 47 16 56 57 24}	1	1	1	1	1	0	0	0	0	0
{13 34 35}	2	0	0	0	0	2	1	0	0	0
{14 45 15}	0	1	2	0	0	1	0	1	0	0
{17 46 25}	0	0	2	0	2	0	1	0	0	0
{23 37 36}	2	0	0	0	0	0	1	0	2	0
{26 27 67}	0	0	0	1	2	0	0	0	1	1

The vector $z = [0, 1, 0, 0, 0, 0, 1, 0, 0, 1]^T$ gives a solution to the equation $A_{tk}(G)z = \lambda J$, and thus yields a 2-$(7, 3, 1)$ design with $B = \{124, 457, 156, 137, 346, 235, 267\}$ and G a subgroup of its automorphism group.

6.37 Remark If $\lambda = 1$, then $A_{tk}(G)z = \lambda J$ leads to instances of the exact cover problem (Remarks 6.12).

6.38 Remark Solving $A_{tk}(G)z = \lambda J$ is greatly facilitated if one considers (0,1)-vector solutions only. Such solutions correspond to *simple* designs, and consequently, virtually all work in this area is focused on simple designs.

6.39 Remarks A basic backtracking approach may be taken for solving $A_{tk}(G)z = \lambda J$ with $X_i = \{a_1, a_2, \ldots\}$, where a_i is the ith column of $A_{tk}(G)$, and the feasibility property

$$\Pi_i(x_1, x_2, \ldots, x_i) = \sum_{j=1}^{i} x_j \leq \lambda J.$$

One way of improving this approach is to modify X_i so that it contains only columns with a positive element in a given row where $\lambda J - \sum_{j=1}^{i-1} x_j$ is also positive. (This approach can be used for finding both the (0,1)-vector solutions and the solutions with positive integer entries.)

Various pruning strategies in solving diophantine linear systems of equations with a backtracking approach have been proposed [903, 1539, 1622].

6.40 Remark The computation can be further reduced by noticing that, considering $A_{tk}(G)$, the normalizer $N(G)$ moves the orbits of k-sets (resp. t-sets) among themselves. Consequently there is an induced group action of $N_{S_n}(G)$ on a solution z. By considering only one representative from each $N(G)$-orbit of orbits of k-sets in the first level of the search tree, the search can be cut down by a factor of at most $|N(G)|$.

6.41 Remarks A useful algorithm for solving general instances of $A_{tk}(G)z = \lambda J$ is the *basis reduction* method introduced by Lenstra, Lenstra, and Lovász [1424], and first applied to designs by Kreher and Radziszowski [1353]. They noted that if z is a (0,1)-vector solution to this system of equations, then $[z, E]^T$ is a vector in the integer lattice L spanned by the columns of the matrix

$$B = \begin{bmatrix} I_n & 0 \\ A_{tk}(G) & -\lambda J \end{bmatrix},$$

where E is the m-dimensional all-zero vector. That is, $[z, E]^T$ is a linear combination of the columns of B, satisfying

$$\begin{bmatrix} z \\ E \end{bmatrix} = B \begin{bmatrix} a_1 \\ \vdots \\ a_{n+1} \end{bmatrix},$$

where $a_1, a_2, \ldots, a_{n+1}$ are integers.

Kreher and Radziszowski noticed that integer solutions z to $A_{tk}(G)z = \lambda J$ are often short vectors in L. Their algorithm therefore searches for a reduced basis for L all of whose vectors are as short as possible. The three techniques used are

1. An $O(n^4)$ algorithm, $\mathbf{L}^3$ (or LLL), due to Lenstra, Lenstra, and Lovász [1424], for producing a reduced basis with short vectors from a given ordered basis. When the number of rows of $A_{tk}(G)$ is $m = 1$, solving the equation $A_{tk}(G)z = \lambda J$ reduces to solving the subset sum problem; the application of $\mathbf{L}^3$ to this problem is described in [1769]. If $m > 1$, further reduction techniques are necessary.
2. An $O(n^2)$ *weight reduction* algorithm is used to produce a basis with shorter vectors.
3. A *size reduction* algorithm is used to produce a basis with a smaller number of vectors.

6.42 Algorithm Basis reduction algorithm of Kreher and Radziszowski [1353].

Input basis B in the form specified in Remark 6.41;
$B := \mathbf{L}^3(B)$;
$B :=$ Size-Reduction(B);
currentWeight $:= \sum_{b \in B} \| b \|^2$, where $\| \cdot \|$ denotes ordinary euclidean length;
repeat
  oldWeight := *currentWeight*;
  $B :=$ Weight-Reduction(B);
  Sort the vectors in B into order of nondecreasing euclidean norm;
  $B := \mathbf{L}^3(B)$;
  currentWeight $:= \sum_{b \in B} \| b \|^2$
until *currentWeight* = *oldWeight* **or** a solution is found

This algorithm always halts in polynomial time, but does not always find a solution when one exists. For more recent applications of (variants of) the basis reduction algorithm to the construction of designs, see [235, 2124].

6.43 Remarks If one aims at an enumeration of objects with the prescribed group G as a subgroup of the automorphism group, then one faces the problem of carrying out isomorph rejection among the designs corresponding to the solutions of the linear system of equations. Various group-theoretical tools are of great help in solving this problem. For (large) groups G with certain properties there is no need for isomorph rejection as all designs obtained are nonisomorphic (see, for example, [1401] for details).

6.44 Remarks DISCRETA [241] (`http://www.mathe2.uni-bayreuth.de/discreta`) is a publicly available software package that incorporates all three parts of the aforementioned approach (and much more). It has an extensive library of various types of groups, computes the A_{tk}-matrix, and solves the system of linear equations. Furthermore, all parts have been implemented with state-of-the-art algorithms. DISCRETA is useful both for getting acquainted with the concepts discussed here through experimentation as well as for serious research on this topic.

6.45 Table Some examples of t-designs found by the use of A_{tk}-matrices:

t-(v, k, λ)	References	Year
5-$(13, 6, 4)$	Kreher and Radziszowski [1352]	1986
5-$(17, 8, 80)$	Kramer [1333]	1975
5-$(33, 6, 42)$	Magliveras and Leavitt [1508]	1984
5-$(36, 6, 1)$	Betten, Laue, and Wassermann [240]	1999
5-$(108, 6, 1)$	Grannell and Griggs [941]	1994
5-$(132, 6, 1)$	Grannell, Griggs, and Mathon [943]	1993
6-$(14, 7, 4)$	Kreher and Radziszowski [1352]	1986
6-$(28, 8, 42)$	Schmalz [1848]	1993
6-$(33, 8, 36)$	Magliveras and Leavitt [1508]	1984
7-$(33, 8, 10)$	Betten et al. [235]	1995
8-$(31, 10, 93)$	Betten et al. [236]	1998
9-$(28, 14, 3204)$	Laue [1401]	2001

6.46 Remark The use of a prescribed subgroup of the automorphism group to cut down the search space in the context of A_{tk}-matrices is computationally feasible only if the size of the matrix is manageable. In some cases, when the approach of using A_{tk}-matrices is not applicable (for example, with cases involving a small group, a small number of blocks, and large blocks), the following alternative approach can be taken.

6.47 Let G be a subgroup of automorphisms of a t-(v, k, λ) design $D = (V, \mathcal{B})$. Let $V_1, V_2, \ldots, V_m$ and $B_1, B_2, \ldots, B_n$ be the point and block orbits respectively of D under the action of G. A *tactical decomposition* of D with respect to G is an $m \times n$ matrix $T(G) = (t_{ij})$ where t_{ij} is the number of elements from V_i contained in a block from B_j.

6.48 Remarks A search for a design with a subgroup G of automorphism group now proceeds in two stages. In the first stage, possible tactical decompositions of D are generated. In some cases, for large designs, a group action may be imposed on T itself, thus inserting another stage. In the second stage, a set of *base blocks* is constructed for the design conforming to the prescribed tactical decomposition. Rather than checking the occurrence of pairs within blocks, one checks that all *pure* differences (corresponding to points from the same point orbit) and all *mixed* differences (corresponding to points from different point orbits) are covered by base blocks the correct number of times. If a backtrack search is used during this stage, the group of T can be used for partial isomorph rejection. The full design can be obtained by applying the group G to the set of base blocks.

6.49 Example Tactical decomposition is used by Topalova [2065] to enumerate the symmetric 2-$(69, 17, 4)$ designs with automorphisms of order 13.

6.4 Counting Techniques

6.50 Remarks An exhaustive enumeration of nonisomorphic combinatorial objects naturally gives their count as a by-product, and for many classes of objects, this is in fact the fastest counting technique. At the other extreme, the very simplest combinatorial objects—permutations and integer partitions, to mention just two examples—can be counted by a known formula or a simple algorithm. In between, there are objects that, with the current knowledge, require some computational effort for counting, but still less than an exhaustive enumeration.

6.51 Example Combinatorial objects whose exact number can be calculated analytically include nonisomorphic graphs (Remark VII.4.5), nonisomorphic cubic graphs (Remarks VII.4.17), nonisomorphic multigraphs and digraphs (Remark VII.4.37), as well as distinct latin squares (Theorem III.1.19).

6.52 Remark From an enumeration of nonisomorphic objects, the total number of labeled objects is obtained by the Orbit-Stabilizer Theorem (Proposition VII.9.23).

6.53 Remark Occasionally, counting the labeled objects is easier than counting the nonisomorphic objects. In such cases, one may get a count for the nonisomorphic objects by counting (possibly via an enumeration) the nonisomorphic objects that have nontrivial automorphisms and then calculating the number of nonisomorphic objects with a trivial full automorphism group (such objects are *rigid*) via the Orbit-Stabilizer Theorem. Latin squares, to be discussed next, form one such class of objects.

6.54 Remark Analytical methods for counting the number of distinct latin squares (Theorem III.1.19) are of little use in practice. The approach described here has been used to count the number of reduced latin squares of side up to 11 [1579].

6.55 Given a $k \times n$ latin rectangle L, a bipartite graph $G(L)$ is defined on vertex set $C \cup S$, with one vertex in C for each column in L, one vertex in S for each symbol in $\{1, 2, \ldots n\}$, and one edge for each tile of the rectangle (joining the corresponding vertices in C and S).

6.56 **Remark** The graph $G(L)$ is k-regular.

6.57 Let $m(G)$ be the number of 1-factorizations of a k-regular bipartite graph G on $C \cup S$. Let $\mathcal{G}(k,n)$ denote a complete set of nonisomorphic bipartite k-regular graphs on $C \cup S$. (In determining automorphisms and isomorphisms of such graphs, exchanging the sets C and S is allowed.)

6.58 **Theorem** The number of reduced latin squares of side n is

$$2nk!(n-k)! \sum_{G \in \mathcal{G}(k,n)} m(G)m(\bar{G})|\mathrm{Aut}(G)|^{-1},$$

where $\bar{G}$ is the complement in $K_{n,n}$ of G and k is an arbitrary integer in the range $0 \le k \le n$.

6.59 **Remarks** By Theorem 6.58 the problem of counting latin squares is now transformed into that of enumerating k-regular bipartite graphs and counting the number of 1-factorizations of the enumerated graphs. In determining the number of 1-factorizations of $G \in \mathcal{G}(k,n)$ with $k \ge 1$, one can use the fact that

$$m(G) = \sum_F m(G-F),$$

where the sum is over all 1-factors F of G that include an arbitrary prescribed edge e.

6.60 **Remark** The main practical difficulty in this approach is that of handling an enormous amount of data (large integers). The number of reduced latin squares of side 11 can be obtained using 2 years of CPU time on 1 GHz Pentium computers. This can be improved by one order of magnitude if the computers possess an extensive amount of memory (several GBs) [1579].

6.61 **Remark** 1-factorizations of complete graphs form a class of objects for which the known algorithms for counting labeled objects are faster than those for enumerating the nonisomorphic objects (see [715]).

6.62 **Remarks** Methods for tabulating existence results are also important in design theory. An example is the algorithm used to construct Table III.3.87 of values of $N(n)$. It constructs many new values of $N(n)$ without ever constructing any explicit latin squares. The algorithm is supplied, as input, every known general theorem dealing with the construction of MOLS. It then generates new orders recursively, while maintaining a database of values of $N(n)$. For a detailed discussion, see [543].

6.5 Nonexhaustive Search

6.63 **Remark** Nonexhaustive search techniques can be used to construct designs in situations where one expects that many solutions exist. As they do not guarantee to cover the entire search space, they cannot be used to provide a complete enumeration of a design family. In particular, nonexhaustive methods cannot establish nonexistence results. *Local search* forms the basis for most nonexhaustive search methods.

6.64 Define, for each feasible solution $S \in \Sigma$, a set $T(S)$ of transformations (or *moves*), each of which can be used to change S into another feasible solution S'. The set of solutions that can be reached from S by applying a transformation from $T(S)$ is the *neighborhood* $N(S)$ of S. S is a *local minimum* if $c(S) \le c(S')$ for all $S' \in N(S)$. A *local search* algorithm repeatedly moves from the current solution S to a neighboring solution S' and sets $S := S'$ until some stopping condition is met.

▷ **Hill-Climbing**

6.65 **Remark** *Hill-climbing* (or *iterative improvement*) is a variant of local search in which S' is selected from $N(S)$ such that $c(S') \leq c(S)$. Although contrary to the notion of "climbing", hill-climbing is presented in the context of a minimization problem to be consistent with the presentation of other probabilistic methods, such as simulated annealing.

6.66 **Algorithm** General hill-climbing algorithm.

```
Generate an initial feasible solution S;
while S is not a local minimum do
begin
    Choose any S' ∈ N(S) such that c(S') ≤ c(S);
    S := S'
end
```

6.67 **Remark** With designs, a feasible solution is often defined to be a partially completed design D, and the associated cost $c(D)$ to be the number of blocks needed to complete the partial design. The neighborhood $N(D)$ of D is the set of designs obtainable from D by altering and/or adding a small number of blocks. Unlike general optimization problems, an approximation to an optimal solution does not suffice. Only a complete design, which corresponds to a feasible solution with cost 0, is useful.

6.68 **Algorithm** Hill-climbing algorithm for designs.

```
Generate an initial partial design D;
tries := 0;
while tries < maxTries and c(D) > 0 do
begin
    tries := tries +1;
    Select a D' ∈ N(D) such that c(D') ≤ c(D);
    if c(D') < c(D)
    then tries := 0;
    D := D'
end
```

The value of *maxTries* is a "threshold" value specifying how many consecutive moves to feasible solutions with the same cost ("sideways" moves) are allowed before abandoning the search.

6.69 **Remarks** There are useful cost functions other than the number of remaining blocks. For example, a feasible solution could be an assignment of points to blocks in a less restrictive manner than for a valid block design. The cost function could then be a count of the number of violations that must be removed in order to make a valid design. Other interesting ideas for cost functions come from Eslami and Khosrovshahi [791] who consider feasible solutions to be collections of blocks in which all pairs are covered exactly λ times, but with some blocks occurring a negative number of times. A number of cost functions are possible, one being the number of blocks with negative multiplicities. The transition function consists of adding trades, and the hill-climbing objective is to produce a collection of blocks with 0 cost.

6.70 **Remarks** It may be difficult to select a $D' \in N(D)$ such that $c(D') \leq c(D)$. One approach may be to first choose a $D' \in N(D)$ randomly and then check whether $c(D') \leq c(D)$. If this approach is taken, the algorithm must abandon the current construction and start again with a new initial partial design once the number of attempts at finding a D' such that $c(D') \leq c(D)$ exceeds a (second) specified threshold

value. In cases where finding an optimal solution is not guaranteed, a third threshold value is needed to specify the number of restarts that the algorithm permits before completely abandoning the search. The choice of suitable threshold values, cost functions and transformation functions are critical in obtaining good performance from a hill-climbing algorithm.

6.71 Algorithm Stinson's algorithm [1964] for constructing an STS(v).

$D := \emptyset$;
$c(D) := v(v-1)/6$;
while $c(D) > 0$ **do**
begin
  Pick a random (live) element x appearing $< (v-1)/2$ times in D;
  Pick random (live) pairs $\{x, y\}$, $\{x, z\}$ not covered by blocks in D;
  if there is a block $\{y, z, w\} \in D$ (for some w)
  then begin
    $D := D \setminus \{y, z, w\}$;
    $c(D) := c(D) + 1$
  end;
  $D := D \cup \{x, y, z\}$;
  $c(D) := c(D) - 1$
end

In the general hill-climbing algorithm (Algorithm 6.68), finding an $S' \in N(S)$ such that $c(S') \leq c(S)$ may involve a search of the neighborhood $N(S)$. In Stinson's implementation for STS(v) no such search is required.

6.72 Remarks None of the three threshold parameters are needed in Stinson's algorithm for finding Steiner triple systems (Algorithm 6.71). Although one can identify theoretical situations where this algorithm can get stuck, the algorithm seldom encounters these situations in practice and, from empirical evidence, constructs a Steiner triple system in $\Theta(v^2 \log v)$ time, on average. For example, an STS(943) containing 148,051 blocks can be constructed in less than 3 seconds on a 2.8 GHz Dell 2550 server. The algorithm can be adapted to construct an STS with a specified automorphism group structure or one that satisfies other restrictions (see [901]).

6.73 Remark The first successful use of hill-climbing in design theory was an algorithm by Dinitz and Stinson [720] in 1981 to find strong starters.

6.74 Table Some examples of the successful application of hill-climbing for design construction.

Configurations	References
Enclosings of triple systems	Bigelow and Colbourn [267]
Howell designs	Dinitz and Lamken [717]
Leaves of partial triple systems	Colbourn and Mathon [568]
One-factorizations	Seah and Stinson [1863]
Orthogonal STSs	Dinitz, Dukes, and Ling [712]
PBDs with block sizes 3 and 4	Colbourn, Rosa, and Stinson [579]
Quadrilateral-free STSs	Griggs and Murphy [969]
Room frames	Dinitz and Stinson [726]
Room squares	Dinitz and Stinson [722]
Sequencing groups	Anderson [88]
Skolem sequences	Eldin, Shalaby, and Al-Thukair [778]

▷ Simulated Annealing

6.75 Remark *Simulated annealing* is an extension of hill-climbing in which uphill moves are allowed in a controlled fashion. The aim is to reduce the chance of the search becoming trapped in a local minimum.

6.76 Remarks Annealing, in condensed matter physics, refers to a thermal process for obtaining low energy states of a solid in a heat bath. In this process, the solid is first heated to melting temperature and then slowly cooled until the low-energy ground state is reached. If the initial temperature is not sufficiently high or the cooling is carried out too quickly, then the solid freezes into a meta-stable state rather than the ground state. The converse of annealing is quenching, where the temperature of the heat bath is instantaneously lowered, resulting in a meta-stable state.

The physical annealing process can be modeled successfully by using computer simulation methods. In one of these approaches, Metropolis et al. [1595] introduced a simple Monte Carlo algorithm that generates a sequence of states in the solid in the following way. Given a current state i of the solid, characterized by the positions of its particles, with energy E_i, a subsequent state j, with energy E_j, is generated by applying a small distortion to the current state, for example, by the displacement of a particle. If the energy difference, $E_j - E_i$, is ≤ 0, then the state j is accepted as the new current state. If the difference is greater than 0, then the state j is accepted with probability $e^{(E_i - E_j)/k_B T}$ where T denotes the temperature of the heat bath and k_B is a physical constant known as the Boltzmann constant. This acceptance rule is known as the Metropolis criterion and the associated algorithm is known as the Metropolis algorithm.

If the lowering of the temperature is done sufficiently slowly, the solid can reach thermal equilibrium at each temperature. In the Metropolis algorithm this is achieved by generating a large number of transitions at a given temperature value. In thermal equilibrium the probability of occurrence of a solid being in a state i with energy E_i at temperature T is given by the Boltzmann distribution $P_T\{X = i\} = e^{(-E_i/k_B T)}/Z(T)$, where X is a stochastic variable denoting the current state of the solid. $Z(T)$ is the partition function defined as $Z(T) = \Sigma\, e^{-E_j/k_B T}$, where the summation extends over all possible states.

6.77 Table The following correspondences demonstrate an analogy between the physical annealing process and the task of solving combinatorial optimization problems.

Physical Process	Optimization Problem
States of solid	Feasible solutions
Energy of state	Cost of feasible solution
Melting point state	Randomly generated feasible solution
Slight distortion of state	Elementary change to feasible solution
Temperature of heat bath	Control parameter T

6.78 Remarks The simulated annealing algorithm is an iteration of the Metropolis algorithm, executed with decreasing values of the control parameter. Initially the control parameter is given a large value, and starting with an initial randomly chosen feasible solution, a sequence (or Markov chain) of trials is generated. In each trial, a configuration j is generated randomly from the neighborhood of the current configuration i. Denoting $f(j) - f(i)$ by Δ, the probability of configuration j being the next configuration in the sequence is 1 if $\Delta_{ij} \leq 0$ (for a minimization problem) and $e^{-\Delta_{ij}/T}$ if $\Delta_{ij} > 0$. The control parameter is lowered in steps, with the system being allowed to approach equilibrium through the sequence of trials at each step. After an appropriate stopping condition is met, the final configuration is taken as the solution of the

problem at hand. There are a variety of possible stopping conditions. A common one is to terminate the algorithm when the observed improvement in cost over a number of consecutive Markov chains is small.

6.79 Remark In design construction one can recognize when an optimal solution is found, so the stopping condition is modified to detect this. Also, if the algorithm terminates without finding an optimal solution, then the annealing process is repeated, starting with a fresh random initial feasible solution.

6.80 Algorithm The general simulated annealing algorithm.

```
repeat
    Set values of temperature T_0 and Markov chain length L_0;
    Generate an initial feasible solution S;
    k := 0;
    repeat
        repeat L_k times
        begin
            Apply a random transition to S to obtain S' ∈ N(S);
            Δ := c(S') − c(S);
            if Δ ≤ 0 or random[0, 1) < e^{−Δ/T}
            then S := S';
            if c(S) = 0
            then exit loop
        end
        k := k + 1;
        Set L_k;
        Set T_k to some value < T_{k−1}
    until stop condition is met or c(S) = 0
until c(S) = 0
```

6.81 Remarks In Algorithm 6.80, T_k is the value of the control parameter and L_k the length of the Markov chain generated at the kth iteration of the Metropolis algorithm. The function `random`$[0, 1)$ returns a random number generated from a uniform distribution on the interval $[0, 1)$.

6.82 Remarks The performance of Algorithm 6.80 is influenced by the following factors:

1. The value of T_0.
2. The method for obtaining T_k from T_{k-1}.
3. The length of the Markov chain L_k.
4. The choice of stopping condition.

The specification of these parameters constitutes a *cooling schedule*. Generic and problem-specific decisions that must be made in order to produce an effective simulated annealing program are outlined in [1797].

6.83 Example An N_2 latin square contains no 2×2 latin subsquares (see §III.1.5) and often contains no other latin subsquares (see Elliott and Gibbons [783]). A simulated annealing algorithm for constructing latin squares that are N_2 (and, therefore, usually latin subsquare free) is described.

A feasible solution is a latin square, and its cost is the number of 2×2 subsquares contained in it. The transition function is described as follows. Suppose x and y are elements, and r a row, of a latin square L of side n. Define the (r, x, y)-cycle of L as the sequence $((r_1, c_1), (r_2, c_2), \ldots, (r_m, c_m))$, where $r_1 = r, r_2, \ldots, r_m = r$ are rows of L; $c_1, c_2, \ldots, c_m$ are columns of L; and

1. If i is even, then let $L(r_i, c_i) = y$ and $c_i = c_{i-1}$;
2. If i is odd, then let $L(r_i, c_i) = x$ and $r_i = r_{i-1}$ (for $i > 1$).

8	2	3	4	5	6	7	**1**
2	3	1	5	6	7	8	4
3	5	4	**8**	7	**1**	6	2
4	6	8	3	1	5	2	7
5	**8**	7	**1**	3	2	4	6
6	7	5	2	8	4	1	3
7	**1**	2	6	4	3	5	**8**
1	4	6	7	2	**8**	3	5

For example, suppose L is the latin square of side 8 given on the left. In this square, the elements of the (1, 1, 8)-cycle, ((1,8), (7,8), (7,2), (5, 2), (5, 4), (3, 4), (3, 6), (8, 6), (8, 1), (1, 1)), are shown in bold type.

If the elements making up a cycle in a latin square are rotated, then a new and, in general, nonisomorphic latin square is obtained. Such a rotation can therefore be used as a transition operation in a simulated annealing algorithm. Select a random 2×2 latin subsquare $L(r_1, c_1) = L(r_2, c_2) = e_1, L(r_1, c_2) = L(r_2, c_1) = e_2$, a random element $x \notin \{e_1, e_2\}$, and a random element $y \in \{e_1, e_2\}$. Performing a rotation on the (r_1, x, y)-cycle destroys the latin subsquare, but may create others.

Decrease the temperature by setting $T_k = \alpha T_{k-1}$, where $\alpha < 1$ is a constant, the *control decrement*. (While this is a popular way of decreasing the control temperature, there are many other methods, including adaptive ones.) The length of the Markov chain is held constant at all temperatures. For the stopping condition, terminate the algorithm once the cost function of the best solution obtained in the last Markov chain remains unchanged for a number of consecutive chains. The number of such chains is the *freezing factor*.

As with hill-climbing, repeat this process until an N_2 latin square is generated. Using the cooling schedule on the right it is possible to generate N_2 latin squares of orders $n \leq 18$.

Initial temperature:	1.0
Control decrement:	0.9995
Markov chain length:	350
Freezing factor:	12

6.84 Table Other examples of the successful application of annealing.

Configurations	References
Antipodal triple systems	Gibbons, Mendelsohn, and Shen [905]
Covering designs	Nurmela and Östergård [1690]
Equitable resolvable coverings	van Dam, Haemers, and Peek [2084]
Lotto designs	Li [1444]
Transversal covers	Stevens and Mendelsohn [1959]

▷ Tabu Search

6.85 Remarks *Tabu search* (see Glover, Taillard, and de Werra [910]) is another variant of local search in which the neighbor S' at each step is selected as a lowest cost feasible solution from a subset of $N(S)$, regardless of whether $c(S) \leq c(S')$. In order to prevent cycling among a set of feasible solutions, a queue, the *tabu list*, of length t, is maintained. This short-term memory records certain attributes of the previous t transitions and has the objective of banning moves with any of these attributes. A long-term memory function can also be used to help persuade the algorithm to visit regions that possibly have not been explored before. Additionally, an *aspiration criterion* can be used to override the tabu status of promising moves, such as those that lead to a better solution than the best one found so far.

As an example, consider the method used by Morales [1630] to construct partially balanced designs (§VI.42). Here a feasible solution is an equireplicate design, that is, an arrangement in which each point occurs in the same number of blocks. The goal is to transform an initial feasible solution into a solution with the required pairwise balancing properties. A transition is the exchange of two points x and y in different blocks l and m, and the tabu list consists of vectors of the form (x, y, l, m) representing

the exchanges that have occurred in the last t iterations. For long-term memory a count of the number of exchanges F_{xy} involving each pair $\{x, y\}$ is maintained. To encourage moves in new territories, the cost of an uphill move involving points x and y is increased by F_{xy}. Morales uses the standard aspiration criterion of allowing the tabu status of a move from S to S' to be canceled if the cost of S' is lower than the cost of the best solution found so far.

Tabu search can be merged with other nonexhaustive search paradigms. For example, a tabu list can be used in the context of a simulated annealing algorithm or within a hill-climbing algorithm (where only horizontal or downhill moves are accepted).

6.86 **Table** Examples of the successful application of tabu search.

Configurations	References
Covering codes	Östergård [1703]
Covering designs	Nurmela and Östergård [1691]
Difference families	Morales [1628]
Packing designs	Nurmela, Kaikkonen, and Östergård [1689]
PBIBDs with two associate classes	Morales [1630]

▷ **Other Methods**

6.87 **Remarks** *Evolutionary algorithms* are probabilistic search methods that model the evolution of populations based on the principle of survival of the fittest. Here a feasible solution corresponds to a chromosome with an associated measure of *fitness*. A population of feasible solutions is maintained, with genetic operators such as selection, recombination, and mutation applied with the objective of improving the overall fitness level of the population and, in particular, the fitness of the best individual member. Various forms of evolutionary algorithms, such as genetic algorithms, evolutionary strategies, and evolutionary programming, have been used for many types of combinatorial optimization problems.

6.88 **Table** Examples of the successful application of evolutionary algorithms.

Configurations	References
Difference families	Martinez, Đoković, and Vera-López [1529]
Lotto designs	Li [1444]
Optimal sequenced matroid bases	Gargano and Edelson [861]

6.89 **Remark** Other optimization problem heuristics worth considering for design construction include *threshold accepting*, *record-to-record travel*, *great deluge*, *variable neighborhood search*, and *reactive local search*.

6.6 Validity of Search Results

6.90 **Remarks** The ever increasing use of the computer to obtain design enumeration results has brought with it the need to justify the correctness of these results. While the existence of a design can be confirmed by a polynomial-time check of a provided example, a complete enumeration of a design family invariably involves the implementation of a variety of complex algorithms in possibly different languages on a set of machines running possibly different operating systems. Errors can arise from incorrect design, software implementation mistakes, and faulty hardware. While standard software engineering principles can, and should, be applied in order to improve confidence in the

design and implementation phases, the possibility of hardware faults, such as random bit flipping, is particularly frustrating as it is outside the control of the user.

Among the first to systematically address the issue of correctness of a design enumeration were Lam, Thiel, and Swiercz [1378] in their computer-based proof of the nonexistence of a projective plane of order 10 (see Remarks 6.27). Subsequently Lam [1370] and others, including Dinitz, Garnick, and McKay [715], Denny and Gibbons [697], and Kaski and Östergård [1268, 1271], outlined issues and techniques specifically related to the testing of computational results. These are summarized next.

6.91 Remark Often the counting techniques described in §6.4 can be used to obtain an independent check of an enumeration result. Such *double counting* checks generally rely on use of the Orbit-Stabilizer Theorem (Proposition VII.9.23) and the representation of the object in a different form.

6.92 Example In their STS(19) enumeration, Kaski and Östergård generate the STSs from a set of subdesigns, or seeds, S_i (see Example 6.14). During the search the number N_i of completions of each S_i to a complete STS is recorded. By the Orbit-Stabilizer Theorem, and the fact that each complete STS contains a total of b subdesigns, the total number of distinct STSs is given by

$$N = \frac{1}{b} \sum_i \frac{19!}{|\mathrm{Aut}(S_i)|} \cdot N_i$$

6.93 Remark This type of check can be extended to counting objects at various levels in the search tree (see [1271]).

6.94 Example In their enumeration of 1-factorizations of K_{12} (see Remarks 6.26 and 6.61), Dinitz, Garnick, and McKay [715] use an enumeration of the regular graphs of order 12 and degree k for $0 \le k < 12$, together with a formula analogous to that in Theorem 6.58, to obtain an independent count of the number of distinct 1-factorizations of K_{12}.

6.95 Remarks In an enumeration result, it is usually feasible to check that all generated objects are nonisomorphic, thereby confirming that the number obtained is a lower bound on the number of isomorphism classes. The main worry therefore is whether any classes have been missed, possibly due to an erroneous isomorph rejection during the search. This highlights a planning decision that must be made in the development of the search method. A partial isomorph rejection strategy is generally simpler to implement and therefore less error-prone. Moreover, it allows multiple paths to a complete solution, so that if one path is blocked (due, for example, to a random hardware error), then the generation of an isomorphic copy is not necessarily blocked. The tradeoff, however, is that the search is less efficient. Such *path redundancy* is particularly important in the justification of nonexistence results.

6.96 Example In the proof of nonexistence of a projective plane of order 10, Lam et al. [1378] address the concern of a hardware error, which they believe occurred on their CRAY-1S computer at the rate of about one per thousand hours of computing. In fact, they discovered one such error and remained concerned about the possibility of other undetected errors. The authors argue that, even with such errors, it is extremely unlikely that a projective plane of order 10 was missed. For, if an undiscovered plane exists, then it can be constructed as the extension of *each* of 24,675 configurations among those generated at the start of the search. In the unlikely worst-case event that all the 24,675 configurations were isomorphic and a hardware error happened to affect this case, a plane could be missed. Since there are about half a million configurations generated at the start of the search, the probability of a hardware error affecting this special configuration is very small under the assumption that one random bit-flip occurred during the entire search. In fact, as any plane of order 10

must have a trivial collineation group, it is more likely that at least two of the 24,675 configurations are nonisomorphic. The probability of hardware errors affecting both of them is infinitesimal.

6.97 Remark The technique of *internal consistency checking* involves performing various intermediate calculations and tests in two or more different ways, at least during testing of the program.

6.98 Example In [1378] the starting configurations used as seeds for the search were generated by two different programs and also checked by hand. A simpler, but slow, program was also used to attempt to extend a configuration to a complete plane. Although not used in the main production run, the results were checked in test runs against those from the fast version. Another check involved predicting the number of times each configuration would be generated during the search, and checking this against the actual count. For other examples of internal consistency checking refer to the generation of 2-$(7, 3, \lambda)$ designs in [697].

6.99 Remark A generalization of internal consistency checking involves developing and executing two or more enumerations independently and within possibly different computing environments so that the results can be cross-checked. Often, with the increasing power of computers, such cross-checks are carried out more easily some years later, sometimes allowing published results to be corrected (see, for example, the correction to the number of Mendelsohn triple systems of order 10 in [697]). It is important, therefore, that enumerators retain full and careful logs of their searches to facilitate later verification ([1378], for example).

6.100 Remark While tried-and-true software engineering techniques can be used in the implementation of a design enumeration, the correctness of the search method itself can be validated only by careful checking of the algorithm and the mathematical results on which key procedures, such as isomorph rejection, are based. Full and descriptive publication of methods is an important part of this process, as is the availability of the enumeration software and the tools used, where possible (for example, Cliquer [1682], DISCRETA [241], and `nauty` [1569]).

6.101 Remarks With an enumeration, one should be careful to run the algorithm on smaller design families that have already been (completely or partially) catalogued. The generality to be able to cater for designs of varying sizes and properties does present the algorithm designer with a dilemma. The tailoring of a general-purpose algorithm to cope with just one specific case can often lead to significant efficiency gains while incurring the chance of making errors that cannot be detected by running the software with other, already investigated design families. This *fine tuning* effect is already well known in software engineering circles. In general, however, designers should be encouraged to utilize well-tested "off the shelf" tools rather than to implement their own versions.

6.102 Example When generating signings of group divisible designs in [902], it was found that a 2 to 3 times speed-up could be achieved by altering the program to specifically sign over the group $\mathbb{Z}_2$ rather than a general group G.

6.7 Search-Related Techniques

6.103 Remark Many subproblems are encountered during an enumeration project. These include key procedures and data structures that must be used during the generation process, techniques that are used to analyse and validate the results, and methods

for cutting down the elapsed time of the generation task. Effective solutions to these subproblems are essential for a successful enumeration.

▷ Isomorphism

6.104 Remarks Closely tied to the problem of generating sets of block designs is the problem of analyzing the results and, in particular, determining the isomorphism classes of the produced designs. Block design isomorphism is graph isomorphism-complete (Remark 6.6), implying that a polynomial-time algorithm for this problem is unlikely to exist. Indeed, many of the graphs that have caused difficulty for isomorphism-testing algorithms are based on block designs or related configurations (see [1534]). Research effort in this area has therefore been directed at developing algorithms that are fast on the average or with special classes of block designs.

6.105 Given a design $D = (V, \mathcal{B})$ where $V = \{x_1, x_2, \ldots, x_v\}$ and $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$, define $G(D)$ to be a graph with vertex set $\{x_1, x_2, \ldots, x_v, B_1, B_2, \ldots, B_b\}$, with the element vertices having one color, and the block vertices having a second color, and edge set $\{\{x_i, B_j\} : x_i \in B_j\}$. The graph $G(D)$ is the *Levi graph* of D.

6.106 Proposition

1. Designs D_1 and D_2 are isomorphic if and only if graphs $G(D_1)$ and $G(D_2)$ are isomorphic.
2. The automorphism group of a simple design D is isomorphic to the automorphism group of the graph $G(D)$.

6.107 Remarks Using the Levi graph representation, one can use any graph isomorphism package to determine block design isomorphism and to calculate automorphism groups. The most practical graph isomorphism tool currently available is the `nauty` software package developed by McKay [1569]. `nauty` is a set of procedures for determining the automorphism group of a vertex-colored graph. This information is provided in the form of a set of generators, the size of the group, and the orbits of the group. It is also able to produce a canonically-labeled isomorph of the graph, which can be used for isomorphism testing. Version 2.2 of `nauty` is available from `http://cs.anu.edu.au/~bdm/nauty/`.

`nauty` is written in a portable subset of the language C. It runs with a variety of C compilers on a variety of machines and includes a large number of procedures and macros for manipulating graphs with the data structures used in the package. For example, `geng` is a fast generator of nonisomorphic graphs.

The user can call `nauty` directly from within a C program specifying a large variety of options, including whether the canonical labeling is required, whether a set of automorphism group generators is required, and what vertex invariant procedure is to be used. For an example of a complete C program that uses `nauty` see [1569].

Alternatively one can use `dreadnaut`, a simple program that can read graphs and execute `nauty`.

6.108 Remarks Using the point-block incidence graph is often not the most efficient way of using `nauty`. Given a design D, a series of *block intersection graphs* $G_i, i = 0, \ldots, k$ can be defined in which the vertices are the blocks of D, with two vertices adjacent if and only if the corresponding blocks intersect in exactly i points. For many families of block designs, it can be proved that the isomorphism class of each design is uniquely determined by the isomorphism class of one of these graphs. For example, this is the case with 2-$(v, k, 1)$ designs with $v > k(k^2 - 2k + 2)$, using the graph G_1.

When $v \ll b$ and v is small, McKay uses a faster version of `nauty` that works with partitions and permutations of the point set alone, essentially viewing the design as a hypergraph.

Crucial to the efficiency of using an isomorphism tester is the availability of a method for partitioning a list of designs into classes such that two isomorphic designs are in the same class. A property that partitions a list in such a way is an isomorphism invariant.

6.109 Example Take the design $D = (V = \{1,2,3,4\}, \mathcal{B} = \{\{1,2,4\},\{1,3\},\{2,3,4\}\})$, and label $G(D)$ so that the elements of D correspond to vertices 1 to 4, while the blocks correspond to vertices 5 to 7. The following example of a `dreadnaut` session is taken from [1569] and computes the group of D and displays its canonical labeling.

```
> $=1                                          label vertices starting at 1
> n=7 g
1:  5:                                         go to vertex 5 (block 1)
5:  1 2 4;
6:  1 3;
7:  2 3 4;
> f=[1:4]                                      fix the varieties set-wise
> cx                                           run nauty
[fixing partition]
(2 4)                                          group generators
level 2:  6 orbits; 2 fixed; index 2
(1 3)(5 7)
level 1:  4 orbits; 1 fixed; index 2
4 orbits; grpsize=4; 2 gens; 6 nodes; maxlev=3
tctotal=6; canupdates=1; cpu time = 0.02 seconds
> o                                            display the orbits
1 3; 2 4; 5 7; 6;
> b                                            display the canonical labeling
1 3 2 4 6 5 7                                  the vertices in canonical order
1 :  5 6;                                      the relabeled graph
2 :  5 7;
3 :  6 7;
4 :  6 7;
5 :  1 2;
6 :  1 3 4;
7 :  2 3 4;
> q                                            quit
```

6.110 An *isomorphism invariant* is a function I for which $I(D_1) = I(D_2)$ if D_1 and D_2 are isomorphic. When $I(D_1) = I(D_2)$ if and only if D_1 and D_2 are isomorphic, the invariant is *complete*.

6.111 Remark As there is currently no known efficiently computable complete invariant for designs in general, one must at present resort to incomplete invariants. In the resulting partitioned list isomorphism of pairs of designs within the same class must still be tested. With this in mind, a good measure of the effectiveness of an invariant is its *sensitivity*, viz. the ratio of the number of classes it distinguishes to the number of nonisomorphic designs under consideration.

6.112 Remark A complete invariant (also known as a *certificate*) has sensitivity one.

6.113 Remarks Often an invariant is formed by a count of the number of subconfigurations of a certain kind in a design. By counting the number of such subconfigurations containing each point (respectively block) one obtains a *point* (respectively *block*) invariant that partitions the vertices (respectively blocks) of a given design into classes such that two points (respectively blocks) in the same orbit are in the same class. The process can be extended to partitions of pairs, triples, and so on, so as to provide an automorphism group invariant partitioning of points and blocks within various stabilizer subgroups of the automorphism group. For example, suppose the point pairs $\{0,1\}$ and $\{0,2\}$ are in different classes in such a partition of pairs. Then, in constructing the group of the design, one can avoid searching for automorphisms that map $1 \rightarrow 2$ in the stabilizer subgroup that fixes 0. This information is critically important to an algorithm such as `nauty`, which is working to generate a canonical labeling of the design and to generate its automorphism group.

A great variety of design invariants are available, many being based on graph invariants such as those described in [1569]. These vertex invariants are generally obtained from an analysis of the numbers of subgraphs of prescribed types containing each vertex. A key feature of these types of graph invariants is that the induced partitions can be refined by analysing the partition classes of the vertices in the subgraphs containing each vertex. This refinement continues until the partition becomes stable.

Further refinements are produced as each possible isomorphism (or automorphism) is investigated. Each new vertex mapping $x \rightarrow y$ can be accepted onlyif the class structure of the neighboring vertices of x (the *context* of x) is the same as the context of y. If this is the case, then the context forms a refinement of the current partitioning. For details see Chapter 7 of [1360].

6.114 Example A general invariant that is effective for many classes of (nonsymmetric) designs is a clique analysis of one or more block intersection graphs of a design D. An isomorphism invariant of D is the total number of cliques of various sizes in G_i, as well as the spectrum of numbers of vertices, vertex pairs, vertex triples, and so on, belonging to cliques of various sizes. For many classes of designs, such as the 2-$(9,3,2)$ design family, the 2-$(9,4,3)$ design family, and cyclic STSs for $v \leq 27$, this invariant is complete. Generally the invariant is effective, although the computation of it, while polynomial-time, can be expensive due to the often large number of cliques for relatively small values of v.

6.115 Remark A clique-finding program, Cliquer, has been made publicaly available by Niskanen and Östergård [1682] at `http://www.tkk.fi/~pat/cliquer.html`. For other applications of clique-finding in design theory, see [1706].

6.116 Example An example of a specialized invariant for an STS is a *Pasch configuration* (or *fragment* or *quadrilateral*) consisting of a set of four blocks and six points of the form $\{\{u,v,w\}, \{u,x,y\}, \{z,v,x\}, \{z,w,y\}\}$. The set of Pasch configurations in an STS corresponds to a subset of the set of 4-cliques in the block intersection graph G_1. Computing the total number of Pasch configurations, together with counts of those containing each point, provides a part of the cycle-structure of an STS [588]. Although computing the Pasch configuration structure has the same $O(v^3)$ time-complexity as computing the complete cycle structure, it is considerably quicker and requires less space ($O(v)$). The invariant is complete for $v \leq 15$ and very effective for larger v [1964]. It has been widely used in the generation and analysis of STSs (for example, see Remarks 6.24).

A complete invariant for STS(15) used by Anglada and Maurras [101] counts the number of facets in the polyhedra constructed from the convex hull of the characteristic vectors of the blocks of the designs (these range from 150 to 32699 facets). Another

invariant for STS is the indegree list of the compact train [591].

6.117 Remark For 1-factorizations of the complete graph, one very sensitive invariant is the *train invariant* [731]. Additional useful invariants include the *tricolor invariant* [971], as well as the *hamiltonian circuits across the factors* and *4-cycles around the vertices*.

▷ Group Maintenance

6.118 Remark Operations involving all or parts of the automorphism group of a design are required to carry out isomorph rejection during an enumeration procedure. Efficient methods for storing, maintaining, and accessing permutation groups are therefore critical to the development of an effective enumeration. Typical operations include the following:

1. Given the set of generators of a group, compute the orbit of a given point.
2. Given the orbit partition under a given set of permutations, update the partition when a new permutation π is added.
3. Given a set of generators for a group G, list all the elements in G.
4. Given a set of generators for a group G, check whether a given permutation belongs to G.

6.119 Algorithm The first problem can be solved using the following simple closure algorithm to compute the orbit O of a point x.

```
O := W := {x};
while W ≠ ∅ do
begin
    Choose any point y ∈ W;
    W := W \ {y};
    for all g ∈ S do
    begin
        z := gy;
        if z ∉ O
        then begin
                 O := O ∪ {z};
                 W := W ∪ {z}
             end
    end
end
```

6.120 Remark Problem 2 can be solved by checking, for each point x, whether x and $\pi(x)$ are currently in different orbits and, if so, merging them. The well-known "union-find" algorithm (see Chapter 22 of [606]) can be used to perform a sequence of these checks and updates in near-linear time.

6.121 Remarks Problems 3 and 4 can be solved using the *Schreier–Sims representation* of G. The following description of this representation is adapted from Chapter 6 of [1360]. Let G consist of permutations on the point set $V = \{1, 2, \ldots, v\}$. Let $(y_1, y_2, \ldots, y_v)$ be a permutation of V. Define the chain of point stabilizer subgroups $G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_v = \{I\}$ as follows: $G = G_0, G_i = \{g \in G_{i-1} : g(y_i) = y_i\}, i = 1, 2, \ldots, v$. Let $orb(i) = \{g(y_i) : g \in G_{i-1}\} = \{x_{i,1}, x_{i,2}, \ldots, x_{i,n_i}\}, i = 1, 2, \ldots, v$, and define $U_i = \{h_{i,1}, h_{i,2}, \ldots, h_{i,n_i}\}, i = 1, 2, \ldots, v$ where $h_{i,j} \in G$ has $h_{i,j}(y_i) = x_{i,j}$. Then for all $i = 1, 2, \ldots, v$, U_i is a left transversal of G_i in G_{i-1}. The data structure $\vec{G} = [U_1, U_2, \ldots, U_v]$ is the *Schreier–Sims representation* of G.

Any $g \in G$ can now be uniquely represented as $g = h_{1,i_1} h_{2,i_2} \dots h_{v,i_v}$ by a process of sifting (see [1271]), and a simple backtrack procedure (see Chapter 6 of [1360]) can be used to run through all the elements of G without repetition. Sifting can also be used to determine membership of the group. The sequence $(y_1, y_2, \dots, y_v)$ is a *base* for G. In fact, any subsequence $(y_1, y_2, \dots, y_j)$ where $G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_j = \{I\}$ is a base and is *nonredundant* if $G_i \supset G_{i+1}$ for all $i = 1, 2, \dots, j-1$. A set S of permutations of the point set V is a *strong generating set* (SGS) for G relative to B if $\langle S \cap G_i \rangle = G_i$ for all $1 \le i \le j$. The Schreier–Sims algorithm, described in [1271, 1883], is used to determine a nonredundant base and an associated SGS for a given group G. The main objective of the algorithm is to obtain a small set of generators for G_{i+1} given generators for G_i. For more details on group maintenance operations see [1360].

▷ Distributed Search

6.122 Remarks Many large-scale enumerations have become feasible onlyby distributing the computation over a potentially large number of individual workstations (for notable examples, see [715, 1268, 1574]). Such parallelization of work can become complicated if the distributed tasks are not independent and require considerable intercommunication. Fortunately, most backtrack algorithms can be split into parts that require no mutual communication at all.

A key feature of an orderly algorithm that uses a canonicity test such as the one discussed in Remarks 6.19 is the ability to generate and test each design independently, without the need to explicitly examine any other design constructed at another point of the search. Parallelization of the algorithm is therefore relatively straightforward and can be achieved by splitting the backtrack generation of the structures into a number of segments. The structures within each segment of the search can then be tested for isomorphism independently using the canonicity test.

An important consideration is how to define the ranges of the segments such that the time taken to enumerate the designs within each segment is balanced as evenly as possible. The most effective way of doing this is to split the search on a set of N seeds, labeled 0 to $N-1$, over P processors, labeled 0 to $P-1$, so that processor i generates the extensions of all seeds labeled j, such that $j \bmod P = i$ (see [1571]). The individual seeds required for each processor can either be supplied explicitly or actually generated by the processor. In the latter case, it is important that the time taken to generate the seeds is negligible compared with the time required for the complete enumeration. For orderly algorithms (Remark 6.21), the lexicographically smaller seeds take longer to extend because they tend to generate the bulk of completed configurations that are in canonical form, so that the isomorph rejection techniques are less effective in the early stages of the search. This factor must be taken into account when choosing the seeds and allocating them to the processors.

With networks of computers, the use of a batch system, such as `autoson` [1570] (available from `http://cs.anu.edu.au/~bdm/autoson`), is highly recommended.

▷ Fine Tuning

6.123 Remark While algorithm design techniques can often result in order-of-magnitude running time improvements, significant (usually constant time) improvements can be achieved by *fine tuning* procedures (see [215]).

6.124 Example In a simulated annealing program, the computation of $e^{-\Delta/T}$, being nested inside the innermost loop, can account for up to a third of the total computation time. It is important, therefore, that efficient methods are used to calculate this expression.

For example, it is often faster to calculate the energy change Δ directly rather than to compute $c(S')$ separately and then set $\Delta = c(S') - c(S)$. In addition, a discrete approximation to the exponential distribution can be used. Suppose that the cost function c is integer-valued. Then whenever the value of T is changed, the value $E[i] = e^{-i/T}$ is calculated and stored for all integers i in the range of possible positive values for Δ. During execution of the program, the value of $e^{-\Delta/T}$ can be obtained by simply looking up $E[\lfloor\Delta\rfloor]$.

6.125 Remark Efficient data structures, particularly for the representation of sets, lists, and graphs, are crucial to the development of an effective program (see [1360]). Clever indexing systems can often be used to avoid the need for a search.

6.126 Example When hill-climbing in Algorithm 6.71, the operations of selecting live points and pairs are executed many times. With careful use of data structures, these operations can be made to run in constant time. For example, the operation of selecting a random live point can be done in constant time by using an array *livePoints*$[0 \ldots v-1]$, where the points *livePoints*$[0 \ldots$*numLivePoints*$-1]$ are live, and the points *livePoints*$[$*numLivePoints*$\ldots v-1]$ are dead. Thus selecting a random live point amounts to selecting a random number *livePointIndex* in the range 0 to *numLivePoints*-1, and then using the live point $x =$ *livePoints*$[$*livePointIndex*$]$. When x is used in a new block it may become dead. If so, the array *livePoints* is updated in constant time as follows, where *used*$[x]$ records the number of blocks containing x:

```
used[x] := used[x] + 1;
if used[x] = (v − 1)/2
then begin /* x must die */
        numLivePoints := numLivePoints−1;
        swap(livePoints[livePointIndex],livePoints[numLivePoints])
     end
```

Using similar data structures, each of the following operations can be carried out in constant time: Select a random live pair; kill a pair; resurrect a dead point; and resurrect a dead pair. For details see Chapter 5 of [1360].

6.127 Remarks Efficient methods of storing the generated catalogue of configurations are important in a large-scale enumeration. While efficient coding techniques are useful, with orderly algorithms (Remark 6.21) additional space can be saved by using the fact that the listed configurations are presented in increasing lexicographical order. This more sophisticated coding scheme completely stores the first configuration generated and thereafter stores only the changes from each previous configuration. For example, in the generation of twofold triple systems of order 12 in [696] it was found that on average each design could be stored in approximately 14.4 bytes, rather than 43.7 bytes when the complete designs are represented.

See Also

[588]	A comprehensive survey of block design construction and analysis techniques. Excellent introduction to the area.
[1271]	Coverage of enumeration algorithms.
[1360]	Good description of fundamental combinatorial algorithms.
[1569]	Description of state-of-the-art software package for graph enumeration and isomorphism.
[1571]	Discussion of isomorph-free exhaustive generation.
[1784]	Classic paper on orderly enumeration.

References Cited: [88, 101, 106, 215, 227, 235, 236, 240, 241, 267, 521, 522, 523, 536, 538, 539, 540, 543, 546, 568, 579, 584, 588, 591, 599, 606, 664, 696, 697, 711, 712, 714, 715, 717, 720, 722, 723, 726, 731, 778, 783, 791, 808, 860, 861, 899, 901, 902, 903, 905, 910, 941, 943, 969, 971, 1265, 1268, 1270, 1271, 1287, 1315, 1318, 1333, 1343, 1352, 1353, 1360, 1370, 1372, 1378, 1399, 1401, 1424, 1444, 1508, 1522, 1529, 1534, 1536, 1539, 1569, 1570, 1571, 1574, 1579, 1595, 1622, 1628, 1630, 1632, 1682, 1689, 1690, 1691, 1703, 1706, 1738, 1769, 1784, 1797, 1838, 1848, 1863, 1883, 1941, 1945, 1959, 1964, 2065, 2084, 2124]

7 Linear Algebra and Designs

Peter J. Dukes
Richard M. Wilson

7.1 Vector Spaces

7.1 Let $\mathbb{F}$ be a field. A set V of elements (*vectors*) is a *vector space over* $\mathbb{F}$ if

1. V is a group under an operation $+$, *vector addition*;
2. there is an operation, *scalar multiplication*, that assigns to each $c \in \mathbb{F}$ and $\mathbf{v} \in V$ a unique vector $c\mathbf{v} \in V$;
3. $1\mathbf{v} = \mathbf{v}$, $c_1(c_2\mathbf{v}) = (c_1c_2)\mathbf{v}$, $c(\mathbf{u}+\mathbf{v}) = c\mathbf{u}+c\mathbf{v}$, and $(c_1+c_2)\mathbf{v} = c_1\mathbf{v}+c_2\mathbf{v}$ for all $c, c_1, c_2 \in \mathbb{F}$ and all $\mathbf{u}, \mathbf{v} \in V$.

7.2 **Example** The set $\mathbb{F}^n$ of ordered n-tuples of elements of $\mathbb{F}$ is a vector space with componentwise vector addition and scalar multiplication.

7.3 Given a vector space V over $\mathbb{F}$, a subset $U \subseteq V$ is a *subspace* of V if it is also a vector space under the same operations as V. That is, U is a subspace if $c\mathbf{u}_1 + \mathbf{u}_2 \in U$ whenever $\mathbf{u}_1, \mathbf{u}_2 \in U$ and $c \in \mathbb{F}$.

7.4 For a nonempty set $S \subseteq V$, the *span* of S is the set $\operatorname{span}(S) = \{c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n : n \geq 1, \mathbf{v}_i \in S, c_i \in \mathbb{F}\}$. Define $\operatorname{span}(\emptyset) = \{0\}$.

7.5 **Remark** The span of $S \subseteq V$ is always a subspace of V.

7.6 A nonempty set $S \subseteq V$ of a vector space V is

1. *linearly independent* if for every finite subset $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq S$, $c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = 0$ implies $c_i = 0$ for each i;
2. *spanning* if $\operatorname{span}(S) = V$;
3. a *basis of* V if it is both linearly independent and spanning.

7.7 **Theorem** Every vector space V has a basis and any two bases of V have the same cardinality, the *dimension* of V.

7.8 **Remark** Here, it is assumed that all vector spaces have finite dimension.

7.9 Let V_1 and V_2 be vector spaces over $\mathbb{F}$. A *linear transformation* from V_1 to V_2 is a function $f : V_1 \to V_2$ such that $f(c\mathbf{v}) = cf(\mathbf{v})$ and $f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$.

7.10 Two vector spaces V_1 and V_2 over $\mathbb{F}$ are *isomorphic* if there exists a one-to-one and onto linear transformation f from V_1 to V_2. Such a mapping f is an *isomorphism*.

7.11 **Theorem** Every vector space over $\mathbb{F}$ of dimension n is isomorphic to $\mathbb{F}^n$ with componentwise addition and scalar multiplication.

7.12 **Remark** In light of Theorem 7.11, henceforth all vector spaces over $\mathbb{F}$ are represented by $\mathbb{F}^n$, $n \geq 1$, with the usual operations.

7.13 **Proposition** Consider the vector space $V = \mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$ of order q. For $1 \leq i \leq n$, the number of subspaces of V of dimension i equals

$$\begin{bmatrix} n \\ i \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

When $i = 0$, $\begin{bmatrix} n \\ i \end{bmatrix} = 1$. $\begin{bmatrix} n \\ i \end{bmatrix}_q$ are the *gaussian coefficients* (see Proposition VII.2.34).

7.14 Let V be a vector space and let $U \subseteq V$ be a subspace. A *coset* U' of U is a maximal collection of elements of V such that $\mathbf{v}_1 - \mathbf{v}_2 \in U$ for all $\mathbf{v}_1, \mathbf{v}_2 \in U'$. Write $U' = \mathbf{v} + U$ for any *representative* $\mathbf{v} \in U'$. The *quotient space* V/U has as vectors all cosets of U, addition given by $(\mathbf{v}_1 + U) + (\mathbf{v}_2 + U) = (\mathbf{v}_1 + \mathbf{v}_2) + U$, and scalar multiplication given by $c(\mathbf{v} + U) = (c\mathbf{v}) + U$. If U has dimension i, a coset of U is an *i-flat* of V.

7.15 **Remark** The vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$ is central to finite geometry and design theory. Two standard families of designs are given in Constructions 7.16 and 7.17. See §VII.2 for many more details.

7.16 **Construction** Let $V = \mathbb{F}_q^n$, $n \geq 1$, and let $\mathcal{B}$ be the set of all i-flats of V. Every pair of distinct vectors $\mathbf{u}, \mathbf{v} \in V$ lies in the unique 1-flat $\mathbf{u} + \operatorname{span}(\{\mathbf{v} - \mathbf{u}\})$. So $(V, \mathcal{B})$ is a (resolvable) 2-(q^n, q^i, λ) design, where $\lambda = \begin{bmatrix} n-1 \\ i-1 \end{bmatrix}_q$. This design is often denoted $\mathrm{AG}_i(n, q)$. (See §VII.2.4.)

7.17 **Construction** Let $V = \mathbb{F}_q^{n+1}$ and let $X = \{U_1, \ldots, U_{1+q+\cdots+q^n}\}$ be the set of all subspaces of dimension 1. For each subspace $W \subseteq V$ denote by B_W the set of all $U_j \in X$ with $U_j \subseteq W$. For some $i \geq 0$, let $\mathcal{B}$ be the set of all B_W, where W has dimension $i + 1$. Then $(X, \mathcal{B})$ is a 2-(v, k, λ) design, where $v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$, $k = \begin{bmatrix} i+1 \\ 1 \end{bmatrix}_q$, and $\lambda = \begin{bmatrix} n-1 \\ i-1 \end{bmatrix}_q$. When $n = 2$ and $i = 1$, this is a projective plane of order q. (See §VII.2.3.)

7.2 Matrices: Rank, Eigenvalues, and Projections

7.18 **Remark** Let m and n be positive integers and $\mathbb{F}$ a field. Familiarity is assumed with the vector space of $m \times n$ matrices over $\mathbb{F}$, as well as the definition and elementary properties of matrix multiplication, transpose, and determinant. Vectors of length n are regarded as $n \times 1$ matrices.

7.19 Let A be an $m \times n$ matrix over $\mathbb{F}$.

1. The *row space* of A is the span of the set of rows of A.
2. The *column space* of A is the span of the set of columns of A.
3. The *rank* of a matrix A is the dimension of both the row space and column space of A, which is well defined in light of Theorem 7.20.

7.20 **Theorem** Let A be an $m \times n$ matrix over $\mathbb{F}$. The dimension of the row space of A equals the dimension of the column space of A. Therefore, $\operatorname{rank}(A) = \operatorname{rank}(A^\top)$.

7.21 **Proposition** Suppose A is $m \times n$ and B is $n \times p$. Then $\operatorname{rank}(A) + \operatorname{rank}(B) - n \leq \operatorname{rank}(AB) \leq \min\{\operatorname{rank}(A), \operatorname{rank}(B)\}$.

7.22 **Proposition** A is invertible if and only if A is $n \times n$ and $\operatorname{rank}(A) = n$;

7.23 **Example** The $n \times n$ *identity matrix* I_n (or simply I) has rank n. The $m \times n$ *all ones matrix* J_{mn} (or simply J) has rank 1.

7.24 **Proposition** Over the real numbers $\mathbb{R}$, $\operatorname{rank}(A) = \operatorname{rank}(AA^\top)$.

7.25 Let A be an $n \times n$ matrix over a field $\mathbb{F}$. An element $x \in \mathbb{F}$ is an *eigenvalue* of A if there exists a nonzero $\mathbf{v} \in \mathbb{F}^n$ such that $A\mathbf{v} = x\mathbf{v}$. The *multiplicity* of x is the dimension of the span of all such $\mathbf{v}$.

7.26 Remarks

1. An eigenvalue x of A has multiplicity m if and only if $A - xI_n$ has rank $n - m$.
2. The sum of the multiplicities of all eigenvalues of A is at most n.

7.27 Theorem If A is an $n \times n$ symmetric matrix over $\mathbb{R}$, then A has n real eigenvalues, counting multiplicities. Their product (with multiplicities) equals $\det(A)$.

7.28 A symmetric $n \times n$ matrix A over $\mathbb{R}$ is *positive semidefinite* (respectively, *positive definite*) if $\mathbf{v}^\top A\mathbf{v} \geq 0$ for all $\mathbf{v}$ (respectively, if $\mathbf{v}^\top A\mathbf{v} > 0$ for all $\mathbf{v} \neq \mathbf{0}$.)

7.29 Theorem The following are equivalent for real symmetric matrices A.

1. A is positive semidefinite;
2. $\det(A') \geq 0$ for all principal submatrices A' of A; and
3. all of the eigenvalues of A are nonnegative.

7.30 Let U be a subspace of V, and $\mathbf{v} \in V$. The *orthogonal projection of* $\mathbf{v}$ *onto* U is the unique vector $\mathbf{v}' \in U$ such that $\mathbf{v} - \mathbf{v}'$ is *orthogonal* to $\mathbf{v}$; that is, $\mathbf{v}^\top(\mathbf{v} - \mathbf{v}') = 0$.

7.31 Proposition If U is the row space (over the reals) of an $m \times n$ matrix B with rank m, then the orthogonal projection from $\mathbb{R}^n$ onto U is a linear transformation given by $\mathbf{v} \mapsto P\mathbf{v}$, where $P = B^\top(BB^\top)^{-1}B$.

7.32 Remarks If $\mathbf{u} \in U$, the orthogonal projection onto U fixes $\mathbf{u}$; that is, $P\mathbf{u} = \mathbf{u}$. Hence, it follows that $P^2 = P$, the eigenvalues of P are are all 0 and 1, and both P and $I - P$ are positive semidefinite.

7.3 The Incidence Matrix of a Design

7.33 Let $\mathcal{D} = (X, \mathcal{B})$ be an incidence structure with points $X = \{x_1, \ldots, x_v\}$ and blocks $\mathcal{B} = \{B_1, \ldots, B_b\}$. An *incidence matrix* $N = (N_{ij})$ for $\mathcal{D}$ is a $v \times b$ matrix defined by $N_{ij} = 1$ if x_i is incident with B_j and $N_{ij} = 0$ otherwise.

7.34 Example An incidence matrix for the unique 2-$(6, 3, 2)$ design (Example II.1.18) is given on the right.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

7.35 Proposition The incidence matrix N for a 2-(v, k, λ) design having replication number r satisfies

1. $NN^\top = (r - \lambda)I + \lambda J$;
2. $JN = kJ$; and
3. $NJ = rJ$.

7.36 Corollary

1. $NN^\top$ has eigenvalues rk, with multiplicity 1, and $r - \lambda$, with multiplicity $v - 1$;
2. $\det(NN^\top) = rk(r - \lambda)^{v-1}$; and
3. over $\mathbb{R}$, $\operatorname{rank}(N) = v$ provided $v > k$ and $\lambda > 0$.

7.37 Remark A consequence of Corollary 7.36 is Fisher's Inequality ($b \geq v$ for nontrivial BIBDs, Theorem II.1.9). Certain similar statements can be made for PBDs and partially balanced designs; see [2155].

7.38 **Proposition** Two 2-(v,k,λ) designs with incidence matrices N_1 and N_2 are isomorphic if and only if there exist permutation matrices P and Q such that $PN_1Q = N_2$.

7.39 **Theorem** (Connor's Inequality, [596]) Suppose m blocks of a 2-(v,k,λ) design are chosen. Let N_0 denote the $v \times m$ submatrix of N corresponding to the chosen blocks and let $C = \lambda kJ + r(r-\lambda)I - rN_0^\top N_0$. Then

$$\begin{cases} \det(C) \geq 0 & \text{if } m < b - v; \\ \det(C) = 0 & \text{if } m > b - v; \\ kr^{-m+1}(r-\lambda)^{v-m-1}\det(C) \text{ is a perfect square} & \text{if } m = b - v. \end{cases}$$

7.40 **Corollary** [596] Suppose in a 2-(v,k,λ) design that there are two blocks intersecting in μ points. Then $k + \lambda - r \leq \mu \leq \frac{2k\lambda}{r} - (k + \lambda - r)$.

7.41 **Construction** [1907] Let N be the incidence matrix of a 2-$(v,k,1)$ design with replication number $r = 2k+1$. Then $NN^\top = 2kI + J$. Let $M = N^\top N - kI$, a symmetric $0,1$-matrix. The row and column sums of M are $2k^2$ and $MM^\top = k^2(I+J)$. Therefore, M is the incidence matrix of a symmetric 2-$(4k^2-1, 2k^2, k^2)$ design.

7.42 **Construction** Suppose N is the incidence matrix of a Hadamard 2-(v,k,λ) design with $v = 4n-1$, $k = 2n-1$, $\lambda = n-1$ (§V.1). Let $\overline{N} = J - N$. Then

$$\begin{pmatrix} N & \overline{N} \\ J_{1v} & 0_{1v} \end{pmatrix}$$

is the incidence matrix of a 3-$(v+1, k+1, \lambda)$ design, a Hadamard 3-design.

7.4 Rational Congruence and Symmetric Designs

7.43 Given $b, c \in \mathbb{Q}$ and a prime p, the *Hilbert norm residue symbol* $(b,c)_p$ is defined to be 1 or -1 according as $bx^2 + cy^2 \equiv z^2 \pmod{p^m}$ has integer solutions x, y, z, not all multiples of p, for all positive integers m. Define $(b,c)_\infty$ similarly according as the equation $bx^2 + cy^2 = z^2$ has a solution over $\mathbb{R}$.

7.44 **Theorem** The equation $bx^2 + cy^2 = z^2$ has solutions in integers x, y, z not all zero if and only if $(b,c)_p = 1$ for all primes p, and for $p = \infty$.

7.45 **Proposition** For integers b, b', c,

1. $(b,c)_\infty = 1$ unless $b, c < 0$;
2. for $p \neq \infty$, $(b,c)_p = 1$ unless $p|b$ or $p|c$;
3. $(b,c)_p(b',c)_p = (bb',c)_p$ for any p; and
4. $\prod (b,c)_p = 1$, where the product is over all primes p and $p = \infty$.

7.46 Given a positive definite $n \times n$ matrix A, let D_m be the determinant of the $m \times m$ leading principal submatrix of A, $m = 1, 2, \ldots$. The *Hasse–Minkowski invariants* of A are defined, for p a prime or ∞ as

$$C_p(A) = (-1, -D_m)_p \prod_{i=1}^{m} (D_i, -D_{i+1})_p.$$

7.47 Two $n \times n$ symmetric matrices A and B over the rationals $\mathbb{Q}$ are *rationally congruent* if there exists a nonsingular matrix M over $\mathbb{Q}$ with $M^\top AM = B$.

7.48 **Theorem** (Hasse–Minkowski Theorem) Two positive definite $n \times n$ symmetric matrices A and B over $\mathbb{Q}$ are rationally congruent if and only if $C_p(A) = C_p(B)$ for every odd prime p and for $p = \infty$.

7.49 **Proposition** Suppose N is an incidence matrix of a symmetric 2-(v,k,λ) design. Then

1. $N^\top$ is the incidence matrix of a symmetric 2-(v,k,λ) design;

2. $\det(NN^\top) = (\det(N))^2$, the square of an integer; and
3. I_v and $(k-\lambda)I_v + \lambda J_{vv}$ must be rationally congruent.

7.50 Remarks

1. Part 1 in Theorem 7.49 is due to Ryser. See also Theorem 7.84.
2. The Bruck–Ryser–Chowla Theorem (see §II6.2) follows from parts 2 and 3 in Theorem 7.49 and Theorem 7.48. If v is even, then $k^2(k-\lambda)^{v-1}$, and hence, $k-\lambda$, must be a perfect square. For v odd, one computes as in [1016] that $C_p((k-\lambda)I_v + \lambda J_{vv}) = (-1,-1)_p(n,(-1)^{(v-1)/2}\lambda)_p$ for all $p \neq 2$. But $C_p(I_v) = (-1,-1)_p$. So by Theorems 7.44 and 7.48, $nx^2 + (-1)^{(v-1)/2}\lambda y^2 = z^2$ must have a solution in integers not all zero.
3. See Theorem 7.91 for another application of rational congruence.

7.5 Smith Normal Form and the p-Rank of a Design

7.51 Let p be a prime, and A an integral matrix. The *p-rank* of A is the rank of A over the field $\mathbb{F}_p$.

7.52 Let A be an $m \times n$ integral matrix, and suppose $m \leq n$. Then there exist integral matrices U and V with $\det(U), \det(V) = \pm 1$, such that $UAV = [D|O]$, where D is the diagonal matrix with nonnegative entries $d_1, d_2, \ldots, d_m$ such that $d_1 \mid d_2 \mid \cdots \mid d_m$, and O is the $m \times (n-m)$ zero matrix. The matrix $[D|O]$ is the *Smith Normal Form* (SNF) of A, and the d_i are the the *invariant factors* of A.

7.53 Remarks

1. The SNF of a matrix is unique and can be computed from elementary row and column operations that are invertible over $\mathbb{Z}$.
2. If A is square matrix with invariant factors $d_1, \ldots, d_n$, then $\det(A) = d_1 d_2 \cdots d_n$.
3. The p-rank of A is the number of invariant factors relatively prime to p.

7.54 Example The invariant factors of the matrix

$$A = \begin{pmatrix} 2 & -6 & -8 & 4 \\ -4 & 0 & 16 & 4 \\ 0 & -6 & 0 & 6 \end{pmatrix}$$

are $d_1 = 2$, $d_2 = 6$, and $d_3 = 0$. The p-ranks of A for $p = 2, 3, 5$ are $0, 1, 2$, respectively.

7.55 The *Smith Normal Form* and *p-rank of a design* are those of its incidence matrix.

7.56 Remark From Proposition 7.38 designs with different p-ranks or SNF's are nonisomorphic.

7.57 Example [448] Consider the designs $\mathcal{D}_1$ and $\mathcal{D}_2$ constructed from the difference sets presented in Construction VI.18.38 and Conjecture VI.18.39, respectively, each with parameters $(\frac{1}{2}(3^m-1), 3^{m-1}, 2\cdot 3^{m-2})$. For each m, the invariant factors are all powers of 3, and the number of invariant factors equal to 1 (hence the 3-rank) is identical for both $\mathcal{D}_1$ and $\mathcal{D}_2$. However, for $m = 9$, $\mathcal{D}_1$ has 1251 invariant factors equal to 3 and $\mathcal{D}_2$ has 1440 invariant factors equal to 3, so the resulting designs are nonisomorphic.

7.58 Remark From Proposition 7.36, the p-rank of a 2-(v,k,λ) design with replication number r is full unless $p \mid rk(r-\lambda)$.

7.59 Proposition The p-rank of a 2-(v,k,λ) design with replication number r equals

$$\begin{cases} v & \text{if } p \mid r \text{ and } p \nmid k(r-\lambda); \\ v-1 & \text{if } p \mid k \text{ and } p \nmid r-\lambda. \end{cases}$$

7.60 **Example** The three nonisomorphic 2-$(10, 4, 2)$ designs in Table II.1.25 have 2-ranks $6, 7, 5$, respectively.

7.61 **Theorem** [1023] The p-rank of a symmetric 2-(v, k, λ) design is at least $v - h$, where h is the maximum integer such that $p^{2h} \mid k^2(k-\lambda)^{v-1}$.

7.62 **Theorem** [1397] The p-rank of a symmetric 2-(v, k, λ) design is exactly $(v+1)/2$ whenever $p \mid k - \lambda$, $p^2 \nmid k - \lambda$ and $p \nmid k$.

7.63 **Remarks**

1. Under the hypotheses of Theorem 7.62, v must be odd in light of the Bruck–Ryser–Chowla Theorem and $(v+1)/2$ is the minimum p-rank allowed in Theorem 7.61.
2. The hypotheses of Theorem 7.62 hold for projective planes of order n, where $p \mid n$ but $p^2 \nmid n$. For a contrasting result, see Theorem 7.64.

7.64 **Theorem** The p-rank of a desarguesian projective plane of order p^s is $1 + \binom{p+1}{2}^s$.

7.65 **Theorem** [1602] Suppose $p \mid n$. The p-rank of a skew Hadamard 2-$(4n-1, 2n-1, n-1)$ design equals $2n$ (see §V1).

7.66 **Remark** Given an STS(v) (a 2-$(v, 3, 1)$ design), any subsystem of order $(v-1)/2$ is a *projective hyperplane*. The set of all projective hyperplanes of any STS has the structure of a projective space over $\mathbb{F}_2$ [2010]. Its dimension, denoted d_P, is the *projective dimension* of the STS. The *affine dimension* d_A is defined similarly over $\mathbb{F}_3$ with disjoint subsystems of order $v/3$. The projective STS($2^n - 1$) has $d_P = n - 1$ and the affine STS(3^n) has $d_A = n$.

7.67 **Theorem** [746] The p-rank of an STS(v) equals v if $p \neq 2, 3$; $v - d_P - 1$ if $p = 2$; and $v - d_A - 1$ if $p = 3$.

7.6 Higher Incidence Matrices and t-Designs

7.68 Let X be a set of v points, and for some integer t with $1 \le t \le v$, let $\{T_1, \ldots, T_{\binom{v}{t}}\}$ be the set of all t-subsets of V. Suppose $\mathcal{D} = (X, \mathcal{B})$ is an incidence structure with blocks $\{B_1, \ldots, B_b\}$. A *higher incidence matrix* N_t for $\mathcal{D}$ is a $\binom{v}{t} \times b$ matrix with ij-entry 1 if $T_i \subseteq B_j$ and 0 otherwise. If $\mathcal{D}$ consists of all k-subsets of V, the notation W_{tk} is used for N_t.

7.69 **Proposition** The existence of a (simple) t-(v, k, λ) design is equivalent to the existence of a nonnegative integer ($\{0, 1\}$) solution ϕ to $W_{tk}\phi = \lambda\mathbf{j}$, where $\mathbf{j}$ is the $\binom{v}{t} \times 1$ all ones vector (see §VII.6.3).

7.70 **Remarks**

1. For a t-design, the vector ϕ (the *characteristic vector* of the design) has length $\binom{v}{k}$ and the entry in position i equals the number of times block B_i appears in the design.
2. Consequences of $W_{tk}\phi = \mathbf{z}$ having *nonnegative* solutions for certain designs are considered in [760].
3. The *integer* solutions to a more general system of equations are described in [2156].

7.71 **Proposition** For $s \le t \le k$, $W_{st}W_{tk} = \binom{k-s}{t-s}W_{sk}$.

7.72 **Proposition** The higher incidence matrices $N_0, N_1, N_2, \ldots$ of a t-(v, k, λ) design satisfy

1. $W_{ie}N_e = \binom{k-i}{e-i}N_i$ for $0 \le i \le e \le k$;

2. $N_e N_f^\top = \sum_i b^i_{e+f-i} W_{ie}^\top W_{if}$ whenever $e + f \le t$, where $b^i_j = \lambda\binom{v-i-j}{k-j}/\binom{v-t}{k-t}$ is the number of blocks containing all of a given set of i points and none of a disjoint set of j points.

7.73 Remark One consequence of Theorem 7.72 is the bound $b \ge \binom{v}{s}$ for t-designs with $t \ge 2s$ and $v \ge k + s$. See Corollary 7.78 and [1783, 2155].

7.74 Theorem [2155] Let $N_0, N_1, N_2, \ldots$ be the higher incidence matrices of a t-(v, k, λ) design, and suppose the orthogonal projection from $\mathbb{R}^b$ onto the row space of N_s is given by the matrix P_s. Suppose $t \ge 2s$ and $v \ge k + s$. Then the ij-entry of P_s is $f_s(|B_i \cap B_j|)$, where

$$f_s(x) = \sum_{i=0}^{s} (-1)^{s-i} \binom{k-i-1}{s-i} (b_i^s)^{-1} \binom{x}{i}.$$

7.75 Corollary Let $A_1, A_2, \ldots, A_m$ be blocks chosen from a t-(v, k, λ) design. With $f_s(x)$ as above, $\det(I - [f_s(|A_i \cap A_j|)]) \ge 0$.

7.76 Remarks

1. Corollary 7.75 follows from the fact that $I - P_s$ is positive semidefinite. See Theorem 7.29 and Remarks 7.32.
2. The case $t = 2$, $s = 1$ reduces to Corollary 7.40.

7.77 Theorem [2153] Let $t \ge 2s$, $v \ge k + s$. Suppose M is an m-subset of V, where $s \le m \le v - s$. Suppose that a t-(v, k, λ) design on V has blocks $B_1, \ldots, B_n$ that are all contained in M. Then

$$b \ge n \sum_{i=0}^{s} \left(\binom{v}{i} - \binom{v}{i-1} \right) \binom{k}{i} \binom{v-m}{i} \binom{m}{i}^{-1} \binom{v-k}{i}^{-1},$$

with equality only if $f_s(|M \cap B_j|) = 0$ for $j = n + 1, \ldots, b$.

7.78 Corollary Let $t \ge 2s$, $v \ge k + s$. If a t-(v, k, λ) design has an n-fold repeated block, then $b \ge n\binom{v}{s}$.

7.79 Remark One proof of Theorem 7.77 follows from considering the orthogonal projection of $(\overbrace{1, \ldots, 1}^{b}, 0, \ldots, 0)$ onto the subspace of $\mathbb{R}^b$ spanned by the vectors

$$\left(\binom{|M \cap B_1|}{i}, \ldots, \binom{|M \cap B_b|}{i} \right), \quad i = 0, \ldots, s.$$

7.80 For $0 \le s \le k$, let P_s be the matrix corresponding to orthogonal projection from $\mathbb{R}^{\binom{v}{k}}$ onto the row space of W_{sk}. For $s \ge 1$, $E_s = P_s - P_{s-1}$, is the sth *idempotent*.

7.81 Proposition $E_i E_j = E_i$ if $i = j$; and 0 if $i \ne j$.

7.82 Theorem [673] ϕ is the characteristic vector of a t-(v, k, λ) design if and only if $E_s \phi = \mathbf{0}$ for all $s = 1, \ldots, t$.

7.83 Remark Together with *Delsarte's inequalities* $\phi^\top E_s \phi \ge 0$ (see §VI.1), Theorem 7.82 provides a strong LP constraint on t-designs.

7.7 Duality and PBIBDs

7.84 Theorem [1901] Suppose N is the incidence matrix of a quasi-symmetric 2-(v, k, λ) design (see §VI.48). Then $N^\top$ is the incidence matrix of a PBIBD with two associate classes (see §VI.42).

7.85 **Remarks** The PBIBD with incidence matrix $N^\top$ is the *dual* of the design with incidence matrix N. For a generalization to t-designs, see [414].

7.86 **Proposition** In particular, suppose N is the incidence matrix of a 2-$(v,k,1)$ design (with $v > k$). Then $M = N^\top N - kI$ is the adjacency matrix of a strongly regular graph. Indeed, $M^2 = (r-2k-1)M + k^2J + k(r-k-1)I$.

7.87 **Theorem** [1663] For a two associate class PBIBD with v points, block size k, and indices $\lambda_0 = r, \lambda_1, \lambda_2$, either $r \geq k$ or

$$(r-\lambda_1)(r-\lambda_2) + (\lambda_1-\lambda_2)[p_{12}^2(r-\lambda_1) - p_{12}^1(r-\lambda_2)] = 0.$$

7.88 **Remark** Theorem 7.87 is known as Nair's condition and follows from the fact that $NN^\top$ has zero as an eigenvalue for $k > r$. For a generalization to m associate class PBIBDs, see [1663, 1770].

7.89 **Proposition** Let N be the incidence matrix of a group divisible PBIBD$(v,k,\lambda_1,\lambda_2)$ with m groups of size n. The eigenvalues of $NN^\top$ are rk, with multiplicity 1; $r-\lambda_1$, with multiplicity $m-1$; and $rk - v\lambda_2$, with multiplicity $n(m-1)$.

7.90 **Corollary** Under these assumptions, the number of blocks b satisfies

$$b \geq \begin{cases} r+m-1 & \text{if } r = \lambda_1; \\ v-m+1 & \text{if } r > \lambda_1 \text{ and } rk = v\lambda_2; \\ v & \text{if } r > \lambda_1 \text{ and } rk > v\lambda_2. \end{cases}$$

7.91 **Theorem** [1770] Necessary conditions for the existence of a symmetric group divisible PBIBD$(v,k,\lambda_1,\lambda_2)$ with m groups of size n are

1. $(k-\lambda_1)^{m-1}(k^2 - v\lambda_2)^{m(n-1)}$ is a perfect square and
2. $(-1, k^2-v\lambda_2)_p^{m(m-1)/2}(-1,k-\lambda_1)_p^{m(n-1)(m(n-1)+1)/2}$
   $\times (k^2-v\lambda_2, vn^m)_p (k-\lambda_1, n)_p^m = 1$ for all odd primes p.

7.92 **Remark** There is a computational advantage in performing statistical experiments with PBIBDs having a small number m of associate classes. Let N be the incidence matrix of such a PBIBD on v points and b blocks (with full rank), and consider the linear regression model $\mathbf{y} = N^\top\beta + \epsilon$. Here, $\mathbf{y}$ is a vector of observed values, β is a vector of unknown constants to be determined, and ϵ is an "error" vector. The *least squares estimate* of β is the orthogonal projection of β onto the column space of $N^\top$, or $\hat{\beta} = (NN^\top)^{-1}N\mathbf{y}$. Because $NN^\top$ belongs to the algebra generated by the matrices $\{I, A_1, \ldots, A_m\}$ of the association scheme (see §VI.1), its inverse can be computed efficiently, even if the number of varieties v is large.

See Also

§VI.1	Association schemes and Delsarte's inequalities.
§VII.1	Linear algebra and coding theory.
§VII.2	More on finite geometries.
[1768]	Near vector spaces and designs.
[1120]	A textbook on linear algebra.
[1770]	Various incidence matrix constructions; more on duality and rational congruence.
[940, 953]	*Null designs* are integer solutions ϕ to $W_{tk}\phi = \mathbf{0}$.
[913]	A nice survey of linear algebraic methods in combinatorics.
[2173]	A compilation of many algebraic results on difference sets.
[448, 1397]	The Smith normal form.

References Cited: [414, 448, 596, 673, 746, 760, 913, 940, 953, 1016, 1023, 1120, 1397, 1602, 1663, 1768, 1770, 1783, 1901, 1907, 2010, 2153, 2155, 2156, 2173]

8 Number Theory and Finite Fields

Jeffrey H. Dinitz
Hugh C. Williams

8.1 Table of Primes and Primitive Roots

8.1 A number ω is a *primitive root* for p if $\omega^x \not\equiv 1 \pmod{p}$ for any $0 < x < p-1$, or equivalently, if ω is a generator of $\mathbb{Z}_p^*$, the multiplicative group of $\mathbb{Z}_p$.)

8.2 **Table** For each prime $p < 10000$ the least primitive root ω is given.

p	ω	p	ω	p	ω	p	ω	p	ω	p	ω	p	ω	p	ω	p	ω
3	2	5	2	7	3	11	2	13	2	17	3	19	2	23	5	29	2
31	3	37	2	41	6	43	3	47	5	53	2	59	2	61	2	67	2
71	7	73	5	79	3	83	2	89	3	97	5	101	2	103	5	107	2
109	6	113	3	127	3	131	2	137	3	139	2	149	2	151	6	157	5
163	2	167	5	173	2	179	2	181	2	191	19	193	5	197	2	199	3
211	2	223	3	227	2	229	6	233	3	239	7	241	7	251	6	257	3
263	5	269	2	271	6	277	5	281	3	283	3	293	2	307	5	311	17
313	10	317	2	331	3	337	10	347	2	349	2	353	3	359	7	367	6
373	2	379	2	383	5	389	2	397	5	401	3	409	21	419	2	421	2
431	7	433	5	439	15	443	2	449	3	457	13	461	2	463	3	467	2
479	13	487	3	491	2	499	7	503	5	509	2	521	3	523	2	541	2
547	2	557	2	563	2	569	3	571	3	577	5	587	2	593	3	599	7
601	7	607	3	613	2	617	3	619	2	631	3	641	3	643	11	647	5
653	2	659	2	661	2	673	5	677	2	683	5	691	3	701	2	709	2
719	11	727	5	733	6	739	3	743	5	751	3	757	2	761	6	769	11
773	2	787	2	797	2	809	3	811	3	821	2	823	3	827	2	829	2
839	11	853	2	857	3	859	2	863	5	877	2	881	3	883	2	887	5
907	2	911	17	919	7	929	3	937	5	941	2	947	2	953	3	967	5
971	6	977	3	983	5	991	6	997	7	1009	11	1013	3	1019	2	1021	10
1031	14	1033	5	1039	3	1049	3	1051	7	1061	2	1063	3	1069	6	1087	3
1091	2	1093	5	1097	3	1103	5	1109	2	1117	2	1123	2	1129	11	1151	17
1153	5	1163	5	1171	2	1181	7	1187	2	1193	3	1201	11	1213	2	1217	3
1223	5	1229	2	1231	3	1237	2	1249	7	1259	2	1277	2	1279	3	1283	2
1289	6	1291	2	1297	10	1301	2	1303	6	1307	2	1319	13	1321	13	1327	3
1361	3	1367	5	1373	2	1381	2	1399	13	1409	3	1423	3	1427	2	1429	6
1433	3	1439	7	1447	3	1451	2	1453	2	1459	3	1471	6	1481	3	1483	2
1487	5	1489	14	1493	2	1499	2	1511	11	1523	2	1531	2	1543	5	1549	2
1553	3	1559	19	1567	3	1571	2	1579	3	1583	5	1597	11	1601	3	1607	5
1609	7	1613	3	1619	2	1621	2	1627	3	1637	2	1657	11	1663	3	1667	2
1669	2	1693	2	1697	3	1699	3	1709	3	1721	3	1723	3	1733	2	1741	2
1747	2	1753	7	1759	6	1777	5	1783	10	1787	2	1789	6	1801	11	1811	6
1823	5	1831	3	1847	5	1861	2	1867	2	1871	14	1873	10	1877	2	1879	6
1889	3	1901	2	1907	2	1913	3	1931	2	1933	5	1949	2	1951	3	1973	2
1979	2	1987	2	1993	5	1997	2	1999	3	2003	5	2011	3	2017	5	2027	2
2029	2	2039	7	2053	2	2063	5	2069	2	2081	3	2083	2	2087	5	2089	7

p	ω	p	ω	p	ω	p	ω	p	ω	p	ω	p	ω	p	ω
2099	2	2111	7	2113	5	2129	3	2131	2	2137	10	2141	2	2143	3	2153	3
2161	23	2179	7	2203	5	2207	5	2213	2	2221	2	2237	2	2239	3	2243	2
2251	7	2267	2	2269	2	2273	3	2281	7	2287	19	2293	2	2297	5	2309	2
2311	3	2333	2	2339	2	2341	7	2347	3	2351	13	2357	2	2371	2	2377	5
2381	3	2383	5	2389	2	2393	3	2399	11	2411	6	2417	3	2423	5	2437	2
2441	6	2447	5	2459	2	2467	2	2473	5	2477	2	2503	3	2521	17	2531	2
2539	2	2543	5	2549	2	2551	6	2557	2	2579	2	2591	7	2593	7	2609	3
2617	5	2621	2	2633	3	2647	3	2657	3	2659	2	2663	5	2671	7	2677	2
2683	2	2687	5	2689	19	2693	2	2699	2	2707	2	2711	7	2713	5	2719	3
2729	3	2731	3	2741	2	2749	6	2753	3	2767	3	2777	3	2789	2	2791	6
2797	2	2801	3	2803	2	2819	2	2833	5	2837	2	2843	2	2851	2	2857	11
2861	2	2879	7	2887	5	2897	3	2903	5	2909	2	2917	5	2927	5	2939	2
2953	13	2957	2	2963	2	2969	3	2971	10	2999	17	3001	14	3011	2	3019	2
3023	5	3037	2	3041	3	3049	11	3061	6	3067	2	3079	6	3083	2	3089	3
3109	6	3119	7	3121	7	3137	3	3163	3	3167	5	3169	7	3181	7	3187	2
3191	11	3203	2	3209	3	3217	5	3221	10	3229	6	3251	6	3253	2	3257	3
3259	3	3271	3	3299	2	3301	6	3307	2	3313	10	3319	6	3323	2	3329	3
3331	3	3343	5	3347	2	3359	11	3361	22	3371	2	3373	5	3389	3	3391	3
3407	5	3413	2	3433	5	3449	3	3457	7	3461	2	3463	3	3467	2	3469	2
3491	2	3499	2	3511	7	3517	2	3527	5	3529	17	3533	2	3539	2	3541	7
3547	2	3557	2	3559	3	3571	2	3581	2	3583	3	3593	3	3607	5	3613	2
3617	3	3623	5	3631	15	3637	2	3643	2	3659	2	3671	13	3673	5	3677	2
3691	2	3697	5	3701	2	3709	2	3719	7	3727	3	3733	2	3739	7	3761	3
3767	5	3769	7	3779	2	3793	5	3797	2	3803	2	3821	3	3823	3	3833	3
3847	5	3851	2	3853	2	3863	5	3877	2	3881	13	3889	11	3907	2	3911	13
3917	2	3919	3	3923	2	3929	3	3931	2	3943	3	3947	2	3967	6	3989	2
4001	3	4003	2	4007	5	4013	2	4019	2	4021	2	4027	3	4049	3	4051	10
4057	5	4073	3	4079	11	4091	2	4093	2	4099	2	4111	12	4127	5	4129	13
4133	2	4139	2	4153	5	4157	2	4159	3	4177	5	4201	11	4211	6	4217	3
4219	2	4229	2	4231	3	4241	3	4243	2	4253	2	4259	2	4261	2	4271	7
4273	5	4283	2	4289	3	4297	5	4327	3	4337	3	4339	10	4349	2	4357	2
4363	2	4373	2	4391	14	4397	2	4409	3	4421	3	4423	3	4441	21	4447	3
4451	2	4457	3	4463	5	4481	3	4483	2	4493	2	4507	2	4513	7	4517	2
4519	3	4523	5	4547	2	4549	6	4561	11	4567	3	4583	5	4591	11	4597	5
4603	2	4621	2	4637	2	4639	3	4643	5	4649	3	4651	3	4657	15	4663	3
4673	3	4679	11	4691	2	4703	5	4721	6	4723	2	4729	17	4733	5	4751	19
4759	3	4783	6	4787	2	4789	2	4793	3	4799	7	4801	7	4813	2	4817	3
4831	3	4861	11	4871	11	4877	2	4889	3	4903	3	4909	6	4919	13	4931	6
4933	2	4937	3	4943	7	4951	6	4957	2	4967	5	4969	11	4973	2	4987	2
4993	5	4999	3	5003	2	5009	3	5011	2	5021	3	5023	3	5039	11	5051	2
5059	2	5077	2	5081	3	5087	5	5099	2	5101	6	5107	2	5113	19	5119	3
5147	2	5153	5	5167	6	5171	2	5179	2	5189	2	5197	7	5209	17	5227	2
5231	7	5233	10	5237	3	5261	2	5273	3	5279	7	5281	7	5297	3	5303	5
5309	2	5323	5	5333	2	5347	3	5351	11	5381	3	5387	2	5393	3	5399	7
5407	3	5413	5	5417	3	5419	3	5431	3	5437	5	5441	3	5443	2	5449	7
5471	7	5477	2	5479	3	5483	2	5501	2	5503	3	5507	2	5519	13	5521	11
5527	5	5531	10	5557	2	5563	2	5569	13	5573	2	5581	6	5591	11	5623	5
5639	7	5641	14	5647	3	5651	2	5653	5	5657	3	5659	2	5669	3	5683	2
5689	11	5693	2	5701	2	5711	19	5717	2	5737	5	5741	2	5743	10	5749	2
5779	2	5783	7	5791	6	5801	3	5807	5	5813	2	5821	6	5827	2	5839	6
5843	2	5849	3	5851	2	5857	7	5861	3	5867	5	5869	2	5879	11	5881	31

p	ω	p	ω	p	ω	p	ω	p	ω	p	ω	p	ω	p	ω
5897	3	5903	5	5923	2	5927	5	5939	2	5953	7	5981	3	5987	2	6007	3
6011	2	6029	2	6037	5	6043	5	6047	5	6053	2	6067	2	6073	10	6079	17
6089	3	6091	7	6101	2	6113	3	6121	7	6131	2	6133	5	6143	5	6151	3
6163	3	6173	2	6197	2	6199	3	6203	2	6211	2	6217	5	6221	3	6229	2
6247	5	6257	3	6263	5	6269	2	6271	11	6277	2	6287	7	6299	2	6301	10
6311	7	6317	2	6323	2	6329	3	6337	10	6343	3	6353	3	6359	13	6361	19
6367	3	6373	2	6379	2	6389	2	6397	2	6421	6	6427	3	6449	3	6451	3
6469	2	6473	3	6481	7	6491	2	6521	6	6529	7	6547	2	6551	17	6553	10
6563	5	6569	3	6571	3	6577	5	6581	14	6599	13	6607	3	6619	2	6637	2
6653	2	6659	2	6661	6	6673	5	6679	7	6689	3	6691	2	6701	2	6703	5
6709	2	6719	11	6733	2	6737	3	6761	3	6763	2	6779	2	6781	2	6791	7
6793	10	6803	2	6823	3	6827	2	6829	2	6833	3	6841	22	6857	3	6863	5
6869	2	6871	3	6883	2	6899	2	6907	2	6911	7	6917	2	6947	2	6949	2
6959	7	6961	13	6967	5	6971	2	6977	3	6983	5	6991	6	6997	5	7001	3
7013	2	7019	2	7027	2	7039	3	7043	2	7057	5	7069	2	7079	7	7103	5
7109	2	7121	3	7127	5	7129	7	7151	7	7159	3	7177	10	7187	2	7193	3
7207	3	7211	2	7213	5	7219	2	7229	2	7237	2	7243	2	7247	5	7253	2
7283	2	7297	5	7307	2	7309	6	7321	7	7331	2	7333	6	7349	2	7351	6
7369	7	7393	5	7411	2	7417	5	7433	3	7451	2	7457	3	7459	2	7477	2
7481	6	7487	5	7489	7	7499	2	7507	2	7517	2	7523	2	7529	3	7537	7
7541	2	7547	2	7549	2	7559	13	7561	13	7573	2	7577	3	7583	5	7589	2
7591	6	7603	2	7607	5	7621	2	7639	7	7643	2	7649	3	7669	2	7673	3
7681	17	7687	6	7691	2	7699	3	7703	5	7717	2	7723	3	7727	5	7741	7
7753	10	7757	2	7759	3	7789	2	7793	3	7817	3	7823	5	7829	2	7841	12
7853	2	7867	3	7873	5	7877	2	7879	3	7883	2	7901	2	7907	2	7919	7
7927	3	7933	2	7937	3	7949	2	7951	6	7963	5	7993	5	8009	3	8011	14
8017	5	8039	11	8053	2	8059	3	8069	2	8081	3	8087	5	8089	17	8093	2
8101	6	8111	11	8117	2	8123	2	8147	2	8161	7	8167	3	8171	2	8179	2
8191	17	8209	7	8219	2	8221	2	8231	11	8233	10	8237	2	8243	2	8263	3
8269	2	8273	3	8287	3	8291	2	8293	2	8297	3	8311	3	8317	6	8329	7
8353	5	8363	2	8369	3	8377	5	8387	2	8389	6	8419	3	8423	5	8429	2
8431	3	8443	2	8447	5	8461	6	8467	2	8501	7	8513	5	8521	13	8527	5
8537	3	8539	2	8543	5	8563	2	8573	2	8581	6	8597	2	8599	3	8609	3
8623	3	8627	2	8629	6	8641	17	8647	3	8663	5	8669	2	8677	2	8681	15
8689	13	8693	2	8699	2	8707	5	8713	5	8719	3	8731	2	8737	5	8741	2
8747	2	8753	3	8761	23	8779	11	8783	5	8803	2	8807	5	8819	2	8821	2
8831	7	8837	2	8839	3	8849	3	8861	2	8863	3	8867	2	8887	3	8893	5
8923	2	8929	11	8933	2	8941	6	8951	13	8963	2	8969	3	8971	2	8999	7
9001	7	9007	3	9011	2	9013	5	9029	2	9041	3	9043	3	9049	7	9059	2
9067	3	9091	3	9103	6	9109	10	9127	3	9133	6	9137	3	9151	3	9157	6
9161	3	9173	2	9181	2	9187	3	9199	3	9203	2	9209	3	9221	2	9227	2
9239	19	9241	13	9257	3	9277	5	9281	3	9283	2	9293	2	9311	7	9319	3
9323	2	9337	5	9341	2	9343	5	9349	2	9371	2	9377	3	9391	3	9397	2
9403	3	9413	3	9419	2	9421	2	9431	7	9433	5	9437	2	9439	22	9461	3
9463	3	9467	2	9473	3	9479	7	9491	2	9497	3	9511	3	9521	3	9533	2
9539	2	9547	2	9551	11	9587	2	9601	13	9613	2	9619	2	9623	5	9629	2
9631	3	9643	2	9649	7	9661	2	9677	2	9679	3	9689	3	9697	10	9719	17
9721	7	9733	2	9739	3	9743	5	9749	2	9767	5	9769	13	9781	6	9787	3
9791	11	9803	2	9811	3	9817	5	9829	10	9833	3	9839	7	9851	2	9857	5
9859	2	9871	3	9883	2	9887	5	9901	2	9907	2	9923	2	9929	3	9931	10
9941	2	9949	2	9967	3	9973	11										

8.3 **Conjecture** (Artin) 2 is an primitive root for infinitely many primes.

8.4 **Theorem** [995] For any three distinct primes p, q, and r, at least one of p, q, or r is a primitive root for infinitely many primes.

8.5 Let S denote a finite set of primes. If N represents the product of the elements of S, then the integer x, $1 < x \leq N-1$ is a *common primitive root* of the elements of S if and only if for each $p \in S$, x is congruent to $\omega \pmod{p}$ where ω is a primitive root of p.

8.6 **Remark** The number of common primitive roots equals $\prod_{p \in S} \phi(p-1)$ where ϕ is the Euler ϕ-function (§8.2).

8.7 **Table** Table of (all) common primitive roots for $S = \{p, q\}$ with $1 < p, q \leq 19$.

p	q	Common Primitive Roots
3	5	2 8
3	7	5 17
3	11	2 8 17 29
3	13	2 11 20 32
3	17	5 11 14 20 23 29 41 44
3	19	2 14 29 32 41 53
5	7	3 12 17 33
5	11	2 7 8 13 17 18 28 52
5	13	2 7 28 32 33 37 58 63
5	17	3 7 12 22 23 27 28 37 48 57 58 62 63 73 78 82
5	19	2 3 13 22 32 33 48 52 53 67 72 78
7	11	17 19 24 40 52 61 68 73
7	13	19 24 33 45 54 59 80 89
7	17	3 5 10 12 24 31 40 45 54 61 73 75 80 82 96 108
7	19	3 10 33 40 52 59 89 108 110 117 124 129
11	13	2 6 7 19 24 28 41 46 50 63 72 84 85 106 123 128
11	17	6 7 24 28 29 39 40 41 46 57 61 62 63 73 74 79 90 95 96 105 107 112 116 129 139 150 156 160 167 173 182 184
11	19	2 13 29 40 41 51 52 72 79 90 105 116 117 127 128 129 162 167 173 184 193 200 204 205
13	17	6 7 11 20 24 28 37 41 45 46 54 58 63 71 80 97 124 141 150 158 163 167 175 176 180 184 193 197 201 210 214 215
13	19	2 15 32 33 41 59 67 71 72 89 97 98 110 124 128 136 154 162 167 184 193 219 223 241
17	19	3 10 14 22 29 40 41 48 71 78 79 90 91 97 105 108 109 116 124 129 143 146 147 148 165 167 173 181 184 192 193 211 224 231 241 243 249 250 260 261 262 269 279 295 299 300 317 318

8.8 **Table** The least common primitive root ω for pairs of primes $p, q < 50$, with $q > 19$.

$q \backslash p$	3	5	7	11	13	17	19	23	29	31	37	41	43
23	5	7	5	7	7	5	10						
29	2	2	3	2	2	3	2	10					
31	11	3	3	13	11	3	3	11	3				
37	2	2	5	2	2	5	2	5	2	3			
41	11	7	12	6	6	6	13	7	11	11	13		
43	5	3	3	18	9	3	3	5	3	3	5	12	
47	5	13	5	13	11	5	10	5	10	11	5	11	5

8.2 Number Theoretic Functions

8.9 The Euler $\phi(n)$ function denotes the number of positive integers less than n that are relatively prime to n.

8.10 **Theorems** Elementary theorems concerning $\phi(n)$.

1. $\phi(p) = p - 1$ for any prime p.
2. $\phi(ab) = \phi(a) \times \phi(b)$ if a and b are relatively prime.
3. If $n > 1$, then $\phi(n) = n \prod_{p|n}(1 - 1/p)$.
4. For $n \geq 1$, $\sum_{d|n} \phi(d) = n$.
5. If a and n are relatively prime, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

8.11 $\sigma_k(n)$ is the sum of the kth powers of the positive divisors of n.
$\sigma(n) = \sigma_1(n)$ is the sum of the positive divisors of n.
$\tau(n) = \sigma_0(n)$ is the number of positive divisors of n.

8.12 **Theorems** Elementary theorems concerning σ and τ.

1. If p is prime, then $\sigma(p) = p + 1$ and $\tau(p) = 2$.
2. If a and b are relatively prime, then $\sigma(ab) = \sigma(a) \times \sigma(b)$ and $\tau(ab) = \tau(a) \times \tau(b)$.
3. If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then
   (a) $\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$, and
   (b) $\sigma(n) = \prod_i^r \frac{p_i^{e_i+1} - 1}{p_i - 1}$.

8.13 The *Möbius function* $\mu(n)$ is

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } a^2 | n \text{ for some } a > 1 \\ (-1)^r & if n = p_1 p_2 \cdots p_r, \text{ distinct prime factors} \end{cases}$$

8.14 **Theorems** Elementary theorems concerning μ.

1. $\mu(p) = -1$ for any prime p.
2. $\mu(ab) = \mu(a) \times \mu(b)$ if a and b are relatively prime.
3. If $n > 1$, then $\sum_{d|n} \mu(d) = 0$.
4. (*Möbius inversion formula*) If $F(n) = \sum_{d|n} f(d)$ for every positive integer n, then $f(n) = \sum_{d|n} \mu(d) F(n/d)$.

8.15 **Table** Values of $\phi(n), \sigma(n), \tau(n),$ and $\mu(n)$ for $1 \leq n \leq 500$.

n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ
1	1	1	1	1	2	1	3	2	-1	3	2	4	2	-1	4	2	7	3	0	5	4	6	2	-1
6	2	12	4	1	7	6	8	2	-1	8	4	15	4	0	9	6	13	3	0	10	4	18	4	1
11	10	12	2	-1	12	4	28	6	0	13	12	14	2	-1	14	6	24	4	1	15	8	24	4	1
16	8	31	5	0	17	16	18	2	-1	18	6	39	6	0	19	18	20	2	-1	20	8	42	6	0
21	12	32	4	1	22	10	36	4	1	23	22	24	2	-1	24	8	60	8	0	25	20	31	3	0
26	12	42	4	1	27	18	40	4	0	28	12	56	6	0	29	28	30	2	-1	30	8	72	8	-1
31	30	32	2	-1	32	16	63	6	0	33	20	48	4	1	34	16	54	4	1	35	24	48	4	1
36	12	91	9	0	37	36	38	2	-1	38	18	60	4	1	39	24	56	4	1	40	16	90	8	0
41	40	42	2	-1	42	12	96	8	-1	43	42	44	2	-1	44	20	84	6	0	45	24	78	6	0
46	22	72	4	1	47	46	48	2	-1	48	16	124	10	0	49	42	57	3	0	50	20	93	6	0
51	32	72	4	1	52	24	98	6	0	53	52	54	2	-1	54	18	120	8	0	55	40	72	4	1
56	24	120	8	0	57	36	80	4	1	58	28	90	4	1	59	58	60	2	-1	60	16	168	12	0
61	60	62	2	-1	62	30	96	4	1	63	36	104	6	0	64	32	127	7	0	65	48	84	4	1
66	20	144	8	-1	67	66	68	2	-1	68	32	126	6	0	69	44	96	4	1	70	24	144	8	-1
71	70	72	2	-1	72	24	195	12	0	73	72	74	2	-1	74	36	114	4	1	75	40	124	6	0
76	36	140	6	0	77	60	96	4	1	78	24	168	8	-1	79	78	80	2	-1	80	32	186	10	0

n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ
81	54	121	5	0	82	40	126	4	1	83	82	84	2	-1	84	24	224	12	0	85	64	108	4	1
86	42	132	4	1	87	56	120	4	1	88	40	180	8	0	89	88	90	2	-1	90	24	234	12	0
91	72	112	4	1	92	44	168	6	0	93	60	128	4	1	94	46	144	4	1	95	72	120	4	1
96	32	252	12	0	97	96	98	2	-1	98	42	171	6	0	99	60	156	6	0	100	40	217	9	0
101	100	102	2	-1	102	32	216	8	-1	103	102	104	2	-1	104	48	210	8	0	105	48	192	8	-1
106	52	162	4	1	107	106	108	2	-1	108	36	280	12	0	109	108	110	2	-1	110	40	216	8	-1
111	72	152	4	1	112	48	248	10	0	113	112	114	2	-1	114	36	240	8	-1	115	88	144	4	1
116	56	210	6	0	117	72	182	6	0	118	58	180	4	1	119	96	144	4	1	120	32	360	16	0
121	110	133	3	0	122	60	186	4	1	123	80	168	4	1	124	60	224	6	0	125	100	156	4	0
126	36	312	12	0	127	126	128	2	-1	128	64	255	8	0	129	84	176	4	1	130	48	252	8	-1
131	130	132	2	-1	132	40	336	12	0	133	108	160	4	1	134	66	204	4	1	135	72	240	8	0
136	64	270	8	0	137	136	138	2	-1	138	44	288	8	-1	139	138	140	2	-1	140	48	336	12	0
141	92	192	4	1	142	70	216	4	1	143	120	168	4	1	144	48	403	15	0	145	112	180	4	1
146	72	222	4	1	147	84	228	6	0	148	72	266	6	0	149	148	150	2	-1	150	40	372	12	0
151	150	152	2	-1	152	72	300	8	0	153	96	234	6	0	154	60	288	8	-1	155	120	192	4	1
156	48	392	12	0	157	156	158	2	-1	158	78	240	4	1	159	104	216	4	1	160	64	378	12	0
161	132	192	4	1	162	54	363	10	0	163	162	164	2	-1	164	80	294	6	0	165	80	288	8	-1
166	82	252	4	1	167	166	168	2	-1	168	48	480	16	0	169	156	183	3	0	170	64	324	8	-1
171	108	260	6	0	172	84	308	6	0	173	172	174	2	-1	174	56	360	8	-1	175	120	248	6	0
176	80	372	10	0	177	116	240	4	1	178	88	270	4	1	179	178	180	2	-1	180	48	546	18	0
181	180	182	2	-1	182	72	336	8	-1	183	120	248	4	1	184	88	360	8	0	185	144	228	4	1
186	60	384	8	-1	187	160	216	4	1	188	92	336	6	0	189	108	320	8	0	190	72	360	8	-1
191	190	192	2	-1	192	64	508	14	0	193	192	194	2	-1	194	96	294	4	1	195	96	336	8	-1
196	84	399	9	0	197	196	198	2	-1	198	60	468	12	0	199	198	200	2	-1	200	80	465	12	0
201	132	272	4	1	202	100	306	4	1	203	168	240	4	1	204	64	504	12	0	205	160	252	4	1
206	102	312	4	1	207	132	312	6	0	208	96	434	10	0	209	180	240	4	1	210	48	576	16	1
211	210	212	2	-1	212	104	378	6	0	213	140	288	4	1	214	106	324	4	1	215	168	264	4	1
216	72	600	16	0	217	180	256	4	1	218	108	330	4	1	219	144	296	4	1	220	80	504	12	0
221	192	252	4	1	222	72	456	8	-1	223	222	224	2	-1	224	96	504	12	0	225	120	403	9	0
226	112	342	4	1	227	226	228	2	-1	228	72	560	12	0	229	228	230	2	-1	230	88	432	8	-1
231	120	384	8	-1	232	112	450	8	0	233	232	234	2	-1	234	72	546	12	0	235	184	288	4	1
236	116	420	6	0	237	156	320	4	1	238	96	432	8	-1	239	238	240	2	-1	240	64	744	20	0
241	240	242	2	-1	242	110	399	6	0	243	162	364	6	0	244	120	434	6	0	245	168	342	6	0
246	80	504	8	-1	247	216	280	4	1	248	120	480	8	0	249	164	336	4	1	250	100	468	8	0
251	250	252	2	-1	252	72	728	18	0	253	220	288	4	1	254	126	384	4	1	255	128	432	8	-1
256	128	511	9	0	257	256	258	2	-1	258	84	528	8	-1	259	216	304	4	1	260	96	588	12	0
261	168	390	6	0	262	130	396	4	1	263	262	264	2	-1	264	80	720	16	0	265	208	324	4	1
266	108	480	8	-1	267	176	360	4	1	268	132	476	6	0	269	268	270	2	-1	270	72	720	16	0
271	270	272	2	-1	272	128	558	10	0	273	144	448	8	-1	274	136	414	4	1	275	200	372	6	0
276	88	672	12	0	277	276	278	2	-1	278	138	420	4	1	279	180	416	6	0	280	96	720	16	0
281	280	282	2	-1	282	92	576	8	-1	283	282	284	2	-1	284	140	504	6	0	285	144	480	8	-1
286	120	504	8	-1	287	240	336	4	1	288	96	819	18	0	289	272	307	3	0	290	112	540	8	-1
291	192	392	4	1	292	144	518	6	0	293	292	294	2	-1	294	84	684	12	0	295	232	360	4	1
296	144	570	8	0	297	180	480	8	0	298	148	450	4	1	299	264	336	4	1	300	80	868	18	0
301	252	352	4	1	302	150	456	4	1	303	200	408	4	1	304	144	620	10	0	305	240	372	4	1
306	96	702	12	0	307	306	308	2	-1	308	120	672	12	0	309	204	416	4	1	310	120	576	8	-1
311	310	312	2	-1	312	96	840	16	0	313	312	314	2	-1	314	156	474	4	1	315	144	624	12	0
316	156	560	6	0	317	316	318	2	-1	318	104	648	8	-1	319	280	360	4	1	320	128	762	14	0
321	212	432	4	1	322	132	576	8	-1	323	288	360	4	1	324	108	847	15	0	325	240	434	6	0
326	162	492	4	1	327	216	440	4	1	328	160	630	8	0	329	276	384	4	1	330	80	864	16	1
331	330	332	2	-1	332	164	588	6	0	333	216	494	6	0	334	166	504	4	1	335	264	408	4	1
336	96	992	20	0	337	336	338	2	-1	338	156	549	6	0	339	224	456	4	1	340	128	756	12	0
341	300	384	4	1	342	108	780	12	0	343	294	400	4	0	344	168	660	8	0	345	176	576	8	-1
346	172	522	4	1	347	346	348	2	-1	348	112	840	12	0	349	348	350	2	-1	350	120	744	12	0
351	216	560	8	0	352	160	756	12	0	353	352	354	2	-1	354	116	720	8	-1	355	280	432	4	1
356	176	630	6	0	357	192	576	8	-1	358	178	540	4	1	359	358	360	2	-1	360	96	1170	24	0

n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ	n	ϕ	σ	τ	μ
361	342	381	3	0	362	180	546	4	1	363	220	532	6	0	364	144	784	12	0	365	288	444	4	1
366	120	744	8	-1	367	366	368	2	-1	368	176	744	10	0	369	240	546	6	0	370	144	684	8	-1
371	312	432	4	1	372	120	896	12	0	373	372	374	2	-1	374	160	648	8	-1	375	200	624	8	0
376	184	720	8	0	377	336	420	4	1	378	108	960	16	0	379	378	380	2	-1	380	144	840	12	0
381	252	512	4	1	382	190	576	4	1	383	382	384	2	-1	384	128	1020	16	0	385	240	576	8	-1
386	192	582	4	1	387	252	572	6	0	388	192	686	6	0	389	388	390	2	-1	390	96	1008	16	1
391	352	432	4	1	392	168	855	12	0	393	260	528	4	1	394	196	594	4	1	395	312	480	4	1
396	120	1092	18	0	397	396	398	2	-1	398	198	600	4	1	399	216	640	8	-1	400	160	961	15	0
401	400	402	2	-1	402	132	816	8	-1	403	360	448	4	1	404	200	714	6	0	405	216	726	10	0
406	168	720	8	-1	407	360	456	4	1	408	128	1080	16	0	409	408	410	2	-1	410	160	756	8	-1
411	272	552	4	1	412	204	728	6	0	413	348	480	4	1	414	132	936	12	0	415	328	504	4	1
416	192	882	12	0	417	276	560	4	1	418	180	720	8	-1	419	418	420	2	-1	420	96	1344	24	0
421	420	422	2	-1	422	210	636	4	1	423	276	624	6	0	424	208	810	8	0	425	320	558	6	0
426	140	864	8	-1	427	360	496	4	1	428	212	756	6	0	429	240	672	8	-1	430	168	792	8	-1
431	430	432	2	-1	432	144	1240	20	0	433	432	434	2	-1	434	180	768	8	-1	435	224	720	8	-1
436	216	770	6	0	437	396	480	4	1	438	144	888	8	-1	439	438	440	2	-1	440	160	1080	16	0
441	252	741	9	0	442	192	756	8	-1	443	442	444	2	-1	444	144	1064	12	0	445	352	540	4	1
446	222	672	4	1	447	296	600	4	1	448	192	1016	14	0	449	448	450	2	-1	450	120	1209	18	0
451	400	504	4	1	452	224	798	6	0	453	300	608	4	1	454	226	684	4	1	455	288	672	8	-1
456	144	1200	16	0	457	456	458	2	-1	458	228	690	4	1	459	288	720	8	0	460	176	1008	12	0
461	460	462	2	-1	462	120	1152	16	1	463	462	464	2	-1	464	224	930	10	0	465	240	768	8	-1
466	232	702	4	1	467	466	468	2	-1	468	144	1274	18	0	469	396	544	4	1	470	184	864	8	-1
471	312	632	4	1	472	232	900	8	0	473	420	528	4	1	474	156	960	8	-1	475	360	620	6	0
476	192	1008	12	0	477	312	702	6	0	478	238	720	4	1	479	478	480	2	-1	480	128	1512	24	0
481	432	532	4	1	482	240	726	4	1	483	264	768	8	-1	484	220	931	9	0	485	384	588	4	1
486	162	1092	12	0	487	486	488	2	-1	488	240	930	8	0	489	324	656	4	1	490	168	1026	12	0
491	490	492	2	-1	492	160	1176	12	0	493	448	540	4	1	494	216	840	8	-1	495	240	936	12	0
496	240	992	10	0	497	420	576	4	1	498	164	1008	8	-1	499	498	500	2	-1	500	200	1092	12	0

8.16 Table Inverse of the Euler ϕ-function.

x	Integers n for which $\phi(n) = x$	x	Integers n for which $\phi(n) = x$
1	1, 2	2	3, 4, 6
4	5, 8, 10, 12	6	7, 9, 14, 18
8	15, 16, 20, 24, 30	10	11, 22
12	13, 21, 26, 28, 36, 42	16	17, 32, 34, 40, 48, 60
18	19, 27, 38, 54	20	25, 33, 44, 50, 66
22	23, 46	24	35, 39, 45, 52, 56, 70, 72, 78, 84, 90
28	29, 58	30	31, 62
32	51, 64, 68, 80, 96, 102, 120	36	37, 57, 63, 74, 76, 108, 114, 126
40	41, 55, 75, 82, 88, 100, 110, 132, 150	42	43, 49, 86, 98
44	69, 92, 138	46	47, 94
48	65, 104, 105, 112, 130, 140, 144, 156, 168, 180, 210	52	53, 106
54	81, 162	56	87, 116, 174
58	59, 118	60	61, 77, 93, 99, 122, 124, 154, 186, 198
64	85, 128, 136, 160, 170, 192, 204, 240	66	67, 134
70	71, 142	72	73, 91, 95, 111, 117, 135, 146, 148, 152, 182, 190, 216, 222, 228, 234, 252, 270
78	79, 158	80	123, 164, 165, 176, 200, 220, 246, 264, 300, 330
82	83, 166	84	129, 147, 172, 196, 258, 294
88	89, 115, 178, 184, 230, 276	92	141, 188, 282
96	97, 119, 153, 194, 195, 208, 224, 238, 260, 280, 288, 306, 312, 336, 360, 390, 420	100	101, 125, 202, 250

8.17 $\pi(n)$ is the number of primes $p \le n$.
p_n denotes the nth prime. ($p_1 = 2, p_2 = 3, p_3 = 5 \ldots$)

8.18 **Theorem** (prime number theorem) $\lim_{n\to\infty} \frac{\pi(n)}{n/\log n} = 1$.

8.19 **Theorems** Bounds on $\pi(x)$ [1827].

1. $\frac{x}{\log x}(1 + \frac{1}{2\log x}) < \pi(x) < \frac{x}{\log x}(1 + \frac{3}{2\log x})$ if $x \ge 59$.
2. $x/(\log x - \frac{1}{2}) < \pi(x) < x/(\log x - \frac{3}{2})$ if $x \ge 67$.
3. $x/\log x < \pi(x) < 1.25x/\log x$ if $x \ge 17,\ x \ne 113$.

8.20 **Theorems** Other bounds [1827].

1. $n(\log n + \log\log n - \frac{3}{2}) < p_n < n(\log n + \log\log n - \frac{1}{2})$ if $n \ge 20$.
2. $\log\log x + B - 1/(2\log^2 x) < \sum_{p\le x} 1/p < \log\log x + B + 1/(2\log^2 x)$ if $x \ge 286$ where $B \approx 0.261497212847643$.
3. $\log x + E - 1/(2\log x) < \sum_{p\le x} (\log p)/p < \log x + E + 1/(2\log x)$ if $x > 319$ where $E \approx -1.332582275733221$.

8.21 If p denotes an odd prime and $\gcd(a,p) = 1$, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is 1 if a is a quadratic residue ($x^2 \equiv a \pmod p$), and -1 if a is a quadratic nonresidue mod p.

8.22 **Theorems** Let p and q be distinct odd primes, then

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$;
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;
3. if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
4. (*quadratic reciprocity*) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{[(p-1)/2][(q-1)/2]}$.

8.3 Table of Indices for Primes

8.23 **Table** For each prime $p \le 113$ two tables are given. Let g be least primitive element of the group $\mathbb{F}_p^*$ and assume $g^x = y$. The table on the left has a y in position x, while the one on the right has an x in position y.

3

N	0	1	2	3	4	5	6	7	8	9
0		2	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	1							

5

N	0	1	2	3	4	5	6	7	8	9
0		4	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3	1					

7

N	0	1	2	3	4	5	6	7	8	9
0		6	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5	1			

11

N	0	1	2	3	4	5	6	7	8	9
0		10	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1	1									

13

N	0	1	2	3	4	5	6	7	8	9
0		12	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7	1							

17

N	0	1	2	3	4	5	6	7	8	9
0		16	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6	1			

19

N	0	1	2	3	4	5	6	7	8	9
0		18	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10	1	

23

N	0	1	2	3	4	5	6	7	8	9
0		22	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14	1							

29

N	0	1	2	3	4	5	6	7	8	9
0		28	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15	1	

31

N	0	1	2	3	4	5	6	7	8	9
0		30	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21
3	1									

37

N	0	1	2	3	4	5	6	7	8	9
0		36	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19	1			

41

N	0	1	2	3	4	5	6	7	8	9
0		40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7
4	1									

43

N	0	1	2	3	4	5	6	7	8	9
0		42	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29	1							

47

N	0	1	2	3	4	5	6	7	8	9
0		46	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19	1			

53

N	0	1	2	3	4	5	6	7	8	9
0		52	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27	1							

59

N	0	1	2	3	4	5	6	7	8	9
0		58	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30	1	

61

N	0	1	2	3	4	5	6	7	8	9
0		60	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31
6	1									

67

N	0	1	2	3	4	5	6	7	8	9
0		66	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34	1			

71

N	0	1	2	3	4	5	6	7	8	9
0		70	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61
7	1									

73

N	0	1	2	3	4	5	6	7	8	9
0		72	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44	1							

79

N	0	1	2	3	4	5	6	7	8	9
0		78	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53	1	

83

N	0	1	2	3	4	5	6	7	8	9
0		82	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42	1							

89

N	0	1	2	3	4	5	6	7	8	9
0		88	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30	1	

97

N	0	1	2	3	4	5	6	7	8	9
0		96	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39	1			

101

N	0	1	2	3	4	5	6	7	8	9
0		100	1	69	2	24	70	9	3	38
1	25	13	71	66	10	93	4	30	39	96
2	26	78	14	86	72	48	67	7	11	91
3	94	84	5	82	31	33	40	56	97	35
4	27	45	79	42	15	62	87	58	73	18
5	49	99	68	23	8	37	12	65	92	29
6	95	77	85	47	6	90	83	81	32	55
7	34	44	41	61	57	17	98	22	36	64
8	28	76	46	89	80	54	43	60	16	21
9	63	75	88	53	59	20	74	52	19	51
10	50									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	27	54	7
1	14	28	56	11	22	44	88	75	49	98
2	95	89	77	53	5	10	20	40	80	59
3	17	34	68	35	70	39	78	55	9	18
4	36	72	43	86	71	41	82	63	25	50
5	100	99	97	93	85	69	37	74	47	94
6	87	73	45	90	79	57	13	26	52	3
7	6	12	24	48	96	91	81	61	21	42
8	84	67	33	66	31	62	23	46	92	83
9	65	29	58	15	30	60	19	38	76	51
10	1									

103

N	0	1	2	3	4	5	6	7	8	9
0		102	44	39	88	1	83	4	30	78
1	45	61	25	72	48	40	74	70	20	80
2	89	43	3	24	69	2	14	15	92	86
3	84	57	16	100	12	5	64	93	22	9
4	31	50	87	77	47	79	68	85	11	8
5	46	7	58	97	59	62	34	17	28	98
6	26	36	101	82	60	73	42	13	56	63
7	49	67	6	33	35	41	66	65	53	18
8	75	54	94	38	29	71	19	23	91	99
9	21	76	10	96	27	81	55	32	52	37
10	90	95	51							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	22	7	35	72	51	49	39
1	92	48	34	67	26	27	32	57	79	86
2	18	90	38	87	23	12	60	94	58	84
3	8	40	97	73	56	74	61	99	83	3
4	15	75	66	21	2	10	50	44	14	70
5	41	102	98	78	81	96	68	31	52	54
6	64	11	55	69	36	77	76	71	46	24
7	17	85	13	65	16	80	91	43	9	45
8	19	95	63	6	30	47	29	42	4	20
9	100	88	28	37	82	101	93	53	59	89
10	33	62	1							

107

N	0	1	2	3	4	5	6	7	8	9
0		106	1	70	2	47	71	43	3	34
1	48	22	72	14	44	11	4	29	35	78
2	49	7	23	62	73	94	15	104	45	32
3	12	27	5	92	30	90	36	38	79	84
4	50	40	8	59	24	81	63	66	74	86
5	95	99	16	52	105	69	46	42	33	21
6	13	10	28	77	6	61	93	103	31	26
7	91	89	37	83	39	58	80	65	85	98
8	51	68	41	20	9	76	60	102	25	88
9	82	57	64	97	67	19	75	101	87	56
10	96	18	100	55	17	54	53			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	21	42	84
1	61	15	30	60	13	26	52	104	101	95
2	83	59	11	22	44	88	69	31	62	17
3	34	68	29	58	9	18	36	72	37	74
4	41	82	57	7	14	28	56	5	10	20
5	40	80	53	106	105	103	99	91	75	43
6	86	65	23	46	92	77	47	94	81	55
7	3	6	12	24	48	96	85	63	19	38
8	76	45	90	73	39	78	49	98	89	71
9	35	70	33	66	25	50	100	93	79	51
10	102	97	87	67	27	54	1			

109

N	0	1	2	3	4	5	6	7	8	9
0		108	57	52	6	76	1	40	63	104
1	25	83	58	67	97	20	12	93	53	75
2	82	92	32	33	7	44	16	48	46	34
3	77	14	69	27	42	8	2	5	24	11
4	31	45	41	30	89	72	90	17	64	80
5	101	37	73	49	105	51	103	19	91	47
6	26	10	71	36	18	35	84	95	99	85
7	65	78	59	56	62	96	81	15	68	23
8	88	100	102	70	98	61	87	86	38	28
9	21	107	39	66	74	43	13	4	29	79
10	50	9	94	55	22	60	106	3	54	

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	107	97	37	4	24	35	101
1	61	39	16	96	31	77	26	47	64	57
2	15	90	104	79	38	10	60	33	89	98
3	43	40	22	23	29	65	63	51	88	92
4	7	42	34	95	25	41	28	59	27	53
5	100	55	3	18	108	103	73	2	12	72
6	105	85	74	8	48	70	93	13	78	32
7	83	62	45	52	94	19	5	30	71	99
8	49	76	20	11	66	69	87	86	80	44
9	46	58	21	17	102	67	75	14	84	68
10	81	50	82	56	9	54	106	91	1	

113

N	0	1	2	3	4	5	6	7	8	9
0		112	12	1	24	83	13	8	36	2
1	95	74	25	22	20	84	48	5	14	99
2	107	9	86	41	37	54	34	3	32	89
3	96	50	60	75	17	91	26	67	111	23
4	7	94	21	47	98	85	53	31	49	16
5	66	6	46	52	15	45	44	100	101	71
6	108	102	62	10	72	105	87	109	29	42
7	103	77	38	63	79	55	11	82	35	73
8	19	4	106	40	33	88	59	90	110	93
9	97	30	65	51	43	70	61	104	28	76
10	78	81	18	39	58	92	64	69	27	80
11	57	68	56							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	17	51	40	7	21
1	63	76	2	6	18	54	49	34	102	80
2	14	42	13	39	4	12	36	108	98	68
3	91	47	28	84	26	78	8	24	72	103
4	83	23	69	94	56	55	52	43	16	48
5	31	93	53	46	25	75	112	110	104	86
6	32	96	62	73	106	92	50	37	111	107
7	95	59	64	79	11	33	99	71	100	74
8	109	101	77	5	15	45	22	66	85	29
9	87	35	105	89	41	10	30	90	44	19
10	57	58	61	70	97	65	82	20	60	67
11	88	38	1							

8.4 Prime Powers

8.24 Table Prime powers $q = p^\alpha$, $q \le 10000$, $\alpha \ge 2$.

q	p	q	p	q	p	q	p	q	p	q	p	q	p	q	p	q	p
4	2	8	2	9	3	16	2	25	5	27	3	32	2	49	7	64	2
81	3	121	11	125	5	128	2	169	13	243	3	256	2	289	17	343	7
361	19	512	2	529	23	625	5	729	3	841	29	961	31	1024	2	1331	11
1369	37	1681	41	1849	43	2048	2	2187	3	2197	13	2209	47	2401	7	2809	53
3125	5	3481	59	3721	61	4096	2	4489	67	4913	17	5041	71	5329	73	6241	79
6561	3	6859	19	6889	83	7921	89	8192	2	9409	97						

8.5 Indices and Power Residues for Prime Power Fields

8.25 Remark In Tables 8.26, 8.27, 8.28, and 8.29, if g is a generator of $\mathbb{F}_{p^n}$ and if $g^u = v$, then u is in cell v of the array where the row and column indices are added to get the value of v.

8.26 Table Indices and power residues for $\mathbb{F}_{2^n}$, $n \le 7$.

$\mathbb{F}_{2^2}$, $g = x$

	000	001	010	011	100	101	110	111
0		3	1	2				

$\mathbb{F}_{2^3}$, $g = x$

	000	001	010	011	100	101	110	111
0		7	1	3	2	6	4	5

$\mathbb{F}_{2^4}$, $g = x + 1$

	000	001	010	011	100	101	110	111
0		15	12	1	9	2	13	7
1000	6	8	14	11	10	5	4	3

$\mathbb{F}_{2^5}$, $g = x$

	000	001	010	011	100	101	110	111
0		31	1	14	2	28	15	22
1000	3	5	29	26	16	7	23	11
10000	4	25	6	10	30	13	27	21
11000	17	18	8	19	24	9	12	20

$\mathbb{F}_{2^6}$, $g = x + 1$

	000	001	010	011	100	101	110	111
0		63	56	1	49	2	57	20
1000	42	21	58	25	50	53	13	3
10000	35	4	14	16	51	40	18	54
11000	43	37	46	22	6	26	59	31
100000	28	32	60	10	7	8	9	27
101000	44	29	33	38	11	23	47	61
110000	36	45	30	5	39	17	15	34
111000	62	55	19	48	52	12	24	41

$\mathbb{F}_{2^7}$
$g = x$

	000	001	010	011	100	101	110	111
0		127	1	89	2	51	90	59
1000	3	21	52	113	91	85	60	13
10000	4	102	22	95	53	118	114	47
11000	92	107	86	110	61	75	14	66
100000	5	28	103	17	23	122	96	37
101000	54	32	119	69	115	72	48	82
110000	93	45	108	64	87	57	111	11
111000	62	9	76	78	15	35	67	80
1000000	6	42	29	25	104	99	18	124
1001000	24	41	123	98	97	40	38	39
1010000	55	43	33	7	120	26	70	30
1011000	116	100	73	105	49	125	83	19
1100000	94	101	46	117	109	106	65	74
1101000	88	126	58	50	112	20	12	84
1110000	63	44	10	56	77	8	79	34
1111000	16	27	36	121	68	31	81	71

8.27 **Table** Indices and power residues for $\mathbb{F}_{3^n}$, $n \leq 4$.

$\mathbb{F}_{3^2}$
$g = x$

	00	01	02	10	11	12	20	21	22
0		8	4	1	2	7	5	3	6

$\mathbb{F}_{3^3}$
$g = x$

	00	01	02	10	11	12	20	21	22
0		26	13	1	19	4	14	17	6
100	2	22	23	20	8	24	5	12	3
200	15	10	9	18	16	25	7	11	21

$\mathbb{F}_{3^4}$
$g = x$

	00	01	02	10	11	12	20	21	22
0		80	40	1	15	49	41	9	55
100	2	37	64	16	18	13	50	30	60
200	42	24	77	10	20	70	56	53	58
1000	3	45	67	38	62	75	65	34	26
1100	17	29	36	19	52	23	14	8	79
1200	51	7	28	31	32	6	61	33	44
2000	43	27	5	25	66	74	78	35	22
2100	11	68	47	21	4	73	71	46	72
2200	57	76	69	54	39	48	59	63	12

8.28 **Table** Indices and power residues for $\mathbb{F}_{5^2}$.

$\mathbb{F}_{5^2}$
$g = x$

	00	01	02	03	04	10	11	12	13	14
0		24	6	18	12	1	17	14	15	10
20	7	21	23	16	20	19	8	4	11	9
40	13	22	3	2	5					

8.29 **Table** Indices and power residues for $\mathbb{F}_{7^2}$.

$\mathbb{F}_{7^2}$
$g = x$

	0	1	2	3	4	5	6
0		48	16	8	32	40	24
10	1	31	11	26	12	14	5
20	17	28	47	30	27	21	42
30	9	22	34	39	13	20	19
40	33	43	44	37	15	10	46
50	41	18	45	3	6	23	4
60	25	29	38	36	2	35	7

8.6 Prime Power Decompositions up to 2500

8.30 Table Integer factorizations of integers up to 2500 as products of prime powers. Prime numbers are shown in bold.

	0	1	2	3	4	5	6	7	8	9
0	0	1	**2**	**3**	2^2	**5**	2·3	**7**	2^3	3^2
1	2·5	**11**	2^2·3	**13**	2·7	3·5	2^4	**17**	2·3^2	**19**
2	2^2·5	3·7	2·11	**23**	2^3·3	5^2	2·13	3^3	2^2·7	**29**
3	2·3·5	**31**	2^5	3·11	2·17	5·7	2^2·3^2	**37**	2·19	3·13
4	2^3·5	**41**	2·3·7	**43**	2^2·11	3^2·5	2·23	**47**	2^4·3	7^2
5	2·5^2	3·17	2^2·13	**53**	2·3^3	5·11	2^3·7	3·19	2·29	**59**
6	2^2·3·5	**61**	2·31	3^2·7	2^6	5·13	2·3·11	**67**	2^2·17	3·23
7	2·5·7	**71**	2^3·3^2	**73**	2·37	3·5^2	2^2·19	7·11	2·3·13	**79**
8	2^4·5	3^4	2·41	**83**	2^2·3·7	5·17	2·43	3·29	2^3·11	**89**
9	2·3^2·5	7·13	2^2·23	3·31	2·47	5·19	2^5·3	**97**	2·7^2	3^2·11
10	2^2·5^2	**101**	2·3·17	**103**	2^3·13	3·5·7	2·53	**107**	2^2·3^3	**109**
11	2·5·11	3·37	2^4·7	**113**	2·3·19	5·23	2^2·29	3^2·13	2·59	7·17
12	2^3·3·5	11^2	2·61	3·41	2^2·31	5^3	2·3^2·7	**127**	2^7	3·43
13	2·5·13	**131**	2^2·3·11	7·19	2·67	3^3·5	2^3·17	**137**	2·3·23	**139**
14	2^2·5·7	3·47	2·71	11·13	2^4·3^2	5·29	2·73	3·7^2	2^2·37	**149**
15	2·3·5^2	**151**	2^3·19	3^2·17	2·7·11	5·31	2^2·3·13	**157**	2·79	3·53
16	2^5·5	7·23	2·3^4	**163**	2^2·41	3·5·11	2·83	**167**	2^3·3·7	13^2
17	2·5·17	3^2·19	2^2·43	**173**	2·3·29	5^2·7	2^4·11	3·59	2·89	**179**
18	2^2·3^2·5	**181**	2·7·13	3·61	2^3·23	5·37	2·3·31	11·17	2^2·47	3^3·7
19	2·5·19	**191**	2^6·3	**193**	2·97	3·5·13	2^2·7^2	**197**	2·3^2·11	**199**
20	2^3·5^2	3·67	2·101	7·29	2^2·3·17	5·41	2·103	3^2·23	2^4·13	11·19
21	2·3·5·7	**211**	2^2·53	3·71	2·107	5·43	2^3·3^3	7·31	2·109	3·73
22	2^2·5·11	13·17	2·3·37	**223**	2^5·7	3^2·5^2	2·113	**227**	2^2·3·19	**229**
23	2·5·23	3·7·11	2^3·29	**233**	2·3^2·13	5·47	2^2·59	3·79	2·7·17	**239**
24	2^4·3·5	**241**	2·11^2	3^5	2^2·61	5·7^2	2·3·41	13·19	2^3·31	3·83
25	2·5^3	**251**	2^2·3^2·7	11·23	2·127	3·5·17	2^8	**257**	2·3·43	7·37
26	2^2·5·13	3^2·29	2·131	**263**	2^3·3·11	5·53	2·7·19	3·89	2^2·67	**269**
27	2·3^3·5	**271**	2^4·17	3·7·13	2·137	5^2·11	2^2·3·23	**277**	2·139	3^2·31
28	2^3·5·7	**281**	2·3·47	**283**	2^2·71	3·5·19	2·11·13	7·41	2^5·3^2	17^2
29	2·5·29	3·97	2^2·73	**293**	2·3·7^2	5·59	2^3·37	3^3·11	2·149	13·23
30	2^2·3·5^2	7·43	2·151	3·101	2^4·19	5·61	2·3^2·17	**307**	2^2·7·11	3·103
31	2·5·31	**311**	2^3·3·13	**313**	2·157	3^2·5·7	2^2·79	**317**	2·3·53	11·29
32	2^6·5	3·107	2·7·23	17·19	2^2·3^4	5^2·13	2·163	3·109	2^3·41	7·47
33	2·3·5·11	**331**	2^2·83	3^2·37	2·167	5·67	2^4·3·7	**337**	2·13^2	3·113
34	2^2·5·17	11·31	2·3^2·19	7^3	2^3·43	3·5·23	2·173	**347**	2^2·3·29	**349**
35	2·5^2·7	3^3·13	2^5·11	**353**	2·3·59	5·71	2^2·89	3·7·17	2·179	**359**
36	2^3·3^2·5	19^2	2·181	3·11^2	2^2·7·13	5·73	2·3·61	**367**	2^4·23	3^2·41
37	2·5·37	7·53	2^2·3·31	**373**	2·11·17	3·5^3	2^3·47	13·29	2·3^3·7	**379**
38	2^2·5·19	3·127	2·191	**383**	2^7·3	5·7·11	2·193	3^2·43	2^2·97	**389**
39	2·3·5·13	17·23	2^3·7^2	3·131	2·197	5·79	2^2·3^2·11	**397**	2·199	3·7·19
40	2^4·5^2	**401**	2·3·67	13·31	2^2·101	3^4·5	2·7·29	11·37	2^3·3·17	**409**
41	2·5·41	3·137	2^2·103	7·59	2·3^2·23	5·83	2^5·13	3·139	2·11·19	**419**
42	2^2·3·5·7	**421**	2·211	3^2·47	2^3·53	5^2·17	2·3·71	7·61	2^2·107	3·11·13
43	2·5·43	**431**	2^4·3^3	**433**	2·7·31	3·5·29	2^2·109	19·23	2·3·73	**439**
44	2^3·5·11	3^2·7^2	2·13·17	**443**	2^2·3·37	5·89	2·223	3·149	2^6·7	**449**
45	2·3^2·5^2	11·41	2^2·113	3·151	2·227	5·7·13	2^3·3·19	**457**	2·229	3^3·17
46	2^2·5·23	**461**	2·3·7·11	**463**	2^4·29	3·5·31	2·233	**467**	2^2·3^2·13	7·67
47	2·5·47	3·157	2^3·59	11·43	2·3·79	5^2·19	2^2·7·17	3^2·53	2·239	**479**
48	2^5·3·5	13·37	2·241	3·7·23	2^2·11^2	5·97	2·3^5	**487**	2^3·61	3·163
49	2·5·7^2	**491**	2^2·3·41	17·29	2·13·19	3^2·5·11	2^4·31	7·71	2·3·83	**499**
50	2^2·5^3	3·167	2·251	**503**	2^3·3^2·7	5·101	2·11·23	3·13^2	2^2·127	**509**
51	2·3·5·17	7·73	2^9	3^3·19	2·257	5·103	2^2·3·43	11·47	2·7·37	3·173
52	2^3·5·13	**521**	2·3^2·29	**523**	2^2·131	3·5^2·7	2·263	17·31	2^4·3·11	23^2
53	2·5·53	3^2·59	2^2·7·19	13·41	2·3·89	5·107	2^3·67	3·179	2·269	7^2·11
54	2^2·3^3·5	**541**	2·271	3·181	2^5·17	5·109	2·3·7·13	**547**	2^2·137	3^2·61
55	2·5^2·11	19·29	2^3·3·23	7·79	2·277	3·5·37	2^2·139	**557**	2·3^2·31	13·43
56	2^4·5·7	3·11·17	2·281	**563**	2^2·3·47	5·113	2·283	3^4·7	2^3·71	**569**
57	2·3·5·19	**571**	2^2·11·13	3·191	2·7·41	5^2·23	2^6·3^2	**577**	2·17^2	3·193

	0	1	2	3	4	5	6	7	8	9
58	$2^2 \cdot 5 \cdot 29$	$7 \cdot 83$	$2 \cdot 3 \cdot 97$	$11 \cdot 53$	$2^3 \cdot 73$	$3^2 \cdot 5 \cdot 13$	$2 \cdot 293$	**587**	$2^2 \cdot 3 \cdot 7^2$	$19 \cdot 31$
59	$2 \cdot 5 \cdot 59$	$3 \cdot 197$	$2^4 \cdot 37$	**593**	$2 \cdot 3^3 \cdot 11$	$5 \cdot 7 \cdot 17$	$2^2 \cdot 149$	$3 \cdot 199$	$2 \cdot 13 \cdot 23$	**599**
60	$2^3 \cdot 3 \cdot 5^2$	**601**	$2 \cdot 7 \cdot 43$	$3^2 \cdot 67$	$2^2 \cdot 151$	$5 \cdot 11^2$	$2 \cdot 3 \cdot 101$	**607**	$2^5 \cdot 19$	$3 \cdot 7 \cdot 29$
61	$2 \cdot 5 \cdot 61$	$13 \cdot 47$	$2^2 \cdot 3^2 \cdot 17$	**613**	$2 \cdot 307$	$3 \cdot 5 \cdot 41$	$2^3 \cdot 7 \cdot 11$	**617**	$2 \cdot 3 \cdot 103$	**619**
62	$2^2 \cdot 5 \cdot 31$	$3^3 \cdot 23$	$2 \cdot 311$	$7 \cdot 89$	$2^4 \cdot 3 \cdot 13$	5^4	$2 \cdot 313$	$3 \cdot 11 \cdot 19$	$2^2 \cdot 157$	$17 \cdot 37$
63	$2 \cdot 3^2 \cdot 5 \cdot 7$	**631**	$2^3 \cdot 79$	$3 \cdot 211$	$2 \cdot 317$	$5 \cdot 127$	$2^2 \cdot 3 \cdot 53$	$7^2 \cdot 13$	$2 \cdot 11 \cdot 29$	$3^2 \cdot 71$
64	$2^7 \cdot 5$	**641**	$2 \cdot 3 \cdot 107$	**643**	$2^2 \cdot 7 \cdot 23$	$3 \cdot 5 \cdot 43$	$2 \cdot 17 \cdot 19$	**647**	$2^3 \cdot 3^4$	$11 \cdot 59$
65	$2 \cdot 5^2 \cdot 13$	$3 \cdot 7 \cdot 31$	$2^2 \cdot 163$	**653**	$2 \cdot 3 \cdot 109$	$5 \cdot 131$	$2^4 \cdot 41$	$3^2 \cdot 73$	$2 \cdot 7 \cdot 47$	**659**
66	$2^2 \cdot 3 \cdot 5 \cdot 11$	**661**	$2 \cdot 331$	$3 \cdot 13 \cdot 17$	$2^3 \cdot 83$	$5 \cdot 7 \cdot 19$	$2 \cdot 3^2 \cdot 37$	$23 \cdot 29$	$2^2 \cdot 167$	$3 \cdot 223$
67	$2 \cdot 5 \cdot 67$	$11 \cdot 61$	$2^5 \cdot 3 \cdot 7$	**673**	$2 \cdot 337$	$3^3 \cdot 5^2$	$2^2 \cdot 13^2$	**677**	$2 \cdot 3 \cdot 113$	$7 \cdot 97$
68	$2^3 \cdot 5 \cdot 17$	$3 \cdot 227$	$2 \cdot 11 \cdot 31$	**683**	$2^2 \cdot 3^2 \cdot 19$	$5 \cdot 137$	$2 \cdot 7^3$	$3 \cdot 229$	$2^4 \cdot 43$	$13 \cdot 53$
69	$2 \cdot 3 \cdot 5 \cdot 23$	**691**	$2^2 \cdot 173$	$3^2 \cdot 7 \cdot 11$	$2 \cdot 347$	$5 \cdot 139$	$2^3 \cdot 3 \cdot 29$	$17 \cdot 41$	$2 \cdot 349$	$3 \cdot 233$
70	$2^2 \cdot 5^2 \cdot 7$	**701**	$2 \cdot 3^3 \cdot 13$	$19 \cdot 37$	$2^6 \cdot 11$	$3 \cdot 5 \cdot 47$	$2 \cdot 353$	$7 \cdot 101$	$2^2 \cdot 3 \cdot 59$	**709**
71	$2 \cdot 5 \cdot 71$	$3^2 \cdot 79$	$2^3 \cdot 89$	$23 \cdot 31$	$2 \cdot 3 \cdot 7 \cdot 17$	$5 \cdot 11 \cdot 13$	$2^2 \cdot 179$	$3 \cdot 239$	$2 \cdot 359$	**719**
72	$2^4 \cdot 3^2 \cdot 5$	$7 \cdot 103$	$2 \cdot 19^2$	$3 \cdot 241$	$2^2 \cdot 181$	$5^2 \cdot 29$	$2 \cdot 3 \cdot 11^2$	**727**	$2^3 \cdot 7 \cdot 13$	3^6
73	$2 \cdot 5 \cdot 73$	$17 \cdot 43$	$2^2 \cdot 3 \cdot 61$	**733**	$2 \cdot 367$	$3 \cdot 5 \cdot 7^2$	$2^5 \cdot 23$	$11 \cdot 67$	$2 \cdot 3^2 \cdot 41$	**739**
74	$2^2 \cdot 5 \cdot 37$	$3 \cdot 13 \cdot 19$	$2 \cdot 7 \cdot 53$	**743**	$2^3 \cdot 3 \cdot 31$	$5 \cdot 149$	$2 \cdot 373$	$3^2 \cdot 83$	$2^2 \cdot 11 \cdot 17$	$7 \cdot 107$
75	$2 \cdot 3 \cdot 5^3$	**751**	$2^4 \cdot 47$	$3 \cdot 251$	$2 \cdot 13 \cdot 29$	$5 \cdot 151$	$2^2 \cdot 3^3 \cdot 7$	**757**	$2 \cdot 379$	$3 \cdot 11 \cdot 23$
76	$2^3 \cdot 5 \cdot 19$	**761**	$2 \cdot 3 \cdot 127$	$7 \cdot 109$	$2^2 \cdot 191$	$3^2 \cdot 5 \cdot 17$	$2 \cdot 383$	$13 \cdot 59$	$2^8 \cdot 3$	**769**
77	$2 \cdot 5 \cdot 7 \cdot 11$	$3 \cdot 257$	$2^2 \cdot 193$	**773**	$2 \cdot 3^2 \cdot 43$	$5^2 \cdot 31$	$2^3 \cdot 97$	$3 \cdot 7 \cdot 37$	$2 \cdot 389$	$19 \cdot 41$
78	$2^2 \cdot 3 \cdot 5 \cdot 13$	$11 \cdot 71$	$2 \cdot 17 \cdot 23$	$3^3 \cdot 29$	$2^4 \cdot 7^2$	$5 \cdot 157$	$2 \cdot 3 \cdot 131$	**787**	$2^2 \cdot 197$	$3 \cdot 263$
79	$2 \cdot 5 \cdot 79$	$7 \cdot 113$	$2^3 \cdot 3^2 \cdot 11$	$13 \cdot 61$	$2 \cdot 397$	$3 \cdot 5 \cdot 53$	$2^2 \cdot 199$	**797**	$2 \cdot 3 \cdot 7 \cdot 19$	$17 \cdot 47$
80	$2^5 \cdot 5^2$	$3^2 \cdot 89$	$2 \cdot 401$	$11 \cdot 73$	$2^2 \cdot 3 \cdot 67$	$5 \cdot 7 \cdot 23$	$2 \cdot 13 \cdot 31$	$3 \cdot 269$	$2^3 \cdot 101$	**809**
81	$2 \cdot 3^4 \cdot 5$	**811**	$2^2 \cdot 7 \cdot 29$	$3 \cdot 271$	$2 \cdot 11 \cdot 37$	$5 \cdot 163$	$2^4 \cdot 3 \cdot 17$	$19 \cdot 43$	$2 \cdot 409$	$3^2 \cdot 7 \cdot 13$
82	$2^2 \cdot 5 \cdot 41$	**821**	$2 \cdot 3 \cdot 137$	**823**	$2^3 \cdot 103$	$3 \cdot 5^2 \cdot 11$	$2 \cdot 7 \cdot 59$	**827**	$2^2 \cdot 3^2 \cdot 23$	**829**
83	$2 \cdot 5 \cdot 83$	$3 \cdot 277$	$2^6 \cdot 13$	$7^2 \cdot 17$	$2 \cdot 3 \cdot 139$	$5 \cdot 167$	$2^2 \cdot 11 \cdot 19$	$3^3 \cdot 31$	$2 \cdot 419$	**839**
84	$2^3 \cdot 3 \cdot 5 \cdot 7$	29^2	$2 \cdot 421$	$3 \cdot 281$	$2^2 \cdot 211$	$5 \cdot 13^2$	$2 \cdot 3^2 \cdot 47$	$7 \cdot 11^2$	$2^4 \cdot 53$	$3 \cdot 283$
85	$2 \cdot 5^2 \cdot 17$	$23 \cdot 37$	$2^2 \cdot 3 \cdot 71$	**853**	$2 \cdot 7 \cdot 61$	$3^2 \cdot 5 \cdot 19$	$2^3 \cdot 107$	**857**	$2 \cdot 3 \cdot 11 \cdot 13$	**859**
86	$2^2 \cdot 5 \cdot 43$	$3 \cdot 7 \cdot 41$	$2 \cdot 431$	**863**	$2^5 \cdot 3^3$	$5 \cdot 173$	$2 \cdot 433$	$3 \cdot 17^2$	$2^2 \cdot 7 \cdot 31$	$11 \cdot 79$
87	$2 \cdot 3 \cdot 5 \cdot 29$	$13 \cdot 67$	$2^3 \cdot 109$	$3^2 \cdot 97$	$2 \cdot 19 \cdot 23$	$5^3 \cdot 7$	$2^2 \cdot 3 \cdot 73$	**877**	$2 \cdot 439$	$3 \cdot 293$
88	$2^4 \cdot 5 \cdot 11$	**881**	$2 \cdot 3^2 \cdot 7^2$	**883**	$2^2 \cdot 13 \cdot 17$	$3 \cdot 5 \cdot 59$	$2 \cdot 443$	**887**	$2^3 \cdot 3 \cdot 37$	$7 \cdot 127$
89	$2 \cdot 5 \cdot 89$	$3^4 \cdot 11$	$2^2 \cdot 223$	$19 \cdot 47$	$2 \cdot 3 \cdot 149$	$5 \cdot 179$	$2^7 \cdot 7$	$3 \cdot 13 \cdot 23$	$2 \cdot 449$	$29 \cdot 31$
90	$2^2 \cdot 3^2 \cdot 5^2$	$17 \cdot 53$	$2 \cdot 11 \cdot 41$	$3 \cdot 7 \cdot 43$	$2^3 \cdot 113$	$5 \cdot 181$	$2 \cdot 3 \cdot 151$	**907**	$2^2 \cdot 227$	$3^2 \cdot 101$
91	$2 \cdot 5 \cdot 7 \cdot 13$	**911**	$2^4 \cdot 3 \cdot 19$	$11 \cdot 83$	$2 \cdot 457$	$3 \cdot 5 \cdot 61$	$2^2 \cdot 229$	$7 \cdot 131$	$2 \cdot 3^3 \cdot 17$	**919**
92	$2^3 \cdot 5 \cdot 23$	$3 \cdot 307$	$2 \cdot 461$	$13 \cdot 71$	$2^2 \cdot 3 \cdot 7 \cdot 11$	$5^2 \cdot 37$	$2 \cdot 463$	$3^2 \cdot 103$	$2^5 \cdot 29$	**929**
93	$2 \cdot 3 \cdot 5 \cdot 31$	$7^2 \cdot 19$	$2^2 \cdot 233$	$3 \cdot 311$	$2 \cdot 467$	$5 \cdot 11 \cdot 17$	$2^3 \cdot 3^2 \cdot 13$	**937**	$2 \cdot 7 \cdot 67$	$3 \cdot 313$
94	$2^2 \cdot 5 \cdot 47$	**941**	$2 \cdot 3 \cdot 157$	$23 \cdot 41$	$2^4 \cdot 59$	$3^3 \cdot 5 \cdot 7$	$2 \cdot 11 \cdot 43$	**947**	$2^2 \cdot 3 \cdot 79$	$13 \cdot 73$
95	$2 \cdot 5^2 \cdot 19$	$3 \cdot 317$	$2^3 \cdot 7 \cdot 17$	**953**	$2 \cdot 3^2 \cdot 53$	$5 \cdot 191$	$2^2 \cdot 239$	$3 \cdot 11 \cdot 29$	$2 \cdot 479$	$7 \cdot 137$
96	$2^6 \cdot 3 \cdot 5$	31^2	$2 \cdot 13 \cdot 37$	$3^2 \cdot 107$	$2^2 \cdot 241$	$5 \cdot 193$	$2 \cdot 3 \cdot 7 \cdot 23$	**967**	$2^3 \cdot 11^2$	$3 \cdot 17 \cdot 19$
97	$2 \cdot 5 \cdot 97$	**971**	$2^2 \cdot 3^5$	$7 \cdot 139$	$2 \cdot 487$	$3 \cdot 5^2 \cdot 13$	$2^4 \cdot 61$	**977**	$2 \cdot 3 \cdot 163$	$11 \cdot 89$
98	$2^2 \cdot 5 \cdot 7^2$	$3^2 \cdot 109$	$2 \cdot 491$	**983**	$2^3 \cdot 3 \cdot 41$	$5 \cdot 197$	$2 \cdot 17 \cdot 29$	$3 \cdot 7 \cdot 47$	$2^2 \cdot 13 \cdot 19$	$23 \cdot 43$
99	$2 \cdot 3^2 \cdot 5 \cdot 11$	**991**	$2^5 \cdot 31$	$3 \cdot 331$	$2 \cdot 7 \cdot 71$	$5 \cdot 199$	$2^2 \cdot 3 \cdot 83$	**997**	$2 \cdot 499$	$3^3 \cdot 37$
100	$2^3 \cdot 5^3$	$7 \cdot 11 \cdot 13$	$2 \cdot 3 \cdot 167$	$17 \cdot 59$	$2^2 \cdot 251$	$3 \cdot 5 \cdot 67$	$2 \cdot 503$	$19 \cdot 53$	$2^4 \cdot 3^2 \cdot 7$	**1009**
101	$2 \cdot 5 \cdot 101$	$3 \cdot 337$	$2^2 \cdot 11 \cdot 23$	**1013**	$2 \cdot 3 \cdot 13^2$	$5 \cdot 7 \cdot 29$	$2^3 \cdot 127$	$3^2 \cdot 113$	$2 \cdot 509$	**1019**
102	$2^2 \cdot 3 \cdot 5 \cdot 17$	**1021**	$2 \cdot 7 \cdot 73$	$3 \cdot 11 \cdot 31$	2^{10}	$5^2 \cdot 41$	$2 \cdot 3^3 \cdot 19$	$13 \cdot 79$	$2^2 \cdot 257$	$3 \cdot 7^3$
103	$2 \cdot 5 \cdot 103$	**1031**	$2^3 \cdot 3 \cdot 43$	**1033**	$2 \cdot 11 \cdot 47$	$3^2 \cdot 5 \cdot 23$	$2^2 \cdot 7 \cdot 37$	$17 \cdot 61$	$2 \cdot 3 \cdot 173$	**1039**
104	$2^4 \cdot 5 \cdot 13$	$3 \cdot 347$	$2 \cdot 521$	$7 \cdot 149$	$2^2 \cdot 3^2 \cdot 29$	$5 \cdot 11 \cdot 19$	$2 \cdot 523$	$3 \cdot 349$	$2^3 \cdot 131$	**1049**
105	$2 \cdot 3 \cdot 5^2 \cdot 7$	**1051**	$2^2 \cdot 263$	$3^4 \cdot 13$	$2 \cdot 17 \cdot 31$	$5 \cdot 211$	$2^5 \cdot 3 \cdot 11$	$7 \cdot 151$	$2 \cdot 23^2$	$3 \cdot 353$
106	$2^2 \cdot 5 \cdot 53$	**1061**	$2 \cdot 3^2 \cdot 59$	**1063**	$2^3 \cdot 7 \cdot 19$	$3 \cdot 5 \cdot 71$	$2 \cdot 13 \cdot 41$	$11 \cdot 97$	$2^2 \cdot 3 \cdot 89$	**1069**
107	$2 \cdot 5 \cdot 107$	$3^2 \cdot 7 \cdot 17$	$2^4 \cdot 67$	$29 \cdot 37$	$2 \cdot 3 \cdot 179$	$5^2 \cdot 43$	$2^2 \cdot 269$	$3 \cdot 359$	$2 \cdot 7^2 \cdot 11$	$13 \cdot 83$
108	$2^3 \cdot 3^3 \cdot 5$	$23 \cdot 47$	$2 \cdot 541$	$3 \cdot 19^2$	$2^2 \cdot 271$	$5 \cdot 7 \cdot 31$	$2 \cdot 3 \cdot 181$	**1087**	$2^6 \cdot 17$	$3^2 \cdot 11^2$
109	$2 \cdot 5 \cdot 109$	**1091**	$2^2 \cdot 3 \cdot 7 \cdot 13$	**1093**	$2 \cdot 547$	$3 \cdot 5 \cdot 73$	$2^3 \cdot 137$	**1097**	$2 \cdot 3^2 \cdot 61$	$7 \cdot 157$
110	$2^2 \cdot 5^2 \cdot 11$	$3 \cdot 367$	$2 \cdot 19 \cdot 29$	**1103**	$2^4 \cdot 3 \cdot 23$	$5 \cdot 13 \cdot 17$	$2 \cdot 7 \cdot 79$	$3^3 \cdot 41$	$2^2 \cdot 277$	**1109**
111	$2 \cdot 3 \cdot 5 \cdot 37$	$11 \cdot 101$	$2^3 \cdot 139$	$3 \cdot 7 \cdot 53$	$2 \cdot 557$	$5 \cdot 223$	$2^2 \cdot 3^2 \cdot 31$	**1117**	$2 \cdot 13 \cdot 43$	$3 \cdot 373$
112	$2^5 \cdot 5 \cdot 7$	$19 \cdot 59$	$2 \cdot 3 \cdot 11 \cdot 17$	**1123**	$2^2 \cdot 281$	$3^2 \cdot 5^3$	$2 \cdot 563$	$7^2 \cdot 23$	$2^3 \cdot 3 \cdot 47$	**1129**
113	$2 \cdot 5 \cdot 113$	$3 \cdot 13 \cdot 29$	$2^2 \cdot 283$	$11 \cdot 103$	$2 \cdot 3^4 \cdot 7$	$5 \cdot 227$	$2^4 \cdot 71$	$3 \cdot 379$	$2 \cdot 569$	$17 \cdot 67$
114	$2^2 \cdot 3 \cdot 5 \cdot 19$	$7 \cdot 163$	$2 \cdot 571$	$3^2 \cdot 127$	$2^3 \cdot 11 \cdot 13$	$5 \cdot 229$	$2 \cdot 3 \cdot 191$	$31 \cdot 37$	$2^2 \cdot 7 \cdot 41$	$3 \cdot 383$
115	$2 \cdot 5^2 \cdot 23$	**1151**	$2^7 \cdot 3^2$	**1153**	$2 \cdot 577$	$3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 17^2$	$13 \cdot 89$	$2 \cdot 3 \cdot 193$	$19 \cdot 61$
116	$2^3 \cdot 5 \cdot 29$	$3^3 \cdot 43$	$2 \cdot 7 \cdot 83$	**1163**	$2^2 \cdot 3 \cdot 97$	$5 \cdot 233$	$2 \cdot 11 \cdot 53$	$3 \cdot 389$	$2^4 \cdot 73$	$7 \cdot 167$
117	$2 \cdot 3^2 \cdot 5 \cdot 13$	**1171**	$2^2 \cdot 293$	$3 \cdot 17 \cdot 23$	$2 \cdot 587$	$5^2 \cdot 47$	$2^3 \cdot 3 \cdot 7^2$	$11 \cdot 107$	$2 \cdot 19 \cdot 31$	$3^2 \cdot 131$
118	$2^2 \cdot 5 \cdot 59$	**1181**	$2 \cdot 3 \cdot 197$	$7 \cdot 13^2$	$2^5 \cdot 37$	$3 \cdot 5 \cdot 79$	$2 \cdot 593$	**1187**	$2^2 \cdot 3^3 \cdot 11$	$29 \cdot 41$
119	$2 \cdot 5 \cdot 7 \cdot 17$	$3 \cdot 397$	$2^3 \cdot 149$	**1193**	$2 \cdot 3 \cdot 199$	$5 \cdot 239$	$2^2 \cdot 13 \cdot 23$	$3^2 \cdot 7 \cdot 19$	$2 \cdot 599$	$11 \cdot 109$
120	$2^4 \cdot 3 \cdot 5^2$	**1201**	$2 \cdot 601$	$3 \cdot 401$	$2^2 \cdot 7 \cdot 43$	$5 \cdot 241$	$2 \cdot 3^2 \cdot 67$	$17 \cdot 71$	$2^3 \cdot 151$	$3 \cdot 13 \cdot 31$
121	$2 \cdot 5 \cdot 11^2$	$7 \cdot 173$	$2^2 \cdot 3 \cdot 101$	**1213**	$2 \cdot 607$	$3^5 \cdot 5$	$2^6 \cdot 19$	**1217**	$2 \cdot 3 \cdot 7 \cdot 29$	$23 \cdot 53$

	0	1	2	3	4	5	6	7	8	9
122	$2^2 \cdot 5 \cdot 61$	$3 \cdot 11 \cdot 37$	$2 \cdot 13 \cdot 47$	**1223**	$2^3 \cdot 3^2 \cdot 17$	$5^2 \cdot 7^2$	$2 \cdot 613$	$3 \cdot 409$	$2^2 \cdot 307$	**1229**
123	$2 \cdot 3 \cdot 5 \cdot 41$	**1231**	$2^4 \cdot 7 \cdot 11$	$3^2 \cdot 137$	$2 \cdot 617$	$5 \cdot 13 \cdot 19$	$2^2 \cdot 3 \cdot 103$	**1237**	$2 \cdot 619$	$3 \cdot 7 \cdot 59$
124	$2^3 \cdot 5 \cdot 31$	$17 \cdot 73$	$2 \cdot 3^3 \cdot 23$	$11 \cdot 113$	$2^2 \cdot 311$	$3 \cdot 5 \cdot 83$	$2 \cdot 7 \cdot 89$	$29 \cdot 43$	$2^5 \cdot 3 \cdot 13$	**1249**
125	$2 \cdot 5^4$	$3^2 \cdot 139$	$2^2 \cdot 313$	$7 \cdot 179$	$2 \cdot 3 \cdot 11 \cdot 19$	$5 \cdot 251$	$2^3 \cdot 157$	$3 \cdot 419$	$2 \cdot 17 \cdot 37$	**1259**
126	$2^2 \cdot 3^2 \cdot 5 \cdot 7$	$13 \cdot 97$	$2 \cdot 631$	$3 \cdot 421$	$2^4 \cdot 79$	$5 \cdot 11 \cdot 23$	$2 \cdot 3 \cdot 211$	$7 \cdot 181$	$2^2 \cdot 317$	$3^3 \cdot 47$
127	$2 \cdot 5 \cdot 127$	$31 \cdot 41$	$2^3 \cdot 3 \cdot 53$	$19 \cdot 67$	$2 \cdot 7^2 \cdot 13$	$3 \cdot 5^2 \cdot 17$	$2^2 \cdot 11 \cdot 29$	**1277**	$2 \cdot 3^2 \cdot 71$	**1279**
128	$2^8 \cdot 5$	$3 \cdot 7 \cdot 61$	$2 \cdot 641$	**1283**	$2^2 \cdot 3 \cdot 107$	$5 \cdot 257$	$2 \cdot 643$	$3^2 \cdot 11 \cdot 13$	$2^3 \cdot 7 \cdot 23$	**1289**
129	$2 \cdot 3 \cdot 5 \cdot 43$	**1291**	$2^2 \cdot 17 \cdot 19$	$3 \cdot 431$	$2 \cdot 647$	$5 \cdot 7 \cdot 37$	$2^4 \cdot 3^4$	**1297**	$2 \cdot 11 \cdot 59$	$3 \cdot 433$
130	$2^2 \cdot 5^2 \cdot 13$	**1301**	$2 \cdot 3 \cdot 7 \cdot 31$	**1303**	$2^3 \cdot 163$	$3^2 \cdot 5 \cdot 29$	$2 \cdot 653$	**1307**	$2^2 \cdot 3 \cdot 109$	$7 \cdot 11 \cdot 17$
131	$2 \cdot 5 \cdot 131$	$3 \cdot 19 \cdot 23$	$2^5 \cdot 41$	$13 \cdot 101$	$2 \cdot 3^2 \cdot 73$	$5 \cdot 263$	$2^2 \cdot 7 \cdot 47$	$3 \cdot 439$	$2 \cdot 659$	**1319**
132	$2^3 \cdot 3 \cdot 5 \cdot 11$	**1321**	$2 \cdot 661$	$3^3 \cdot 7^2$	$2^2 \cdot 331$	$5^2 \cdot 53$	$2 \cdot 3 \cdot 13 \cdot 17$	**1327**	$2^4 \cdot 83$	$3 \cdot 443$
133	$2 \cdot 5 \cdot 7 \cdot 19$	11^3	$2^2 \cdot 3^2 \cdot 37$	$31 \cdot 43$	$2 \cdot 23 \cdot 29$	$3 \cdot 5 \cdot 89$	$2^3 \cdot 167$	$7 \cdot 191$	$2 \cdot 3 \cdot 223$	$13 \cdot 103$
134	$2^2 \cdot 5 \cdot 67$	$3^2 \cdot 149$	$2 \cdot 11 \cdot 61$	$17 \cdot 79$	$2^6 \cdot 3 \cdot 7$	$5 \cdot 269$	$2 \cdot 673$	$3 \cdot 449$	$2^2 \cdot 337$	$19 \cdot 71$
135	$2 \cdot 3^3 \cdot 5^2$	$7 \cdot 193$	$2^3 \cdot 13^2$	$3 \cdot 11 \cdot 41$	$2 \cdot 677$	$5 \cdot 271$	$2^2 \cdot 3 \cdot 113$	$23 \cdot 59$	$2 \cdot 7 \cdot 97$	$3^2 \cdot 151$
136	$2^4 \cdot 5 \cdot 17$	**1361**	$2 \cdot 3 \cdot 227$	$29 \cdot 47$	$2^2 \cdot 11 \cdot 31$	$3 \cdot 5 \cdot 7 \cdot 13$	$2 \cdot 683$	**1367**	$2^3 \cdot 3^2 \cdot 19$	37^2
137	$2 \cdot 5 \cdot 137$	$3 \cdot 457$	$2^2 \cdot 7^3$	**1373**	$2 \cdot 3 \cdot 229$	$5^3 \cdot 11$	$2^5 \cdot 43$	$3^4 \cdot 17$	$2 \cdot 13 \cdot 53$	$7 \cdot 197$
138	$2^2 \cdot 3 \cdot 5 \cdot 23$	**1381**	$2 \cdot 691$	$3 \cdot 461$	$2^3 \cdot 173$	$5 \cdot 277$	$2 \cdot 3^2 \cdot 7 \cdot 11$	$19 \cdot 73$	$2^2 \cdot 347$	$3 \cdot 463$
139	$2 \cdot 5 \cdot 139$	$13 \cdot 107$	$2^4 \cdot 3 \cdot 29$	$7 \cdot 199$	$2 \cdot 17 \cdot 41$	$3^2 \cdot 5 \cdot 31$	$2^2 \cdot 349$	$11 \cdot 127$	$2 \cdot 3 \cdot 233$	**1399**
140	$2^3 \cdot 5^2 \cdot 7$	$3 \cdot 467$	$2 \cdot 701$	$23 \cdot 61$	$2^2 \cdot 3^3 \cdot 13$	$5 \cdot 281$	$2 \cdot 19 \cdot 37$	$3 \cdot 7 \cdot 67$	$2^7 \cdot 11$	**1409**
141	$2 \cdot 3 \cdot 5 \cdot 47$	$17 \cdot 83$	$2^2 \cdot 353$	$3^2 \cdot 157$	$2 \cdot 7 \cdot 101$	$5 \cdot 283$	$2^3 \cdot 3 \cdot 59$	$13 \cdot 109$	$2 \cdot 709$	$3 \cdot 11 \cdot 43$
142	$2^2 \cdot 5 \cdot 71$	$7^2 \cdot 29$	$2 \cdot 3^2 \cdot 79$	**1423**	$2^4 \cdot 89$	$3 \cdot 5^2 \cdot 19$	$2 \cdot 23 \cdot 31$	**1427**	$2^2 \cdot 3 \cdot 7 \cdot 17$	**1429**
143	$2 \cdot 5 \cdot 11 \cdot 13$	$3^3 \cdot 53$	$2^3 \cdot 179$	**1433**	$2 \cdot 3 \cdot 239$	$5 \cdot 7 \cdot 41$	$2^2 \cdot 359$	$3 \cdot 479$	$2 \cdot 719$	**1439**
144	$2^5 \cdot 3^2 \cdot 5$	$11 \cdot 131$	$2 \cdot 7 \cdot 103$	$3 \cdot 13 \cdot 37$	$2^2 \cdot 19^2$	$5 \cdot 17^2$	$2 \cdot 3 \cdot 241$	**1447**	$2^3 \cdot 181$	$3^2 \cdot 7 \cdot 23$
145	$2 \cdot 5^2 \cdot 29$	**1451**	$2^2 \cdot 3 \cdot 11^2$	**1453**	$2 \cdot 727$	$3 \cdot 5 \cdot 97$	$2^4 \cdot 7 \cdot 13$	$31 \cdot 47$	$2 \cdot 3^6$	**1459**
146	$2^2 \cdot 5 \cdot 73$	$3 \cdot 487$	$2 \cdot 17 \cdot 43$	$7 \cdot 11 \cdot 19$	$2^3 \cdot 3 \cdot 61$	$5 \cdot 293$	$2 \cdot 733$	$3^2 \cdot 163$	$2^2 \cdot 367$	$13 \cdot 113$
147	$2 \cdot 3 \cdot 5 \cdot 7^2$	**1471**	$2^6 \cdot 23$	$3 \cdot 491$	$2 \cdot 11 \cdot 67$	$5^2 \cdot 59$	$2^2 \cdot 3^2 \cdot 41$	$7 \cdot 211$	$2 \cdot 739$	$3 \cdot 17 \cdot 29$
148	$2^3 \cdot 5 \cdot 37$	**1481**	$2 \cdot 3 \cdot 13 \cdot 19$	**1483**	$2^2 \cdot 7 \cdot 53$	$3^3 \cdot 5 \cdot 11$	$2 \cdot 743$	**1487**	$2^4 \cdot 3 \cdot 31$	**1489**
149	$2 \cdot 5 \cdot 149$	$3 \cdot 7 \cdot 71$	$2^2 \cdot 373$	**1493**	$2 \cdot 3^2 \cdot 83$	$5 \cdot 13 \cdot 23$	$2^3 \cdot 11 \cdot 17$	$3 \cdot 499$	$2 \cdot 7 \cdot 107$	**1499**
150	$2^2 \cdot 3 \cdot 5^3$	$19 \cdot 79$	$2 \cdot 751$	$3^2 \cdot 167$	$2^5 \cdot 47$	$5 \cdot 7 \cdot 43$	$2 \cdot 3 \cdot 251$	$11 \cdot 137$	$2^2 \cdot 13 \cdot 29$	$3 \cdot 503$
151	$2 \cdot 5 \cdot 151$	**1511**	$2^3 \cdot 3^3 \cdot 7$	$17 \cdot 89$	$2 \cdot 757$	$3 \cdot 5 \cdot 101$	$2^2 \cdot 379$	$37 \cdot 41$	$2 \cdot 3 \cdot 11 \cdot 23$	$7^2 \cdot 31$
152	$2^4 \cdot 5 \cdot 19$	$3^2 \cdot 13^2$	$2 \cdot 761$	**1523**	$2^2 \cdot 3 \cdot 127$	$5^2 \cdot 61$	$2 \cdot 7 \cdot 109$	$3 \cdot 509$	$2^3 \cdot 191$	$11 \cdot 139$
153	$2 \cdot 3^2 \cdot 5 \cdot 17$	**1531**	$2^2 \cdot 383$	$3 \cdot 7 \cdot 73$	$2 \cdot 13 \cdot 59$	$5 \cdot 307$	$2^9 \cdot 3$	$29 \cdot 53$	$2 \cdot 769$	$3^4 \cdot 19$
154	$2^2 \cdot 5 \cdot 7 \cdot 11$	$23 \cdot 67$	$2 \cdot 3 \cdot 257$	**1543**	$2^3 \cdot 193$	$3 \cdot 5 \cdot 103$	$2 \cdot 773$	$7 \cdot 13 \cdot 17$	$2^2 \cdot 3^2 \cdot 43$	**1549**
155	$2 \cdot 5^2 \cdot 31$	$3 \cdot 11 \cdot 47$	$2^4 \cdot 97$	**1553**	$2 \cdot 3 \cdot 7 \cdot 37$	$5 \cdot 311$	$2^2 \cdot 389$	$3^2 \cdot 173$	$2 \cdot 19 \cdot 41$	**1559**
156	$2^3 \cdot 3 \cdot 5 \cdot 13$	$7 \cdot 223$	$2 \cdot 11 \cdot 71$	$3 \cdot 521$	$2^2 \cdot 17 \cdot 23$	$5 \cdot 313$	$2 \cdot 3^3 \cdot 29$	**1567**	$2^5 \cdot 7^2$	$3 \cdot 523$
157	$2 \cdot 5 \cdot 157$	**1571**	$2^2 \cdot 3 \cdot 131$	$11^2 \cdot 13$	$2 \cdot 787$	$3^2 \cdot 5^2 \cdot 7$	$2^3 \cdot 197$	$19 \cdot 83$	$2 \cdot 3 \cdot 263$	**1579**
158	$2^2 \cdot 5 \cdot 79$	$3 \cdot 17 \cdot 31$	$2 \cdot 7 \cdot 113$	**1583**	$2^4 \cdot 3^2 \cdot 11$	$5 \cdot 317$	$2 \cdot 13 \cdot 61$	$3 \cdot 23^2$	$2^2 \cdot 397$	$7 \cdot 227$
159	$2 \cdot 3 \cdot 5 \cdot 53$	$37 \cdot 43$	$2^3 \cdot 199$	$3^3 \cdot 59$	$2 \cdot 797$	$5 \cdot 11 \cdot 29$	$2^2 \cdot 3 \cdot 7 \cdot 19$	**1597**	$2 \cdot 17 \cdot 47$	$3 \cdot 13 \cdot 41$
160	$2^6 \cdot 5^2$	**1601**	$2 \cdot 3^2 \cdot 89$	$7 \cdot 229$	$2^2 \cdot 401$	$3 \cdot 5 \cdot 107$	$2 \cdot 11 \cdot 73$	**1607**	$2^3 \cdot 3 \cdot 67$	**1609**
161	$2 \cdot 5 \cdot 7 \cdot 23$	$3^2 \cdot 179$	$2^2 \cdot 13 \cdot 31$	**1613**	$2 \cdot 3 \cdot 269$	$5 \cdot 17 \cdot 19$	$2^4 \cdot 101$	$3 \cdot 7^2 \cdot 11$	$2 \cdot 809$	**1619**
162	$2^2 \cdot 3^4 \cdot 5$	**1621**	$2 \cdot 811$	$3 \cdot 541$	$2^3 \cdot 7 \cdot 29$	$5^3 \cdot 13$	$2 \cdot 3 \cdot 271$	**1627**	$2^2 \cdot 11 \cdot 37$	$3^2 \cdot 181$
163	$2 \cdot 5 \cdot 163$	$7 \cdot 233$	$2^5 \cdot 3 \cdot 17$	$23 \cdot 71$	$2 \cdot 19 \cdot 43$	$3 \cdot 5 \cdot 109$	$2^2 \cdot 409$	**1637**	$2 \cdot 3^2 \cdot 7 \cdot 13$	$11 \cdot 149$
164	$2^3 \cdot 5 \cdot 41$	$3 \cdot 547$	$2 \cdot 821$	$31 \cdot 53$	$2^2 \cdot 3 \cdot 137$	$5 \cdot 7 \cdot 47$	$2 \cdot 823$	$3^3 \cdot 61$	$2^4 \cdot 103$	$17 \cdot 97$
165	$2 \cdot 3 \cdot 5^2 \cdot 11$	$13 \cdot 127$	$2^2 \cdot 7 \cdot 59$	$3 \cdot 19 \cdot 29$	$2 \cdot 827$	$5 \cdot 331$	$2^3 \cdot 3^2 \cdot 23$	**1657**	$2 \cdot 829$	$3 \cdot 7 \cdot 79$
166	$2^2 \cdot 5 \cdot 83$	$11 \cdot 151$	$2 \cdot 3 \cdot 277$	**1663**	$2^7 \cdot 13$	$3^2 \cdot 5 \cdot 37$	$2 \cdot 7^2 \cdot 17$	**1667**	$2^2 \cdot 3 \cdot 139$	**1669**
167	$2 \cdot 5 \cdot 167$	$3 \cdot 557$	$2^3 \cdot 11 \cdot 19$	$7 \cdot 239$	$2 \cdot 3^3 \cdot 31$	$5^2 \cdot 67$	$2^2 \cdot 419$	$3 \cdot 13 \cdot 43$	$2 \cdot 839$	$23 \cdot 73$
168	$2^4 \cdot 3 \cdot 5 \cdot 7$	41^2	$2 \cdot 29^2$	$3^2 \cdot 11 \cdot 17$	$2^2 \cdot 421$	$5 \cdot 337$	$2 \cdot 3 \cdot 281$	$7 \cdot 241$	$2^3 \cdot 211$	$3 \cdot 563$
169	$2 \cdot 5 \cdot 13^2$	$19 \cdot 89$	$2^2 \cdot 3^2 \cdot 47$	**1693**	$2 \cdot 7 \cdot 11^2$	$3 \cdot 5 \cdot 113$	$2^5 \cdot 53$	**1697**	$2 \cdot 3 \cdot 283$	**1699**
170	$2^2 \cdot 5^2 \cdot 17$	$3^5 \cdot 7$	$2 \cdot 23 \cdot 37$	$13 \cdot 131$	$2^3 \cdot 3 \cdot 71$	$5 \cdot 11 \cdot 31$	$2 \cdot 853$	$3 \cdot 569$	$2^2 \cdot 7 \cdot 61$	**1709**
171	$2 \cdot 3^2 \cdot 5 \cdot 19$	$29 \cdot 59$	$2^4 \cdot 107$	$3 \cdot 571$	$2 \cdot 857$	$5 \cdot 7^3$	$2^2 \cdot 3 \cdot 11 \cdot 13$	$17 \cdot 101$	$2 \cdot 859$	$3^2 \cdot 191$
172	$2^3 \cdot 5 \cdot 43$	**1721**	$2 \cdot 3 \cdot 7 \cdot 41$	**1723**	$2^2 \cdot 431$	$3 \cdot 5^2 \cdot 23$	$2 \cdot 863$	$11 \cdot 157$	$2^6 \cdot 3^3$	$7 \cdot 13 \cdot 19$
173	$2 \cdot 5 \cdot 173$	$3 \cdot 577$	$2^2 \cdot 433$	**1733**	$2 \cdot 3 \cdot 17^2$	$5 \cdot 347$	$2^3 \cdot 7 \cdot 31$	$3^2 \cdot 193$	$2 \cdot 11 \cdot 79$	$37 \cdot 47$
174	$2^2 \cdot 3 \cdot 5 \cdot 29$	**1741**	$2 \cdot 13 \cdot 67$	$3 \cdot 7 \cdot 83$	$2^4 \cdot 109$	$5 \cdot 349$	$2 \cdot 3^2 \cdot 97$	**1747**	$2^2 \cdot 19 \cdot 23$	$3 \cdot 11 \cdot 53$
175	$2 \cdot 5^3 \cdot 7$	$17 \cdot 103$	$2^3 \cdot 3 \cdot 73$	**1753**	$2 \cdot 877$	$3^3 \cdot 5 \cdot 13$	$2^2 \cdot 439$	$7 \cdot 251$	$2 \cdot 3 \cdot 293$	**1759**
176	$2^5 \cdot 5 \cdot 11$	$3 \cdot 587$	$2 \cdot 881$	$41 \cdot 43$	$2^2 \cdot 3^2 \cdot 7^2$	$5 \cdot 353$	$2 \cdot 883$	$3 \cdot 19 \cdot 31$	$2^3 \cdot 13 \cdot 17$	$29 \cdot 61$
177	$2 \cdot 3 \cdot 5 \cdot 59$	$7 \cdot 11 \cdot 23$	$2^2 \cdot 443$	$3^2 \cdot 197$	$2 \cdot 887$	$5^2 \cdot 71$	$2^4 \cdot 3 \cdot 37$	**1777**	$2 \cdot 7 \cdot 127$	$3 \cdot 593$
178	$2^2 \cdot 5 \cdot 89$	$13 \cdot 137$	$2 \cdot 3^4 \cdot 11$	**1783**	$2^3 \cdot 223$	$3 \cdot 5 \cdot 7 \cdot 17$	$2 \cdot 19 \cdot 47$	**1787**	$2^2 \cdot 3 \cdot 149$	**1789**
179	$2 \cdot 5 \cdot 179$	$3^2 \cdot 199$	$2^8 \cdot 7$	$11 \cdot 163$	$2 \cdot 3 \cdot 13 \cdot 23$	$5 \cdot 359$	$2^2 \cdot 449$	$3 \cdot 599$	$2 \cdot 29 \cdot 31$	$7 \cdot 257$
180	$2^3 \cdot 3^2 \cdot 5^2$	**1801**	$2 \cdot 17 \cdot 53$	$3 \cdot 601$	$2^2 \cdot 11 \cdot 41$	$5 \cdot 19^2$	$2 \cdot 3 \cdot 7 \cdot 43$	$13 \cdot 139$	$2^4 \cdot 113$	$3^3 \cdot 67$
181	$2 \cdot 5 \cdot 181$	**1811**	$2^2 \cdot 3 \cdot 151$	$7^2 \cdot 37$	$2 \cdot 907$	$3 \cdot 5 \cdot 11^2$	$2^3 \cdot 227$	$23 \cdot 79$	$2 \cdot 3^2 \cdot 101$	$17 \cdot 107$
182	$2^2 \cdot 5 \cdot 7 \cdot 13$	$3 \cdot 607$	$2 \cdot 911$	**1823**	$2^5 \cdot 3 \cdot 19$	$5^2 \cdot 73$	$2 \cdot 11 \cdot 83$	$3^2 \cdot 7 \cdot 29$	$2^2 \cdot 457$	$31 \cdot 59$
183	$2 \cdot 3 \cdot 5 \cdot 61$	**1831**	$2^3 \cdot 229$	$3 \cdot 13 \cdot 47$	$2 \cdot 7 \cdot 131$	$5 \cdot 367$	$2^2 \cdot 3^3 \cdot 17$	$11 \cdot 167$	$2 \cdot 919$	$3 \cdot 613$
184	$2^4 \cdot 5 \cdot 23$	$7 \cdot 263$	$2 \cdot 3 \cdot 307$	$19 \cdot 97$	$2^2 \cdot 461$	$3^2 \cdot 5 \cdot 41$	$2 \cdot 13 \cdot 71$	**1847**	$2^3 \cdot 3 \cdot 7 \cdot 11$	43^2
185	$2 \cdot 5^2 \cdot 37$	$3 \cdot 617$	$2^2 \cdot 463$	$17 \cdot 109$	$2 \cdot 3^2 \cdot 103$	$5 \cdot 7 \cdot 53$	$2^6 \cdot 29$	$3 \cdot 619$	$2 \cdot 929$	$11 \cdot 13^2$

	0	1	2	3	4	5	6	7	8	9
186	$2^2 \cdot 3 \cdot 5 \cdot 31$	**1861**	$2 \cdot 7^2 \cdot 19$	$3^4 \cdot 23$	$2^3 \cdot 233$	$5 \cdot 373$	$2 \cdot 3 \cdot 311$	**1867**	$2^2 \cdot 467$	$3 \cdot 7 \cdot 89$
187	$2 \cdot 5 \cdot 11 \cdot 17$	**1871**	$2^4 \cdot 3^2 \cdot 13$	**1873**	$2 \cdot 937$	$3 \cdot 5^4$	$2^2 \cdot 7 \cdot 67$	**1877**	$2 \cdot 3 \cdot 313$	**1879**
188	$2^3 \cdot 5 \cdot 47$	$3^2 \cdot 11 \cdot 19$	$2 \cdot 941$	$7 \cdot 269$	$2^2 \cdot 3 \cdot 157$	$5 \cdot 13 \cdot 29$	$2 \cdot 23 \cdot 41$	$3 \cdot 17 \cdot 37$	$2^5 \cdot 59$	**1889**
189	$2 \cdot 3^3 \cdot 5 \cdot 7$	$31 \cdot 61$	$2^2 \cdot 11 \cdot 43$	$3 \cdot 631$	$2 \cdot 947$	$5 \cdot 379$	$2^3 \cdot 3 \cdot 79$	$7 \cdot 271$	$2 \cdot 13 \cdot 73$	$3^2 \cdot 211$
190	$2^2 \cdot 5^2 \cdot 19$	**1901**	$2 \cdot 3 \cdot 317$	$11 \cdot 173$	$2^4 \cdot 7 \cdot 17$	$3 \cdot 5 \cdot 127$	$2 \cdot 953$	**1907**	$2^2 \cdot 3^2 \cdot 53$	$23 \cdot 83$
191	$2 \cdot 5 \cdot 191$	$3 \cdot 7^2 \cdot 13$	$2^3 \cdot 239$	**1913**	$2 \cdot 3 \cdot 11 \cdot 29$	$5 \cdot 383$	$2^2 \cdot 479$	$3^3 \cdot 71$	$2 \cdot 7 \cdot 137$	$19 \cdot 101$
192	$2^7 \cdot 3 \cdot 5$	$17 \cdot 113$	$2 \cdot 31^2$	$3 \cdot 641$	$2^2 \cdot 13 \cdot 37$	$5^2 \cdot 7 \cdot 11$	$2 \cdot 3^2 \cdot 107$	$41 \cdot 47$	$2^3 \cdot 241$	$3 \cdot 643$
193	$2 \cdot 5 \cdot 193$	**1931**	$2^2 \cdot 3 \cdot 7 \cdot 23$	**1933**	$2 \cdot 967$	$3^2 \cdot 5 \cdot 43$	$2^4 \cdot 11^2$	$13 \cdot 149$	$2 \cdot 3 \cdot 17 \cdot 19$	$7 \cdot 277$
194	$2^2 \cdot 5 \cdot 97$	$3 \cdot 647$	$2 \cdot 971$	$29 \cdot 67$	$2^3 \cdot 3^5$	$5 \cdot 389$	$2 \cdot 7 \cdot 139$	$3 \cdot 11 \cdot 59$	$2^2 \cdot 487$	**1949**
195	$2 \cdot 3 \cdot 5^2 \cdot 13$	**1951**	$2^5 \cdot 61$	$3^2 \cdot 7 \cdot 31$	$2 \cdot 977$	$5 \cdot 17 \cdot 23$	$2^2 \cdot 3 \cdot 163$	$19 \cdot 103$	$2 \cdot 11 \cdot 89$	$3 \cdot 653$
196	$2^3 \cdot 5 \cdot 7^2$	$37 \cdot 53$	$2 \cdot 3^2 \cdot 109$	$13 \cdot 151$	$2^2 \cdot 491$	$3 \cdot 5 \cdot 131$	$2 \cdot 983$	$7 \cdot 281$	$2^4 \cdot 3 \cdot 41$	$11 \cdot 179$
197	$2 \cdot 5 \cdot 197$	$3^3 \cdot 73$	$2^2 \cdot 17 \cdot 29$	**1973**	$2 \cdot 3 \cdot 7 \cdot 47$	$5^2 \cdot 79$	$2^3 \cdot 13 \cdot 19$	$3 \cdot 659$	$2 \cdot 23 \cdot 43$	**1979**
198	$2^2 \cdot 3^2 \cdot 5 \cdot 11$	$7 \cdot 283$	$2 \cdot 991$	$3 \cdot 661$	$2^6 \cdot 31$	$5 \cdot 397$	$2 \cdot 3 \cdot 331$	**1987**	$2^2 \cdot 7 \cdot 71$	$3^2 \cdot 13 \cdot 17$
199	$2 \cdot 5 \cdot 199$	$11 \cdot 181$	$2^3 \cdot 3 \cdot 83$	**1993**	$2 \cdot 997$	$3 \cdot 5 \cdot 7 \cdot 19$	$2^2 \cdot 499$	**1997**	$2 \cdot 3^3 \cdot 37$	**1999**
200	$2^4 \cdot 5^3$	$3 \cdot 23 \cdot 29$	$2 \cdot 7 \cdot 11 \cdot 13$	**2003**	$2^2 \cdot 3 \cdot 167$	$5 \cdot 401$	$2 \cdot 17 \cdot 59$	$3^2 \cdot 223$	$2^3 \cdot 251$	$7^2 \cdot 41$
201	$2 \cdot 3 \cdot 5 \cdot 67$	**2011**	$2^2 \cdot 503$	$3 \cdot 11 \cdot 61$	$2 \cdot 19 \cdot 53$	$5 \cdot 13 \cdot 31$	$2^5 \cdot 3^2 \cdot 7$	**2017**	$2 \cdot 1009$	$3 \cdot 673$
202	$2^2 \cdot 5 \cdot 101$	$43 \cdot 47$	$2 \cdot 3 \cdot 337$	$7 \cdot 17^2$	$2^3 \cdot 11 \cdot 23$	$3^4 \cdot 5^2$	$2 \cdot 1013$	**2027**	$2^2 \cdot 3 \cdot 13^2$	**2029**
203	$2 \cdot 5 \cdot 7 \cdot 29$	$3 \cdot 677$	$2^4 \cdot 127$	$19 \cdot 107$	$2 \cdot 3^2 \cdot 113$	$5 \cdot 11 \cdot 37$	$2^2 \cdot 509$	$3 \cdot 7 \cdot 97$	$2 \cdot 1019$	**2039**
204	$2^3 \cdot 3 \cdot 5 \cdot 17$	$13 \cdot 157$	$2 \cdot 1021$	$3^2 \cdot 227$	$2^2 \cdot 7 \cdot 73$	$5 \cdot 409$	$2 \cdot 3 \cdot 11 \cdot 31$	$23 \cdot 89$	2^{11}	$3 \cdot 683$
205	$2 \cdot 5^2 \cdot 41$	$7 \cdot 293$	$2^2 \cdot 3^3 \cdot 19$	**2053**	$2 \cdot 13 \cdot 79$	$3 \cdot 5 \cdot 137$	$2^3 \cdot 257$	$11^2 \cdot 17$	$2 \cdot 3 \cdot 7^3$	$29 \cdot 71$
206	$2^2 \cdot 5 \cdot 103$	$3^2 \cdot 229$	$2 \cdot 1031$	**2063**	$2^4 \cdot 3 \cdot 43$	$5 \cdot 7 \cdot 59$	$2 \cdot 1033$	$3 \cdot 13 \cdot 53$	$2^2 \cdot 11 \cdot 47$	**2069**
207	$2 \cdot 3^2 \cdot 5 \cdot 23$	$19 \cdot 109$	$2^3 \cdot 7 \cdot 37$	$3 \cdot 691$	$2 \cdot 17 \cdot 61$	$5^2 \cdot 83$	$2^2 \cdot 3 \cdot 173$	$31 \cdot 67$	$2 \cdot 1039$	$3^3 \cdot 7 \cdot 11$
208	$2^5 \cdot 5 \cdot 13$	**2081**	$2 \cdot 3 \cdot 347$	**2083**	$2^2 \cdot 521$	$3 \cdot 5 \cdot 139$	$2 \cdot 7 \cdot 149$	**2087**	$2^3 \cdot 3^2 \cdot 29$	**2089**
209	$2 \cdot 5 \cdot 11 \cdot 19$	$3 \cdot 17 \cdot 41$	$2^2 \cdot 523$	$7 \cdot 13 \cdot 23$	$2 \cdot 3 \cdot 349$	$5 \cdot 419$	$2^4 \cdot 131$	$3^2 \cdot 233$	$2 \cdot 1049$	**2099**
210	$2^2 \cdot 3 \cdot 5^2 \cdot 7$	$11 \cdot 191$	$2 \cdot 1051$	$3 \cdot 701$	$2^3 \cdot 263$	$5 \cdot 421$	$2 \cdot 3^4 \cdot 13$	$7^2 \cdot 43$	$2^2 \cdot 17 \cdot 31$	$3 \cdot 19 \cdot 37$
211	$2 \cdot 5 \cdot 211$	**2111**	$2^6 \cdot 3 \cdot 11$	**2113**	$2 \cdot 7 \cdot 151$	$3^2 \cdot 5 \cdot 47$	$2^2 \cdot 23^2$	$29 \cdot 73$	$2 \cdot 3 \cdot 353$	$13 \cdot 163$
212	$2^3 \cdot 5 \cdot 53$	$3 \cdot 7 \cdot 101$	$2 \cdot 1061$	$11 \cdot 193$	$2^2 \cdot 3^2 \cdot 59$	$5^3 \cdot 17$	$2 \cdot 1063$	$3 \cdot 709$	$2^4 \cdot 7 \cdot 19$	**2129**
213	$2 \cdot 3 \cdot 5 \cdot 71$	**2131**	$2^2 \cdot 13 \cdot 41$	$3^3 \cdot 79$	$2 \cdot 11 \cdot 97$	$5 \cdot 7 \cdot 61$	$2^3 \cdot 3 \cdot 89$	**2137**	$2 \cdot 1069$	$3 \cdot 23 \cdot 31$
214	$2^2 \cdot 5 \cdot 107$	**2141**	$2 \cdot 3^2 \cdot 7 \cdot 17$	**2143**	$2^5 \cdot 67$	$3 \cdot 5 \cdot 11 \cdot 13$	$2 \cdot 29 \cdot 37$	$19 \cdot 113$	$2^2 \cdot 3 \cdot 179$	$7 \cdot 307$
215	$2 \cdot 5^2 \cdot 43$	$3^2 \cdot 239$	$2^3 \cdot 269$	**2153**	$2 \cdot 3 \cdot 359$	$5 \cdot 431$	$2^2 \cdot 7^2 \cdot 11$	$3 \cdot 719$	$2 \cdot 13 \cdot 83$	$17 \cdot 127$
216	$2^4 \cdot 3^3 \cdot 5$	**2161**	$2 \cdot 23 \cdot 47$	$3 \cdot 7 \cdot 103$	$2^2 \cdot 541$	$5 \cdot 433$	$2 \cdot 3 \cdot 19^2$	$11 \cdot 197$	$2^3 \cdot 271$	$3^2 \cdot 241$
217	$2 \cdot 5 \cdot 7 \cdot 31$	$13 \cdot 167$	$2^2 \cdot 3 \cdot 181$	$41 \cdot 53$	$2 \cdot 1087$	$3 \cdot 5^2 \cdot 29$	$2^7 \cdot 17$	$7 \cdot 311$	$2 \cdot 3^2 \cdot 11^2$	**2179**
218	$2^2 \cdot 5 \cdot 109$	$3 \cdot 727$	$2 \cdot 1091$	$37 \cdot 59$	$2^3 \cdot 3 \cdot 7 \cdot 13$	$5 \cdot 19 \cdot 23$	$2 \cdot 1093$	3^7	$2^2 \cdot 547$	$11 \cdot 199$
219	$2 \cdot 3 \cdot 5 \cdot 73$	$7 \cdot 313$	$2^4 \cdot 137$	$3 \cdot 17 \cdot 43$	$2 \cdot 1097$	$5 \cdot 439$	$2^2 \cdot 3^2 \cdot 61$	13^3	$2 \cdot 7 \cdot 157$	$3 \cdot 733$
220	$2^3 \cdot 5^2 \cdot 11$	$31 \cdot 71$	$2 \cdot 3 \cdot 367$	**2203**	$2^2 \cdot 19 \cdot 29$	$3^2 \cdot 5 \cdot 7^2$	$2 \cdot 1103$	**2207**	$2^5 \cdot 3 \cdot 23$	47^2
221	$2 \cdot 5 \cdot 13 \cdot 17$	$3 \cdot 11 \cdot 67$	$2^2 \cdot 7 \cdot 79$	**2213**	$2 \cdot 3^3 \cdot 41$	$5 \cdot 443$	$2^3 \cdot 277$	$3 \cdot 739$	$2 \cdot 1109$	$7 \cdot 317$
222	$2^2 \cdot 3 \cdot 5 \cdot 37$	**2221**	$2 \cdot 11 \cdot 101$	$3^2 \cdot 13 \cdot 19$	$2^4 \cdot 139$	$5^2 \cdot 89$	$2 \cdot 3 \cdot 7 \cdot 53$	$17 \cdot 131$	$2^2 \cdot 557$	$3 \cdot 743$
223	$2 \cdot 5 \cdot 223$	$23 \cdot 97$	$2^3 \cdot 3^2 \cdot 31$	$7 \cdot 11 \cdot 29$	$2 \cdot 1117$	$3 \cdot 5 \cdot 149$	$2^2 \cdot 13 \cdot 43$	**2237**	$2 \cdot 3 \cdot 373$	**2239**
224	$2^6 \cdot 5 \cdot 7$	$3^3 \cdot 83$	$2 \cdot 19 \cdot 59$	**2243**	$2^2 \cdot 3 \cdot 11 \cdot 17$	$5 \cdot 449$	$2 \cdot 1123$	$3 \cdot 7 \cdot 107$	$2^3 \cdot 281$	$13 \cdot 173$
225	$2 \cdot 3^2 \cdot 5^3$	**2251**	$2^2 \cdot 563$	$3 \cdot 751$	$2 \cdot 7^2 \cdot 23$	$5 \cdot 11 \cdot 41$	$2^4 \cdot 3 \cdot 47$	$37 \cdot 61$	$2 \cdot 1129$	$3^2 \cdot 251$
226	$2^2 \cdot 5 \cdot 113$	$7 \cdot 17 \cdot 19$	$2 \cdot 3 \cdot 13 \cdot 29$	$31 \cdot 73$	$2^3 \cdot 283$	$3 \cdot 5 \cdot 151$	$2 \cdot 11 \cdot 103$	**2267**	$2^2 \cdot 3^4 \cdot 7$	**2269**
227	$2 \cdot 5 \cdot 227$	$3 \cdot 757$	$2^5 \cdot 71$	**2273**	$2 \cdot 3 \cdot 379$	$5^2 \cdot 7 \cdot 13$	$2^2 \cdot 569$	$3^2 \cdot 11 \cdot 23$	$2 \cdot 17 \cdot 67$	$43 \cdot 53$
228	$2^3 \cdot 3 \cdot 5 \cdot 19$	**2281**	$2 \cdot 7 \cdot 163$	$3 \cdot 761$	$2^2 \cdot 571$	$5 \cdot 457$	$2 \cdot 3^2 \cdot 127$	**2287**	$2^4 \cdot 11 \cdot 13$	$3 \cdot 7 \cdot 109$
229	$2 \cdot 5 \cdot 229$	$29 \cdot 79$	$2^2 \cdot 3 \cdot 191$	**2293**	$2 \cdot 31 \cdot 37$	$3^3 \cdot 5 \cdot 17$	$2^3 \cdot 7 \cdot 41$	**2297**	$2 \cdot 3 \cdot 383$	$11^2 \cdot 19$
230	$2^2 \cdot 5^2 \cdot 23$	$3 \cdot 13 \cdot 59$	$2 \cdot 1151$	$7^2 \cdot 47$	$2^8 \cdot 3^2$	$5 \cdot 461$	$2 \cdot 1153$	$3 \cdot 769$	$2^2 \cdot 577$	**2309**
231	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	**2311**	$2^3 \cdot 17^2$	$3^2 \cdot 257$	$2 \cdot 13 \cdot 89$	$5 \cdot 463$	$2^2 \cdot 3 \cdot 193$	$7 \cdot 331$	$2 \cdot 19 \cdot 61$	$3 \cdot 773$
232	$2^4 \cdot 5 \cdot 29$	$11 \cdot 211$	$2 \cdot 3^3 \cdot 43$	$23 \cdot 101$	$2^2 \cdot 7 \cdot 83$	$3 \cdot 5^2 \cdot 31$	$2 \cdot 1163$	$13 \cdot 179$	$2^3 \cdot 3 \cdot 97$	$17 \cdot 137$
233	$2 \cdot 5 \cdot 233$	$3^2 \cdot 7 \cdot 37$	$2^2 \cdot 11 \cdot 53$	**2333**	$2 \cdot 3 \cdot 389$	$5 \cdot 467$	$2^5 \cdot 73$	$3 \cdot 19 \cdot 41$	$2 \cdot 7 \cdot 167$	**2339**
234	$2^2 \cdot 3^2 \cdot 5 \cdot 13$	**2341**	$2 \cdot 1171$	$3 \cdot 11 \cdot 71$	$2^3 \cdot 293$	$5 \cdot 7 \cdot 67$	$2 \cdot 3 \cdot 17 \cdot 23$	**2347**	$2^2 \cdot 587$	$3^4 \cdot 29$
235	$2 \cdot 5^2 \cdot 47$	**2351**	$2^4 \cdot 3 \cdot 7^2$	$13 \cdot 181$	$2 \cdot 11 \cdot 107$	$3 \cdot 5 \cdot 157$	$2^2 \cdot 19 \cdot 31$	**2357**	$2 \cdot 3^2 \cdot 131$	$7 \cdot 337$
236	$2^3 \cdot 5 \cdot 59$	$3 \cdot 787$	$2 \cdot 1181$	$17 \cdot 139$	$2^2 \cdot 3 \cdot 197$	$5 \cdot 11 \cdot 43$	$2 \cdot 7 \cdot 13^2$	$3^2 \cdot 263$	$2^6 \cdot 37$	$23 \cdot 103$
237	$2 \cdot 3 \cdot 5 \cdot 79$	**2371**	$2^2 \cdot 593$	$3 \cdot 7 \cdot 113$	$2 \cdot 1187$	$5^3 \cdot 19$	$2^3 \cdot 3^3 \cdot 11$	**2377**	$2 \cdot 29 \cdot 41$	$3 \cdot 13 \cdot 61$
238	$2^2 \cdot 5 \cdot 7 \cdot 17$	**2381**	$2 \cdot 3 \cdot 397$	**2383**	$2^4 \cdot 149$	$3^2 \cdot 5 \cdot 53$	$2 \cdot 1193$	$7 \cdot 11 \cdot 31$	$2^2 \cdot 3 \cdot 199$	**2389**
239	$2 \cdot 5 \cdot 239$	$3 \cdot 797$	$2^3 \cdot 13 \cdot 23$	**2393**	$2 \cdot 3^2 \cdot 7 \cdot 19$	$5 \cdot 479$	$2^2 \cdot 599$	$3 \cdot 17 \cdot 47$	$2 \cdot 11 \cdot 109$	**2399**
240	$2^5 \cdot 3 \cdot 5^2$	7^4	$2 \cdot 1201$	$3^3 \cdot 89$	$2^2 \cdot 601$	$5 \cdot 13 \cdot 37$	$2 \cdot 3 \cdot 401$	$29 \cdot 83$	$2^3 \cdot 7 \cdot 43$	$3 \cdot 11 \cdot 73$
241	$2 \cdot 5 \cdot 241$	**2411**	$2^2 \cdot 3^2 \cdot 67$	$19 \cdot 127$	$2 \cdot 17 \cdot 71$	$3 \cdot 5 \cdot 7 \cdot 23$	$2^4 \cdot 151$	**2417**	$2 \cdot 3 \cdot 13 \cdot 31$	$41 \cdot 59$
242	$2^2 \cdot 5 \cdot 11^2$	$3^2 \cdot 269$	$2 \cdot 7 \cdot 173$	**2423**	$2^3 \cdot 3 \cdot 101$	$5^2 \cdot 97$	$2 \cdot 1213$	$3 \cdot 809$	$2^2 \cdot 607$	$7 \cdot 347$
243	$2 \cdot 3^5 \cdot 5$	$11 \cdot 13 \cdot 17$	$2^7 \cdot 19$	$3 \cdot 811$	$2 \cdot 1217$	$5 \cdot 487$	$2^2 \cdot 3 \cdot 7 \cdot 29$	**2437**	$2 \cdot 23 \cdot 53$	$3^2 \cdot 271$
244	$2^3 \cdot 5 \cdot 61$	**2441**	$2 \cdot 3 \cdot 11 \cdot 37$	$7 \cdot 349$	$2^2 \cdot 13 \cdot 47$	$3 \cdot 5 \cdot 163$	$2 \cdot 1223$	**2447**	$2^4 \cdot 3^2 \cdot 17$	$31 \cdot 79$
245	$2 \cdot 5^2 \cdot 7^2$	$3 \cdot 19 \cdot 43$	$2^2 \cdot 613$	$11 \cdot 223$	$2 \cdot 3 \cdot 409$	$5 \cdot 491$	$2^3 \cdot 307$	$3^3 \cdot 7 \cdot 13$	$2 \cdot 1229$	**2459**
246	$2^2 \cdot 3 \cdot 5 \cdot 41$	$23 \cdot 107$	$2 \cdot 1231$	$3 \cdot 821$	$2^5 \cdot 7 \cdot 11$	$5 \cdot 17 \cdot 29$	$2 \cdot 3^2 \cdot 137$	**2467**	$2^2 \cdot 617$	$3 \cdot 823$
247	$2 \cdot 5 \cdot 13 \cdot 19$	$7 \cdot 353$	$2^3 \cdot 3 \cdot 103$	**2473**	$2 \cdot 1237$	$3^2 \cdot 5^2 \cdot 11$	$2^2 \cdot 619$	**2477**	$2 \cdot 3 \cdot 7 \cdot 59$	$37 \cdot 67$
248	$2^4 \cdot 5 \cdot 31$	$3 \cdot 827$	$2 \cdot 17 \cdot 73$	$13 \cdot 191$	$2^2 \cdot 3^3 \cdot 23$	$5 \cdot 7 \cdot 71$	$2 \cdot 11 \cdot 113$	$3 \cdot 829$	$2^3 \cdot 311$	$19 \cdot 131$
249	$2 \cdot 3 \cdot 5 \cdot 83$	$47 \cdot 53$	$2^2 \cdot 7 \cdot 89$	$3^2 \cdot 277$	$2 \cdot 29 \cdot 43$	$5 \cdot 499$	$2^6 \cdot 3 \cdot 13$	$11 \cdot 227$	$2 \cdot 1249$	$3 \cdot 7^2 \cdot 17$

8.7 Irreducible Polynomials of Degree n

8.31 An *irreducible polynomial* of *degree* n over $\mathbb{F}_p$ is a polynomial $\sum_{i=0}^{n} a_i x^i$ that cannot be expressed as the product of two polynomials each of smaller degree, with computations of coefficients in $\mathbb{F}_p$.

8.32 **Remark** The polynomial $\sum_{i=0}^{n} a_i x^i$ is written here by specifying the vector $a_n \cdots a_1 a_0$.

8.33 **Table** Irreducible polynomials for $\mathbb{F}_2$ of degree n for $1 \le n \le 10$.

n	Polynomials				
1	10	11			
2	111				
3	1011	1101			
4	10011	11001	11111		
5	100101	101001	101111	110111	111011
	111101				
6	1000011	1001001	1010111	1011011	1100001
	1100111	1101101	1110011	1110101	
7	10000011	10001001	10001111	10010001	10011101
	10100111	10101011	10111001	10111111	11000001
	11001011	11010011	11010101	11100101	11101111
	11110001	11110111	11111101		
8	100011011	100011101	100101011	100101101	100111001
	100111111	101001101	101011111	101100011	101100101
	101101001	101110001	101110111	101111011	110000111
	110001011	110001101	110011111	110100011	110101001
	110110001	110111101	111000011	111001111	111010111
	111011101	111100111	111110011	111110101	111111001
9	1000000011	1000010001	1000010111	1000011011	1000100001
	1000101101	1000110011	1001001011	1001011001	1001011111
	1001100101	1001101001	1001101111	1001110111	1001111101
	1010000111	1010010101	1010011001	1010100011	1010100101
	1010101111	1010110111	1010111101	1011001111	1011010001
	1011011011	1011110101	1011111001	1100000001	1100010011
	1100010101	1100011111	1100100011	1100110001	1100111011
	1101001001	1101001111	1101011011	1101100001	1101101011
	1101101101	1101110011	1101111111	1110000101	1110001111
	1110100001	1110110101	1110111001	1111000111	1111001011
	1111001101	1111010101	1111011001	1111100011	1111101001
	1111111011				
10	10000001001	10000001111	10000011011	10000011101	10000100111
	10000101101	10000110101	10001000111	10001010011	10001100011
	10001100101	10001101111	10010000001	10010001011	10010011001
	10010101001	10010101111	10011000101	10011001001	10011010111
	10011100111	10011101101	10011110011	10011111111	10100001011
	10100001101	10100011001	10100011111	10100100011	10100110001
	10100111101	10101000011	10101010111	10101100001	10101100111
	10101101011	10110000101	10110001111	10110010111	10110011011
	10110100001	10110101011	10110111001	10111000001	10111000111
	10111100101	10111110111	10111111011	11000010011	11000010101
	11000100011	11000100101	11000110001	11000110111	11001000011
	11001001111	11001010001	11001011011	11001111001	11001111111
	11010000101	11010001001	11010100111	11010101101	11010110101
	11010111111	11011000001	11011001101	11011010011	11011011111
	11011110111	11011111101	11100001111	11100010001	11100010111
	11100011101	11100100001	11100101011	11100110101	11100111001

n	Polynomials				
	11101000111	11101001101	11101010101	11101011001	11101100011
	11101111011	11101111101	11110000001	11110000111	11110001101
	11110010011	11110101001	11110110001	11111000101	11111011011

8.34 **Table** Irreducible polynomials for $\mathbb{F}_3$ of degree n for $1 \leq n \leq 7$.

n	Polynomials							
1	10	11	12					
2	101	112	122					
3	1021	1022	1102	1112	1121	1201	1211	1222
4	10012	10022	10102	10111	10121	10202	11002	11021
	11101	11111	11122	11222	12002	12011	12101	12112
	12121	12212						
5	100021	100022	100112	100211	101011	101012	101102	101122
	101201	101221	102101	102112	102122	102202	102211	102221
	110002	110012	110021	110101	110111	110122	111011	111121
	111211	111212	112001	112022	112102	112111	112201	112202
	120001	120011	120022	120202	120212	120221	121012	121111
	121112	121222	122002	122021	122101	122102	122201	122212
6	1000012	1000022	1000111	1000121	1000201	1001012	1001021	1001101
	1001122	1001221	1002011	1002022	1002101	1002112	1002211	1010201
	1010212	1010222	1011001	1011011	1011022	1011122	1012001	1012012
	1012021	1012112	1020001	1020101	1020112	1020122	1021021	1021102
	1021112	1021121	1022011	1022102	1022111	1022122	1100002	1100012
	1100111	1101002	1101011	1101101	1101112	1101212	1102001	1102111
	1102121	1102201	1102202	1110001	1110011	1110122	1110202	1110221
	1111012	1111021	1111111	1111112	1111222	1112011	1112201	1112222
	1120102	1120121	1120222	1121012	1121102	1121122	1121212	1121221
	1122001	1122002	1122122	1122202	1122221	1200002	1200022	1200121
	1201001	1201111	1201121	1201201	1201202	1202002	1202021	1202101
	1202122	1202222	1210001	1210021	1210112	1210202	1210211	1211021
	1211201	1211212	1212011	1212022	1212121	1212122	1212212	1220102
	1220111	1220212	1221001	1221002	1221112	1221202	1221211	1222022
	1222102	1222112	1222211	1222222				
7	10000102	10000121	10000201	10000222	10001011	10001012	10001102	10001111
	10001201	10001212	10002112	10002122	10002211	10002221	10010122	10010222
	10011002	10011101	10011211	10012001	10012022	10012111	10012202	10020121
	10020221	10021001	10021112	10021202	10022002	10022021	10022101	10022212
	10100011	10100012	10100102	10100122	10100201	10100221	10101101	10101112
	10101202	10101211	10102102	10102201	10110022	10110101	10110211	10111001
	10111102	10111121	10111201	10112002	10112012	10112021	10112111	10112122
	10120021	10120112	10120202	10121002	10121102	10121201	10121222	10122001
	10122011	10122022	10122212	10122221	10200001	10200002	10200101	10200112
	10200202	10200211	10201021	10201022	10201121	10201222	10202011	10202012
	10210001	10210121	10210202	10211101	10211111	10211122	10211221	10212011
	10212022	10212101	10212112	10212212	10220002	10220101	10220222	10221122
	10221202	10221212	10221221	10222012	10222021	10222111	10222202	10222211
	11000101	11000222	11001022	11001112	11001211	11002012	11002022	11002121
	11002202	11010001	11010022	11010121	11010221	11011111	11011202	11012002
	11012102	11012212	11020021	11020022	11020102	11020112	11020201	11020222
	11021111	11021122	11021201	11021212	11022101	11022122	11022211	11022221
	11100002	11100022	11100121	11100212	11101012	11101022	11101102	11101111
	11101121	11102002	11102111	11102222	11110001	11110012	11110111	11110112
	11110211	11110222	11111011	11111021	11111201	11111222	11112011	11112221
	11120102	11120111	11120122	11120212	11120221	11121001	11121101	11121202
	11122021	11122112	11122201	11122222	11200201	11200202	11201012	11201021

n	Polynomials							
	11201101	11201111	11201221	11201222	11202002	11202121	11202211	11202212
	11210002	11210011	11210021	11210101	11211001	11211022	11211122	11211212
	11211221	11212012	11212112	11212202	11220001	11220112	11220211	11221022
	11221102	11221112	11221121	11222011	11222102	11222122	11222201	11222221
	12000121	12000202	12001021	12001112	12001211	12002011	12002021	12002101
	12002222	12010021	12010022	12010102	12010121	12010201	12010211	12011102
	12011111	12011212	12011221	12012112	12012122	12012202	12012221	12020002
	12020021	12020122	12020222	12021101	12021212	12022001	12022111	12022201
	12100001	12100021	12100111	12100222	12101011	12101021	12101201	12101212
	12101222	12102001	12102121	12102212	12110111	12110122	12110201	12110212
	12110221	12111002	12111101	12111202	12112022	12112102	12112121	12112211
	12120002	12120011	12120112	12120121	12120211	12120212	12121012	12121022
	12121102	12121121	12122012	12122122	12200101	12200102	12201011	12201022
	12201121	12201122	12201202	12201212	12202001	12202111	12202112	12202222
	12210002	12210112	12210211	12211021	12211201	12211211	12211222	12212012
	12212102	12212122	12212201	12212221	12220001	12220012	12220022	12220202
	12221002	12221021	12221111	12221122	12221221	12222011	12222101	12222211

8.35 Table Irreducible polynomials for $\mathbb{F}_5$ of degree n for $1 \leq n \leq 5$.

n	Polynomials									
1	10	11	12	13	14					
2	102	103	111	112	123	124	133	134	141	142
3	1011	1014	1021	1024	1032	1033	1042	1043	1101	1102
	1113	1114	1131	1134	1141	1143	1201	1203	1213	1214
	1222	1223	1242	1244	1302	1304	1311	1312	1322	1323
	1341	1343	1403	1404	1411	1412	1431	1434	1442	1444
4	10002	10003	10014	10024	10034	10044	10102	10111	10122	10123
	10132	10133	10141	10203	10221	10223	10231	10233	10303	10311
	10313	10341	10343	10402	10412	10413	10421	10431	10442	10443
	11004	11013	11023	11024	11032	11041	11042	11101	11113	11114
	11124	11133	11142	11202	11212	11213	11221	11222	11234	11244
	11301	11303	11321	11342	11344	11402	11411	11414	11441	11443
	12004	12013	12014	12021	12022	12033	12042	12102	12121	12123
	12131	12134	12201	12203	12211	12222	12224	12302	12311	12312
	12324	12332	12333	12344	12401	12414	12422	12433	12434	12443
	13004	13012	13023	13031	13032	13043	13044	13102	13121	13124
	13131	13133	13201	13203	13232	13234	13241	13302	13314	13322
	13323	13334	13341	13342	13401	13413	13423	13424	13432	13444
	14004	14011	14012	14022	14033	14034	14043	14101	14112	14123
	14134	14143	14144	14202	14214	14224	14231	14232	14242	14243
	14301	14303	14312	14314	14331	14402	14411	14413	14441	14444

8.36 Table Irreducible polynomials for $\mathbb{F}_7$ of degree n for $1 \leq n \leq 3$.

n	Polynomials									
1	10	11	12	13	14	15	16			
2	101	102	104	113	114	116	122	123	125	131
	135	136	141	145	146	152	153	155	163	164
	166									
3	1002	1003	1004	1005	1011	1016	1021	1026	1032	1035
	1041	1046	1052	1055	1062	1065	1101	1103	1112	1115
	1124	1126	1131	1135	1143	1146	1151	1152	1153	1154
	1163	1165	1201	1203	1214	1216	1223	1226	1233	1235
	1242	1245	1251	1255	1261	1262	1263	1264	1304	1306
	1311	1314	1322	1325	1333	1334	1335	1336	1341	1343
	1352	1354	1362	1366	1401	1403	1413	1416	1422	1425

n	Polynomials									
	1431	1432	1433	1434	1444	1446	1453	1455	1461	1465
	1504	1506	1511	1513	1521	1524	1532	1534	1542	1545
	1552	1556	1563	1564	1565	1566	1604	1606	1612	1615
	1621	1623	1632	1636	1641	1644	1653	1654	1655	1656
	1662	1664								

8.8 Primitive Polynomials of Degree n

8.37 A polynomial $p(x)$ is a *primitive polynomial* of degree n over $\mathbb{F}_p$ if it is the minimal polynomial over $\mathbb{F}_p$ of a primitive element of $\mathbb{F}_{p^n}$

8.38 **Remark** Each polynomial $\sum_{i=0}^{n} a_i x^i$ is written as a vector $a_n \cdots a_1 a_0$.

8.39 **Table** Primitive polynomials over $\mathbb{F}_2$.

n	Polynomials				
1	11				
2	111				
3	1011	1101			
4	10011	11001			
5	100101	101001	101111	110111	111011
	111101				
6	1000011	1011011	1100001	1100111	1101101
	1110011				
7	10000011	10001001	10001111	10010001	10011101
	10100111	10101011	10111001	10111111	11000001
	11001011	11010011	11010101	11100101	11101111
	11110001	11110111	11111101		
8	100011101	100101011	100101101	101001101	101011111
	101100011	101100101	101101001	101110001	110000111
	110001101	110101001	111000011	111001111	111100111
	111110101				
9	1000010001	1000011011	1000100001	1000101101	1000110011
	1001011001	1001011111	1001101001	1001101111	1001110111
	1001111101	1010000111	1010010101	1010100011	1010100101
	1010101111	1010110111	1010111101	1011001111	1011010001
	1011011011	1011110101	1011111001	1100010011	1100010101
	1100011111	1100100011	1100110001	1100111011	1101001111
	1101011011	1101100001	1101101011	1101101101	1101110011
	1101111111	1110000101	1110001111	1110110101	1110111001
	1111000111	1111001011	1111001101	1111010101	1111011001
	1111100011	1111101001	1111111011		
10	10000001001	10000011011	10000100111	10000101101	10001100101
	10001101111	10010000001	10010001011	10011000101	10011010111
	10011100111	10011110011	10011111111	10100001101	10100011001
	10100100011	10100110001	10100111101	10101000011	10101010111
	10101101011	10110000101	10110001111	10110010111	10110100001
	10111000111	10111100101	10111110111	10111111011	11000010011
	11000010101	11000100101	11000110111	11001000011	11001001111
	11001011011	11001111001	11001111111	11010001001	11010110101
	11011000001	11011010011	11011011111	11011111101	11100010111
	11100011101	11100100001	11100111001	11101000111	11101001101
	11101010101	11101011001	11101100011	11101111101	11110001101
	11110010011	11110110001	11111011011	11111110011	11111111001

8.40 Table Primitive polynomials over $\mathbb{F}_3$.

n	Polynomials							
1	11							
2	112	122						
3	1021	1121	1201	1211				
4	10012	10022	11002	11122	11222	12002	12112	12212
5	100021	100211	101011	101201	101221	102101	102211	110021
	110101	110111	111011	111121	111211	112001	112111	112201
	120001	120011	120221	121111	122021	122101		
6	1000012	1000022	1001012	1002022	1010212	1010222	1011022	1011122
	1012012	1012112	1020112	1020122	1021112	1022122	1100002	1101002
	1101112	1101212	1102202	1110122	1110202	1111012	1111112	1111222
	1112222	1120102	1120222	1121012	1121102	1121212	1122202	1200002
	1201202	1202002	1202122	1202222	1210112	1210202	1211212	1212022
	1212122	1212212	1220102	1220212	1221202	1222022	1222102	1222222

8.41 Table Primitive polynomials over $\mathbb{F}_5$.

n	Polynomials									
1	12	13								
2	112	123	133	142						
3	1032	1033	1042	1043	1102	1113	1143	1203	1213	1222
	1223	1242	1302	1312	1322	1323	1343	1403	1412	1442
4	10122	10123	10132	10133	10412	10413	10442	10443	11013	11023
	11032	11042	11113	11202	11212	11303	11342	11443	12013	12022
	12033	12042	12123	12203	12222	12302	12332	12433	13012	13023
	13032	13043	13133	13203	13232	13302	13322	13423	14012	14022
	14033	14043	14143	14202	14242	14303	14312	14413		

8.42 Table Primitive polynomials over $\mathbb{F}_7$.

n	Polynomials									
1	12	14								
2	113	123	125	135	145	153	155	163		
3	1032	1052	1062	1112	1124	1152	1154	1214	1242	1262
	1264	1304	1314	1322	1334	1352	1354	1362	1422	1432
	1434	1444	1504	1524	1532	1534	1542	1552	1564	1604
	1612	1632	1644	1654	1662	1664				
4	10135	10145	10333	10335	10343	10345	10433	10443	10515	10525
	10533	10543	10555	10565	10613	10623	10635	10645	10653	10663
	11013	11063	11103	11105	11153	11213	11223	11225	11233	11245
	11323	11355	11365	11405	11423	11443	11455	11463	11523	11533
	11545	11605	11625	11643	11653	11665	12025	12055	12123	12135
	12143	12203	12205	12253	12303	12323	12325	12363	12365	12403
	12435	12465	12553	12563	12643	12655	13015	13023	13053	13065
	13103	13115	13135	13155	13205	13213	13225	13243	13323	13345
	13355	13443	13445	13455	13465	13513	13525	13535	13553	13655
	14015	14023	14053	14065	14103	14125	14145	14165	14205	14233
	14255	14263	14325	14335	14353	14415	14425	14433	14435	14523
	14545	14555	14563	14625	15025	15055	15133	15145	15153	15203
	15205	15223	15303	15313	15315	15353	15355	15403	15415	15445
	15513	15523	15625	15633	16013	16063	16103	16105	16123	16235
	16243	16253	16255	16263	16315	16325	16353	16405	16413	16425
	16433	16453	16535	16543	16553	16605	16615	16623	16633	16655

8.43 Remark See Table VI.16.45 for additional primitive polynomials. The paper [1048] gives a primitive polynomial of degree n over $\mathbb{F}_p$ for each $p^n < 10^{50}$ with $p \leq 97$ a prime.

8.44 **Table** Primitive polymonials for extension fields over the ground fields $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_9$, and $\mathbb{F}_{16}$. Ground fields $\mathbb{F}_q$ are generated by a root of $f(y) = 0$. Extension fields $\mathbb{F}_{q^k}$ are generated by a root of $h(x) = 0$ given in the row headed by q^k and the column headed by q.

	$q = 4$	$q = 8$	$q = 9$	$q = 16$
$\mathbb{F}_q$	$f(y) = y^2 + y + 1$	$f(y) = y^3 + y + 1$	$f(y) = y^2 + 2y + 2$	$f(y) = y^4 + y + 1$
q^2	$x^2 + x + y$	$x^2 + yx + y$	$x^2 + x + y$	$x^2 + x + y^7$
q^3	$x^3 + x^2 + x + y$	$x^3 + x + y$	$x^3 + x + y$	$x^3 + x + y^7$
q^4	$x^4 + x^2 + yx + y^2$	$x^4 + x + y^3$	$x^4 + x + y^5$	$x^4 + x^2 + yx + y^2$
q^5	$x^5 + x + y$	$x^5 + x^2 + x + y^3$	$x^5 + x^2 + y$	$x^5 + yx + y^2$
q^6	$x^6 + x^2 + x + y$	$x^6 + x + y$	$x^6 + x^2 + yx + y$	
q^7	$x^7 + x^2 + yx + y^2$	$x^7 + x^2 + yx + y^3$	$x^7 + x + y$	
q^8	$x^8 + x^3 + x + y$			
q^9	$x^9 + x^2 + x + y$			
q^{10}	$x^{10} + x^3 + yx^2 + yx + y$			
q^{11}	$x^{11} + x^2 + x + y$			

8.45 **Example** For $\mathbb{F}_{4^2}$ in Table 8.44 note that $h(x) = x^2+x+y$, with y a root of $y^2+y+1 = 0$. If one takes x as a root of $h(x) = 0$, then $x^3 = x^2 + yx = (1 + y)x + y = y^2x + y$, $x^4 = y^2x^2 + yx = (y^2 + y)x + 1 = x + 1, \cdots, x^{15} = x^0 = 1$.

8.9 Factorizations of $\mathbf{x^n - 1}$

8.46 **Table** Factorizations of $x^n - 1$ over $\mathbb{F}_2$.

n	Factorizations
1	$x + 1$
2	$(x + 1)^2$
3	$(x^2 + x + 1)(x + 1)$
4	$(x + 1)^4$
5	$(x^4 + x^3 + x^2 + x + 1)(x + 1)$
6	$(x^2 + x + 1)^2(x + 1)^2$
7	$(x^3 + x^2 + 1)(x + 1)(x^3 + x + 1)$
8	$(x + 1)^8$
9	$(x^6 + x^3 + 1)(x^2 + x + 1)(x + 1)$
10	$(x^4 + x^3 + x^2 + x + 1)^2(x + 1)^2$
11	$(x + 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
12	$(x^2 + x + 1)^4(x + 1)^4$
13	$(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x + 1)$
14	$(x^3 + x^2 + 1)^2(x + 1)^2(x^3 + x + 1)^2$
15	$(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x^3 + 1)(x + 1)$
16	$(x + 1)^{16}$
17	$(x^8 + x^5 + x^4 + x^3 + 1)(x + 1)(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1)$
18	$(x^6 + x^3 + 1)^2(x^2 + x + 1)^2(x + 1)^2$
19	$(x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x + 1)$
20	$(x^4 + x^3 + x^2 + x + 1)^4(x + 1)^4$
21	$(x^3+x^2+1)(x^6+x^4+x^2+x+1)(x^2+x+1)(x^6+x^5+x^4+x^2+1)(x+1)(x^3+x+1)$
22	$(x + 1)^2(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^2$
23	$(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$
24	$(x^2 + x + 1)^8(x + 1)^8$
25	$(x^4 + x^3 + x^2 + x + 1)(x + 1)(x^{20} + x^{15} + x^{10} + x^5 + 1)$
26	$(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^2(x + 1)^2$

n	Factorizations
27	$(x^6+x^3+1)(x^2+x+1)(x+1)(x^{18}+x^9+1)$
28	$(x^3+x^2+1)^4(x+1)^4(x^3+x+1)^4$
29	$(x+1)(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}+x^{20}+x^{21}+x^{22}+x^{23}+x^{24}+x^{25}+x^{26}+x^{27}+x^{28})$
30	$(x^4+x+1)^2(x^4+x^3+x^2+x+1)^2(x^2+x+1)^2(x^4+x^3+1)^2(x+1)^2$
31	$(x^5+x^4+x^3+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^3+1)(x^5+x^4+x^3+x+1)(x+1)(x^5+x^2+1)(x^5+x^4+x^2+x+1)$
32	$(x+1)^{32}$
33	$(x^{10}+x^7+x^5+x^3+1)(x^2+x+1)(x^{10}+x^9+x^5+x+1)(x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
34	$(x^8+x^5+x^4+x^3+1)^2(x+1)^2(x^8+x^7+x^6+x^4+x^2+x+1)^2$
35	$(x^3+x^2+1)(x^4+x^3+x^2+x+1)(x^{12}+x^{10}+x^9+x^8+x^7+x^4+x^2+x+1)(x+1)(x^3+x+1)(x^{12}+x^{11}+x^{10}+x^8+x^5+x^4+x^3+x^2+1)$
36	$(x^6+x^3+1)^4(x^2+x+1)^4(x+1)^4$
37	$(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}+x^{20}+x^{21}+x^{22}+x^{23}+x^{24}+x^{25}+x^{26}+x^{27}+x^{28}+x^{29}+x^{30}+x^{31}+x^{32}+x^{33}+x^{34}+x^{35}+x^{36})(x+1)$
38	$(x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)^2(x+1)^2$
39	$(x^{12}+x^{11}+x^{10}+x^9+x^5+x^4+x^3+x^2+1)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)(x^{12}+x^{10}+x^9+x^8+x^7+x^3+x^2+x+1)(x^2+x+1)(x+1)$
40	$(x^4+x^3+x^2+x+1)^8(x+1)^8$
41	$(x^{20}+x^{19}+x^{17}+x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^6+x^4+x^3+x+1)(x^{20}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{11}+x^{10}+x^9+x^6+x^5+x^4+x^3+x^2+1)(x+1)$
42	$(x^3+x+1)^2(x^2+x+1)^2(x^6+x^4+x^2+x+1)^2(x^6+x^5+x^4+x^2+1)^2(x+1)^2(x^3+x^2+1)^2$
43	$(x^{14}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+1)(x^{14}+x^{12}+x^{10}+x^7+x^4+x^2+1)(x+1)(x^{14}+x^{13}+x^{11}+x^7+x^3+x+1)$
44	$(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)^4(x+1)^4$
45	$(x^6+x^3+1)(x^4+x^3+1)(x^2+x+1)(x^4+x+1)(x^{12}+x^3+1)(x^4+x^3+x^2+x+1)(x^{12}+x^9+1)(x+1)$
46	$(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)^2(x+1)^2(x^{11}+x^9+x^7+x^6+x^5+x+1)^2$
47	$(x^{23}+x^{19}+x^{18}+x^{14}+x^{13}+x^{12}+x^{10}+x^9+x^7+x^6+x^5+x^3+x^2+x+1)(x+1)(x^{23}+x^{22}+x^{21}+x^{20}+x^{18}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^9+x^5+x^4+1)$
48	$(x^2+x+1)^{16}(x+1)^{16}$
49	$(x^3+x+1)(x^{21}+x^{14}+1)(x^{21}+x^7+1)(x+1)(x^3+x^2+1)$
50	$(x^{20}+x^{15}+x^{10}+x^5+1)^2(x^4+x^3+x^2+x+1)^2(x+1)^2$

8.10 Cyclotomic Numbers for e = 2, 3, 5, and 7

8.47 Let $q = ef + 1$ be a prime power and let H be the subgroup of $\mathbb{F}_q^*$ of order f with $\{H = C_0, C_1, C_2, \ldots, C_{e-1}\}$ the set of (multiplicative) cosets of H in $\mathbb{F}_q^*$ (that is, $C_i = g^i C_0$ where g is the least primitive element of $\mathbb{F}_q$). The *cyclotomic number* (i, j) is $|\{x \in C_i : x + 1 \in C_j\}|$.

8.48 Theorem [1982] Some basic facts about cyclotomic numbers ($q = ef + 1$).

1. For any integers m, n $(i + me, j + me) = (i, j)$.
2. $$(i,j) = \begin{cases} (j,i) & \text{if } f \text{ is even} \\ (j + e/2, i + e/2) & \text{if } f \text{ is odd.} \end{cases}$$
3. $\sum_{j=0}^{e-1}(i,j) = f - \theta_i$ where $$\theta_i = \begin{cases} 1 & \text{if } f \text{ is even and } i = 0 \\ 1 & \text{if } f \text{ is odd and } i = e/2 \\ 0 & \text{otherwise.} \end{cases}$$

4. $\sum_{j=0}^{e-1}(i,j) = f - \alpha_j \quad$ where $\alpha_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{otherwise.} \end{cases}$.
5. The cyclotomic numbers $(0,h)$ are odd or even accordingly as $2 \in C_h$ or not. In particular, exactly one of the numbers $(0,j)$ is odd.

8.49 Theorem (see [1982]) Some connections between cyclotomic numbers and difference sets. (See §VI.18.)

1. C_0 is a difference set in $G = \mathbb{F}_q$ if and only if $\lambda = (i,0) = (f-1)/e$ for all $i = 0, 1 \ldots e-1$.
2. Fix e so that $q = ef+1$, and let C_0 correspond to e. If C_0 is a difference set in G, then e is even and f is odd.
3. $C_0 + \{0\}$ is a difference set in G if and only if $1 + (0,0) = (i,0) = (f+1)/e$ for all $i = 1, 2, \ldots (e-2)/2$.
4. Fix e so that $q = ef+1$, and let C_0 correspond to e. If $C_0 + \{0\}$ is a difference set in G, then e is even and f is odd.
5. If $q = 2f + 1 \equiv 3 \pmod 4$, then C_0 is a difference set in G.
6. If $q \equiv 1 \pmod 4$, then C_0 is a difference set in G if and only if $q = 1 + 4t^2$ (that is, if and only if $k = (q-1)/4$ is an odd square).

8.50 Table Cyclotomic numbers for $e = 2$ $(p = 2f+1)$.

	0	1
0	$(f-2)/2$	$f/2$
1	$f/2$	$f/2$

f even

	0	1
0	$(f-1)/2$	$(f+1)/2$
1	$(f-1)/2$	$(f-1)/2$

f odd

8.51 Table Cyclotomic numbers for $e = 3$ $(p = 3f+1)$.

	0	1	2
0	0	0	1
1	0	1	1
2	1	1	0

$p = 7$

	0	1	2
0	0	1	2
1	1	2	1
2	2	1	1

$p = 13$

	0	1	2
0	2	1	2
1	1	2	3
2	2	3	1

$p = 19$

	0	1	2
0	3	4	2
1	4	2	4
2	2	4	4

$p = 31$

	0	1	2
0	2	5	4
1	5	4	3
2	4	3	5

$p = 37$

	0	1	2
0	3	6	4
1	6	4	4
2	4	4	6

$p = 43$

	0	1	2
0	6	5	8
1	5	8	7
2	8	7	5

$p = 61$

	0	1	2
0	6	9	6
1	9	6	7
2	6	7	9

$p = 67$

	0	1	2
0	8	6	9
1	6	9	9
2	9	9	6

$p = 73$

	0	1	2
0	6	9	10
1	9	10	7
2	10	7	9

$p = 79$

	0	1	2
0	12	9	10
1	9	10	13
2	10	13	9

$p = 97$

	0	1	2
0	12	12	9
1	12	9	13
2	9	13	12

$p = 103$

8.52 Table Cyclotomic numbers for $e = 5$, $(p = 5f + 1)$.

	0	1	2	3	4
0	0	1	0	0	0
1	1	0	0	1	0
2	0	0	0	1	1
3	0	1	1	0	0
4	0	0	1	0	1

$p = 11$

	0	1	2	3	4
0	2	0	0	2	1
1	0	1	2	1	2
2	0	2	2	1	1
3	2	1	1	0	2
4	1	2	1	2	0

$p = 31$

	0	1	2	3	4
0	0	3	2	2	0
1	3	0	2	1	2
2	2	2	2	1	1
3	2	1	1	2	2
4	0	2	1	2	3

$p = 41$

	0	1	2	3	4
0	2	3	0	4	2
1	3	2	2	3	2
2	0	2	4	3	3
3	4	3	3	0	2
4	2	2	3	2	3

$p = 61$

	0	1	2	3	4
0	0	5	4	2	2
1	5	2	2	3	2
2	4	2	2	3	3
3	2	3	3	4	2
4	2	2	3	2	5

$p = 71$

	0	1	2	3	4
0	0	3	6	4	6
1	3	6	4	3	4
2	6	4	4	3	3
3	4	3	3	6	4
4	6	4	3	4	3

$p = 101$

	0	1	2	3	4
0	6	5	2	8	4
1	5	4	6	5	6
2	2	6	8	5	5
3	8	5	5	2	6
4	4	6	5	6	5

$p = 131$

	0	1	2	3	4
0	5	6	6	8	4
1	6	4	8	4	8
2	6	8	8	4	4
3	8	4	4	6	8
4	4	8	4	8	6

$p = 151$

	0	1	2	3	4
0	8	3	6	8	10
1	3	10	8	7	8
2	6	8	8	7	7
3	8	7	7	6	8
4	10	8	7	8	3

$p = 181$

8.53 Table Cyclotomic numbers for $e = 7$, $(p = 7f + 1)$.

	0	1	2	3	4	5	6
0	0	1	0	0	2	0	0
1	1	0	1	0	0	1	1
2	0	1	0	1	1	1	0
3	0	0	1	2	0	1	0
4	2	0	1	0	0	0	1
5	0	1	1	1	0	0	1
6	0	1	0	0	1	1	1

$p = 29$

	0	1	2	3	4	5	6
0	2	0	0	0	2	0	1
1	0	1	1	1	0	2	1
2	0	1	0	2	1	1	1
3	0	1	2	2	0	1	0
4	2	0	1	0	0	1	2
5	0	2	1	1	1	0	1
6	1	1	1	0	2	1	0

$p = 43$

	0	1	2	3	4	5	6
0	0	0	2	2	2	2	1
1	0	1	3	1	2	0	3
2	2	3	2	0	1	1	1
3	2	1	0	2	2	1	2
4	2	2	1	2	2	1	0
5	2	0	1	1	1	2	3
6	1	3	1	2	0	3	0

$p = 71$

	0	1	2	3	4	5	6
0	0	2	2	4	0	5	2
1	2	2	2	3	3	2	2
2	2	2	5	2	1	1	3
3	4	3	2	0	3	1	3
4	0	3	1	3	4	3	2
5	5	2	1	1	3	2	2
6	2	2	3	3	2	2	2

$p = 113$

	0	1	2	3	4	5	6
0	2	2	5	2	4	0	2
1	2	2	4	2	3	1	4
2	5	4	0	1	3	3	2
3	2	2	1	4	3	3	3
4	4	3	3	3	2	2	1
5	0	1	3	3	2	5	4
6	2	4	2	3	1	4	2

$p = 127$

	0	1	2	3	4	5	6
0	6	1	2	4	6	4	4
1	1	4	5	6	2	5	5
2	2	5	4	5	3	3	6
3	4	6	5	6	2	3	2
4	6	2	3	2	4	6	5
5	4	5	3	3	6	2	5
6	4	5	6	2	5	5	1

$p = 197$

	0	1	2	3	4	5	6
0	2	5	8	2	6	2	4
1	5	4	3	6	4	5	3
2	8	3	2	5	3	3	6
3	2	6	5	6	4	3	4
4	6	4	3	4	2	6	5
5	2	5	3	3	6	8	3
6	4	3	6	4	5	3	5

$p = 211$

	0	1	2	3	4	5	6
0	6	2	4	5	2	6	8
1	2	8	5	3	7	4	5
2	4	5	6	4	6	6	3
3	5	3	4	2	7	6	7
4	2	7	6	7	5	3	4
5	6	4	6	6	3	4	5
6	8	5	3	7	4	5	2

$p = 239$

	0	1	2	3	4	5	6
0	12	5	8	6	4	2	2
1	5	2	7	6	6	7	7
2	8	7	2	7	5	5	6
3	6	6	7	4	6	5	6
4	4	6	5	6	6	6	7
5	2	7	5	5	6	8	7
6	2	7	6	6	7	7	5

$p = 281$

8.11 Zech Logarithms for Prime Power Fields

8.54 Let α be a root of $p(x)$, a generator of the multiplicative group of elements of $\mathbb{F}_q$. The *Zech logarithm* is the function $Z : \{1, \ldots, p^n - 1\} \to \mathbb{Z}$ such that $\alpha^{Z(k)} = 1 + \alpha^k$. $Z(k) = \emptyset$ denotes $1 + \alpha^k = 0$.

8.55 **Remark** The Zech logarithm provides a direct method for adding elements α^i and α^j $(i > j)$ in $\mathbb{F}_q$, since $\alpha^i + \alpha^j = \alpha^j(\alpha^{i-j} + 1) = \alpha^j \cdot \alpha^{Z(i-j)}$. The values of the Zech logarithm function depend on the polynomial $p(x)$ used to obtain the field.

8.56 **Table** Zech logarithms for $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$, $\mathbb{F}_{2^5}$, $\mathbb{F}_{3^2}$, $\mathbb{F}_{3^3}$, $\mathbb{F}_{5^2}$, and $\mathbb{F}_{7^2}$ (generator polynomials are the same as given in Tables 8.26 through 8.29).

$\mathbb{F}_{2^3}$

k	1	2	3	4	5	6	7
$Z(k)$	3	6	1	5	4	2	$\emptyset$

$\mathbb{F}_{2^4}$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$Z(k)$	12	9	4	3	10	8	13	6	2	5	14	1	7	11	$\emptyset$

$\mathbb{F}_{2^5}$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$Z(k)$	14	28	5	25	3	10	16	19	24	6	23	20	30	1	22	7	18	17	8	12	27	15	11	9	4

k	26	27	28	29	30	31
$Z(k)$	29	21	2	26	13	$\emptyset$

$\mathbb{F}_{3^2}$

k	1	2	3	4	5	6	7	8
$Z(k)$	2	7	6	$\emptyset$	3	5	1	4

$\mathbb{F}_{3^3}$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
$Z(k)$	19	22	5	1	12	14	11	24	15	9	21	3	$\emptyset$	17	10	25	6	16	4	8	7	23	2	20	18	13

$\mathbb{F}_{5^2}$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
$Z(k)$	17	5	2	11	13	18	21	4	19	1	9	$\emptyset$	22	15	10	20	14	12	8	7	23	3	16	6

$\mathbb{F}_{7^2}$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
$Z(k)$	31	35	6	41	1	23	25	32	22	46	26	14	20	5	10	8	28	45	9	19	42	34	4	$\emptyset$

k	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$Z(k)$	29	12	21	47	38	27	11	40	43	39	7	2	15	36	13	24	18	17	44	37	3	33	30	16

References Cited: [995, 1048, 1827, 1982]

9 Finite Groups and Designs

Leo G. Chouinard II
Robert Jajcay
Spyros S. Magliveras

9.1 Introduction

9.1 A *group* $(P, \cdot)$ is a set P, together with a binary operation $\cdot$ on P, for which
1. if $x, y \in P$, then $x \cdot y \in P$;
2. an *identity* element $e \in P$ exists: $x \cdot e = e \cdot x = x$ for all $x \in P$;
3. $\cdot$ is *associative*: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in P$;
4. every element $x \in P$ has an *inverse*, an element x^{-1} for which $x \cdot x^{-1} = x^{-1} \cdot x = e$.

9.2 If $G = (P, \cdot)$ is a group, $Q \subseteq P$, and $H = (Q, \cdot)$ is also a group, then H is a *subgroup* of G, written $H \leq G$. It is *proper* if H is not the trivial group $\{e\}$, nor the whole group G. The *index* $[G : H]$ of H in G is $|G|/|H|$.

9.3 If G is a group and $H \leq G$, a *right coset* of H in G is any subset of the form $Hx = \{hx : h \in H\}$ for a fixed element $x \in G$. A *left coset* of H in G is similarly defined to be any subset of G of the form $xH = \{xh : h \in H\}$ for $x \in G$ fixed.

9.4 **Remarks** All groups and sets are assumed here to be finite. As is customary, the symbol 1 denotes the rational integer 1, the identity element of a group, as well as the trivial subgroup $\{1\}$. The meaning intended is always clear from the context. If G is a group and $H \leq G$, two right cosets Hx, Hy are identical if and only if $xy^{-1} \in H$; otherwise, they are disjoint. Hence, the number of distinct right cosets of H in G is $[G : H]$. Similarly, the number of distinct left cosets of H in G is $[G : H]$.

9.5 A *permutation* π on the set X is a one to one and onto mapping $\pi : X \to X$. The set of all permutations on X, with composition of functions as a binary operation, forms a group, the *symmetric group* on X. It is denoted by $Sym(X)$ or if $X = \{1, 2, \ldots, n\}$, by $\mathcal{S}_n$. If G is a subgroup of $Sym(X)$, then G is a *permutation group*.

9.6 **Examples** Permutation groups of particular importance in design theory arise from considering a graph, design, or geometry. A permutation of the vertices, elements, or points that "preserves the structure" is an *automorphism*. For example, a permutation on the elements of a simple BIBD is an automorphism when it maps blocks to blocks, and sets that are not blocks to sets that are also not blocks. The collection of all automorphisms forms a permutation group, the *automorphism group* of the structure.

9.7 **Remarks** Automorphism groups of combinatorial structures form a rich source of permutation groups. Although most combinatorial objects admit only the trivial automorphism or have very small automorphism groups, objects with large automorphism groups are elegant and sought after. Designs, graphs, and geometries with large groups are often the easiest to construct, and the first to be discovered among members of specified families. Moreover, such objects can be presented efficiently, frequently in terms of generators of their automorphism groups and certain base blocks.

9.8 A subgroup N of a group G is a *normal* subgroup, written $N \lhd G$, if $a^{-1}Na \subseteq N$ for every $a \in G$.

9.9 A nontrivial group is *simple* if it has no proper, normal subgroups.

9.10 If $N \lhd G$, then, for each $x \in G$, the right coset Nx is identical with the left coset xN, and Nx is a *coset* of N in G. If $N \lhd G$, the collection G/N of all distinct cosets of N forms a group under the operation $Nx \cdot Ny = Nxy$, the *quotient* or *factor* group of G modulo N.

9.11 A *normal series* of a group G is a chain of subgroups

$$1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

whose *factor groups* are G_i/G_{i+1} for $0 \leq i < n$.

9.12 A finite group is *solvable* when it has a normal series in which each factor group is cyclic of prime order.

9.13 The *socle* of a group G is the subgroup generated by the union of all *minimal normal* subgroups of G.

9.14 Remarks A number of references and computational tools were of considerable help in deriving structural information and completing Tables 9.62 and 9.66. The *Atlas* [598] was of particular utility, especially for the information on the primitive spectrum of those simple groups in the list that are included in the *Atlas*. An updated version of the *Atlas* was reprinted in 2003, and much of the data is presently maintained online at [2143]. Of utility also were the libraries of groups in the algebraic computational systems `Magma` [434] and `Gap` [1681], as well as standard references [702, 933, 1014, 2137]. To obtain and check the results, extensive computations were undertaken on a number of workstations, with the computational package `Pythia`, developed by Chouinard and Magliveras, as well as the computational algebra systems `Magma` and `Gap`.

9.2 Permutation Groups

9.15 A *group action* is a triple (X, G, exp), where X is a set, G a group, and $exp : X \times G \to X$ a mapping written as exponentiation, $((x, g) \mapsto x^g)$, such that:

1. $x^1 = x$ for any $x \in X$, where 1 is the identity of G, and
2. $(x^g)^h = x^{(gh)}$ for any $x \in X$, and any $g, h \in G$.

The notation (X, G, exp) is abbreviated to $G|X$. If $G|X$ is a group action, then $|X|$ is the *degree* of $G|X$.

9.16 Example (right regular action) Let G be any group, and let $X = G$. Define an action $G|X$ by $(x, g) \mapsto xg$. Now, (1) and (2) are satisfied since $x \cdot 1 = x$, and $(xg)h = x(gh)$.

9.17 Example (permutation groups) Let G be a permutation group, a subgroup of the symmetric group $\mathcal{S}_n$. If $x \in X$, and $g \in G$, let $x^g = g(x)$.

9.18 Example (right action on cosets) Let G be a group, $H \leq G$, and $\Omega = \{Hx_i : x_i \in G\}$ be the collection of all distinct right cosets of H in G. One can check that the mapping $(Hx, g) \mapsto Hxg$ defines an action $G|\Omega$.

9.19 Remark The action in Example 9.16 is a special case of the action in Example 9.18, where H is the identity subgroup of G.

9.20 Example Let $G|X$ be a group action. Then G acts on the collection of all k-subsets of X in a natural way. For $S \subseteq X$ and $g \in G$, define S^g by $S^g = \{x^g : x \in S\}$. Some

beautiful designs constructed in this way are given in §VI.24, where the symmetric group is acting on the set of all 2-subsets of a set of size n.

9.21 **Example** (G acts on G by conjugation) Let G be any group, and let $X = G$. Define $exp : X \times G \to X$ by $x^g = g^{-1}xg$.

9.22 Let $G|X$ be a group action and let $x \in X$. Then the *orbit of x under G* is $x^G = \{x^g : g \in G\}$. The orbits under G partition X. The *stabilizer of x in G* is $G_x = \{g \in G : x^g = x\}$.

9.23 **Proposition** G_x is a subgroup of G, and when G is finite, $|G| = |x^G| \cdot |G_x|$.

9.24 Let $G|X$ be a group action and let $g \in G$. The set of all elements of X *fixed* by g, $\{x \in X : x^g = x\}$, is denoted by $Fix(g)$. The cardinality of $Fix(g)$ is the *character* of g, denoted by $\chi_{G|X}(g)$ or simply $\chi(g)$, and the mapping $\chi : g \mapsto \chi(g)$ is the *character* of the group action.

9.25 The *kernel* of a given group action $G|X$, denoted by $ker(G|X)$, is the set $\{g \in G : Fix(g) = X\}$. Then $ker(G|X)$ is a normal subgroup of G. $G|X$ is *faithful* if and only if $|ker(G|X)| = 1$.

9.26 **Example** A permutation group is a faithful group action.

9.27 In a group G, two elements x, y are *conjugate* if and only if $x = y^g = g^{-1}yg$ for some $g \in G$. Thus, two elements are conjugate if and only if they are in the same G-orbit in the action of Example 9.21. The G-orbits of G in the action of Example 9.21 are the *conjugacy classes* of G. G is the disjoint union of its conjugacy classes: $G = K_1 + K_2 + \cdots + K_c$ and c is the *class number* of G. Similarly, two subgroups $H_1, H_2 \leq G$ are *conjugate* in G (denoted by $H_1 \sim H_2$) if and only if $H_1 = H_2^g$ for some $g \in G$.

9.28 A group action $G|X$ is *transitive* if and only if X is a single G-orbit. Thus, $G|X$ is transitive if and only if for any two elements $x, y \in X$ there exists a group element $g \in G$ such that $x = y^g$.

9.29 **Remarks** If G is a group and $H \leq G$, the action described in Example 9.18 is transitive. Moreover, any transitive action $G|X$ is isomorphic to one of the type described in Example 9.18. If G is a group and $H_1, H_2 \leq G$, then the two actions of G on the two collections of right cosets of H_1, and H_2, respectively, are isomorphic if and only if the two subgroups H_1 and H_2 are conjugate. These observations are fundamental for the determination of all inequivalent transitive permutation representations of a group.

9.30 If $G|X$ is a permutation group, G is $\frac{1}{2}$-*transitive* or *semi-regular* if all G-orbits of X are of length $|G|$. G is *regular* or *sharply transitive* on X if G is transitive and semi-regular.

9.31 G is *k-transitive* (or *k-fold transitive*) on X if the induced action of G on the collection of all ordered k-subsets of X is transitive. $G|X$ is *k-homogeneous*, or *k^*-transitive*, if G is transitive on the k-subsets of X.

9.32 G is *sharply k-transitive* (*sharply k-homogeneous*) on X if G is *k-transitive* (*k-homogeneous*) on X and the stabilizer in G of an ordered (unordered) k-subset of X is the identity subgroup.

9.33 **Remarks** $G|X$ is k-transitive if and only if $G_x|(X - \{x\})$ is $(k-1)$-transitive for each $x \in X$. If $G|X$ is k-transitive, then it is k-homogeneous. Surprisingly, the converse is also true when $k \geq 5$ [1479]. See Theorem 9.52.

9.34 A permutation group $G|X$ is of *type* k^* if it is k^*-transitive, but not k-transitive. If $G|X$ is a transitive permutation group, the *rank* of G is the number of orbits of G_x on X.

9.35 Let $G|X$ be a transitive group action. A subset Δ of X is a *block of imprimitivity* if for any $g \in G$, $\Delta \cap \Delta^g = \Delta$ or $\emptyset$. The subsets $\emptyset, X$ and the singleton sets $\{x\}, x \in X$ are always blocks of imprimitivity for $G|X$, the *trivial* blocks. If the only blocks of imprimitivity for $G|X$ are the trivial ones, then $G|X$ is a *primitive* action.

9.36 **Remarks** A combinatorial design having an automorphism group that is transitive on its points necessarily has isomorphic derived structures with respect to any two points. Thus transitive permutation groups are important to design theory. A transitive permutation group is either primitive or imprimitive. In Tables 9.62 and 9.63, the primitive groups of degree up to 50 are presented. Transitive imprimitive groups have primitive homomorphic images of degree dividing the degree of the given group; Proposition 9.37 shows how imprimitive groups can be reduced to primitive groups of smaller degree. Intransitive groups can be formed as subdirect products of transitive groups ([1014], p.63).

9.37 **Proposition** Let Δ be a nontrivial block of imprimitivity of the imprimitive group action $G|X$ and set $\Omega = \{\Delta_1, \ldots, \Delta_m\} = \Delta^G$, the orbit of Δ under G. Then

1. Ω is a partition of X, a *system of imprimitivity*.
2. If for each $g \in G$ one defines $\bar{g} : \Omega \mapsto \Omega$ by
$$\bar{g} = \begin{pmatrix} \Delta_1 & \Delta_2 & \cdots & \Delta_m \\ \Delta_1^g & \Delta_2^g & \cdots & \Delta_m^g \end{pmatrix},$$
then $\bar{G} = \{\bar{g} : g \in G\}$ forms a permutation group on Ω and $g \mapsto \bar{g}$ is a homomorphism of G onto $\bar{G}$,
3. $\bar{G}$ is transitive on Ω and is isomorphic to G/N where N is the set of permutations in G that fix each of $\Delta_1, \Delta_2, \ldots, \Delta_m$ as sets; that is, the kernel of the homomorphism $g \mapsto \bar{g}$. N is the *kernel of imprimitivity* for this system of imprimitivity.

9.38 **Proposition** If $G|X$ is a transitive group action and $x, y \in X$, then the respective stabilizer subgroups G_x and G_y are conjugate in G. Moreover, $G|X$ is primitive if and only if G_x is a maximal subgroup of G.

9.39 For k a positive integer, G is $(k + \frac{1}{2})$-*transitive* if the stabilizer of each $x \in X$ is $(k - \frac{1}{2})$-transitive on $X - \{x\}$. G is $(k+1)$-*primitive* if G_x is k-primitive on $X - \{x\}$.

9.40 **Theorem** (Zassenhaus, 1934; Tits, 1952; Huppert, 1962) Let p be an odd prime, and m any odd positive integer. Then there is a unique sharply 3-transitive group of degree $p^m + 1$, namely $\mathrm{PGL}_2(p^m)$. If m is even, then there are precisely two sharply 3-transitive groups of degree $p^m + 1$. These groups are $\mathrm{PGL}_2(p^m)$ and $\mathrm{P\Delta L}_2(p^m)$. If $p = 2$, and m is a positive integer, then $L_2(2^m)$ is the unique sharply 3-transitive group of degree $p^m + 1 = 2^m + 1$.

9.41 **Remark** (Feit, 1960; Ito, 1962; Suzuki, 1962) All doubly transitive groups that contain an element fixing exactly two points but no element except for the identity fixing more than two points have been determined. These all have degree $p^m + 1$, or 2^p, where p is a prime.

9.42 **Theorem** (Huppert) Every solvable, primitive group of degree $1 + p$, p a prime, is 2-transitive. Solvability is a necessary condition.

9.43 **Theorem** (Jordan) If G is a primitive solvable permutation group, then its degree is a prime power p^a, and it contains a normal, elementary abelian subgroup N of order

p^a. If A is a transitive abelian subgroup of G, then $p > 3$ implies that $A = N$. When $p = 3$, A is elementary abelian.

9.44 Theorem (Jordan) If $G|X$ is k-transitive ($k \geq 2$) and N is a proper normal subgroup of G, then N is $(k-1)$-transitive, except when G is the symmetric group on X, or if $|X|$ is a power of 2 and $k = 3$.

9.45 Theorem (Ito) Let G be $(k + \frac{1}{2})$-transitive on X, and let N be a nonregular normal subgroup of G, then N is k-transitive, except possibly when $k = 1$ or 2.

9.46 Theorem (Wielandt and Huppert) If G is k-primitive, then a nonregular normal subgroup is k-transitive.

9.47 Theorem (Ito) For $k > 2$, a nonregular normal subgroup of a k-transitive permutation group $G|X$ is $(k-1)$-primitive.

9.48 An *isomorphism* from group $(P, \cdot)$ to group $(Q, \circ)$ is a one-to-one correspondence $\phi : P \to Q$ for which $\phi(x \cdot y) = \phi(x) \circ \phi(y)$ for all $x, y \in P$. An *automorphism* is an isomorphism from a group onto itself. The automorphism is *inner* if it is conjugation ($x \mapsto a^{-1}xa$) by a fixed group element $a \in G$; otherwise, it is an *outer automorphism*. The collection of all automorphisms of a group G is a subgroup of $Sym(G)$, denoted by $Aut(G)$. The inner automorphisms of G form a normal subgroup $I(G)$ of $Aut(G)$. The quotient group $Aut(G)/I(G)$ is the *outer automorphism* group of G.

9.49 Theorem (Nagao) Let G be a 6-transitive permutation group of degree n. If the outer automorphism group of every simple subgroup of G is solvable, then G is $\mathcal{S}_n$ or $\mathcal{A}_n$.

9.50 Theorem The outer automorphism group of every finite simple group is solvable. (This was known as the *Schreier conjecture*.)

9.51 Remark Theorem 9.50 has been proved using the classification theorem of finite simple groups. No proof has yet been found that does not use the classification theorem.

9.52 Theorem (O'Nan) If G is a nontrivial t-transitive group for which the composition factors of all its proper subgroups have solvable outer automorphism groups, then $t \leq 5$. Hence, there do not exist 6-transitive groups, except for $\mathcal{S}_n$ and $\mathcal{A}_n$.

9.53 Theorem (Wagner) If $G|X$ is 3-transitive and $|X| > 3$ is odd, then any nontrivial normal subgroup of G is also 3-transitive on X.

9.54 A permutation group $G|X$ is *set-transitive* if it is k-homogeneous for each $k \leq |X|$.

9.55 Theorem (Beaumont and Peterson) Apart from $\mathcal{S}_n$ and $\mathcal{A}_n$, there are exactly four set-transitive groups:

1. a metacyclic group of degree 5 and order 20;
2. a group $G \cong \mathcal{S}_5$ represented on six points;
3. $L_2(8)$ of order 504, represented on nine points; and
4. $\mathrm{P\Gamma L}_2(8) = Aut(L_2(8))$ of order 1512, represented on nine points.

9.56 Theorem (Livingstone and Wagner) If $G|X$ is a permutation group of degree n, and $2 < k \leq n/2$, then the number of G-orbits on unordered k-sets is at least the number of G-orbits on ordered $(k-1)$-sets. Thus if G is k^*-transitive, then it must be $(k-1)$-transitive. When $k \geq 5$, G must also be k-transitive.

9.57 Remark (Livingstone and Wagner) Permutation groups $G|X$ of type k^* exist only for $k = 2, 3$, and 4.

9.58 Theorem (Kantor) If $G|X$ is of type 4^*, and G_x is odd, then $G \cong L_2(5)$, $\mathrm{PGL}_2(5)$, $L_2(8)$, $\mathrm{P\Gamma L}_2(8)$, or $\mathrm{P\Gamma L}_2(32)$, in their usual permutation representations.

9.3 Groups and Group Operations

9.59 Table Notation for group operations and names for groups.

Symbol	Description
Operations on Groups:	
$A \times B$	The *direct product* of groups A and B.
A^n	The group $A^{n-1} \times A$, where A is a group, and n a positive integer.
$A \cdot B$	A *semidirect* product (*split extension*) of A by B (the action of B by conjugation on the normal subgroup A is not specified here).
$\mathbb{Z}_m \cdot_j \mathbb{Z}_n$	The semidirect product where the action of a generator of $\mathbb{Z}_n$ on $\mathbb{Z}_m$ is multiplication by $j \in \mathbb{Z}_m$.
$A \backslash B$	A general extension of A whose factor group by the normal subgroup A is B, but which is not a semidirect product of A by B.
$A \wr B$	The wreath product of A by B (which is isomorphic to some $A^n \cdot B$, $B \leq \mathcal{S}_n$).
$\mathcal{A}_n \cap H$	When H is a subgroup of $\mathcal{S}_n$ and contains odd permutations, the subgroup of index 2 in H consisting of the even permutations.
Basic Groups:	
1	The trivial group.
$\mathbb{Z}_n$	The cyclic group of order n.
D_n	The dihedral group of order $2n$.
$\mathcal{S}_n$	The symmetric group on a set of n elements.
$\mathcal{A}_n$	The alternating group on a set of n elements.
V_q	The elementary abelian group of order q, q a prime power.
Q_8	The quaternion group of order 8.
Linear Groups (q a prime power):	
$\mathrm{GL}_n(q)$	The general linear group of all invertible matrices of dimension n over $\mathbb{F}_q$. This is equivalent to the group of $\mathbb{F}_q$-automorphisms of vector space $V = \mathbb{F}_q^n = \mathbb{F}_q \oplus \cdots \oplus \mathbb{F}_q$.
$\mathrm{AGL}_n(q)$	The group of *affine* transformations on V of the form $x \mapsto Ax + b$, where $A \in \mathrm{GL}_n(q)$ and $b \in \mathbb{F}_q^n$. Thus, $\mathrm{AGL}_n(q) \cong \mathbb{F}_q^n \cdot \mathrm{GL}_n(q)$.
$F_{q,v}$	The subgroup of $\mathrm{AGL}_1(q)$ of order $q \cdot v$ of transformations of the form $x \mapsto Ax+b$ where $A^v = 1 \in \mathbb{F}_q$ and $b \in \mathbb{F}_q$. This is also known as the *Frobenius* group of order qv.
$\mathrm{SL}_n(q)$	The *special linear* group of dimension n over $\mathbb{F}_q$, the group of transformations of determinant 1 in $\mathrm{GL}_n(q)$.
$\mathrm{ASL}_n(q)$	The extension $\mathbb{F}_q^n \cdot \mathrm{SL}_n(q) < \mathrm{AGL}_n(q)$.
$L_n(q)$	(or $\mathrm{PSL}(n, \mathbb{F}_q)$ or $\mathrm{PSL}_n(q)$ or $\mathrm{LF}_n(q)$) The projective special linear group formed by taking $\mathrm{SL}_n(q)$ modulo its center.
$\mathrm{PGL}_n(q)$	$\mathrm{GL}_n(q)$ modulo its center.
$\Gamma\mathrm{L}_n(q)$	For $q = p^a$, p a prime, $a > 1$, the extension of $\mathrm{GL}_n(q)$ by the Galois group of $\mathbb{F}_q$ over $\mathbb{F}_p$.
$\Sigma\mathrm{L}_n(q)$	For $q = p^a$, p a prime, $a > 1$, the extension of $\mathrm{SL}_n(q)$ by the Galois group of $\mathbb{F}_q$ over $\mathbb{F}_p$. $\mathrm{A}\Gamma\mathrm{L}_n(q)$, $\mathrm{A}\Sigma\mathrm{L}_n(q)$, $\mathrm{P}\Gamma\mathrm{L}_n(q)$ and $\mathrm{P}\Sigma\mathrm{L}_n(q)$ are similarly defined from these.
$\mathrm{P}\Delta\mathrm{L}_2(q)$	If $p \neq 2$ and $q = p^2$, then $\mathrm{P}\Gamma\mathrm{L}_2(q) \cong \mathrm{PSL}_2(q) \cdot V_4$ contains three extensions of the form $\mathrm{PSL}_2(q) \cdot \mathbb{Z}_2$. Two of these are $\mathrm{PGL}_2(q)$ and $\mathrm{P}\Sigma\mathrm{L}_2(q)$. J.H. Conway suggested denoting the third extension of this sort by $\mathrm{P}\Delta\mathrm{L}_2(q)$ (the *diagonal* of the other two).

Symbol	Description
$U_n(q)$	(or $\mathrm{PSU}_n(q)$, or $\mathrm{PSU}_n(q^2)$) The *projective special unitary* group, a subgroup of $L_n(q^2)$.
$S_{2n}(q)$	(or $\mathrm{PSp}_{2n}(q)$) The *projective symplectic* group, a subgroup of $L_{2n}(q)$.
Lie Type and Sporadic Simple Groups:	
$Sz(8)$, $Sz(32)$	The *Suzuki* groups of orders 29,120 and 32,537,600, respectively.
$G_2(3)$	The Chevalley group of order 4,245,696.
$R(2)'$	($\cong {}^2F_4(2)'$) The *Ree–Tits* group of order 17,971,200.
M_n	for $n = 11, 12, 22, 23, 24$, the five well-known Mathieu simple groups.
J_a	The smallest Janko group, of order 175,600 with smallest transitive representation of degree 266.
HaJ	The *Janko–Hall* group of order 604,800 with minimal transitive representation on 100 points.
J_3	The Janko–Higman–McKay sporadic simple group of order 50,232,960.
HS	The *Higman–Sims* simple group of order 44,352,000.

9.4 Primitive Groups

9.60 Remarks Primitive permutation groups are the building blocks from which all permutation groups can be constructed. Primitive permutation groups are particularly useful in constructing combinatorial designs and finite geometries. A classification of these groups, afforded by the O'Nan–Scott Theorem [1450], divides them into two types: those with *solvable socle* (the *affine groups*) and those with *nonsolvable socle*. The primitive permutation groups with nonsolvable socle of degree at most 1000 were determined in 1988 [732]. The decade 1995–2005 has witnessed significant advances in computational group theory and specifically permutation group algorithms. During the same period, strong advances in computing hardware have made available considerable and inexpensive computing power. In [1816] all primitive permutation groups of degree less than 2500 are determined. In [772] all solvable primitive permutation groups of degree at most 6560 are determined. This section presents only the primitive permutation groups of degree at most 50. The computational complexity of constructing combinatorial designs/geometries is exponential in $\binom{n}{k}/g$ where $n = v$ is the degree of the permutation group (also the number of points of the design sought), k the block size, and g the group order.

9.61 Remark Table 9.62 contains information about the *primitive* groups of degree at most 50. Table 9.63 lists permutations that generate the groups in Table 9.62.

Table 9.62 has eight columns. The first column is an index of the form $d.i$, where d is the degree of the primitive permutation group and i is a serial index distinguishing primitive groups of the same degree. Column 2 contains the *name* of the group, which often also provides structural information about the group. Column 3 contains the *order* of the group. Column 4 provides information about the *depth* of transitivity of the group. For example, 3p! indicates that the group is *sharply 3-primitive*. The "p" notation indicates primitivity, the numeral 3 indicates the depth (the stabilizer of a point is 2-primitive on $d-1$ points), and the exclamation mark indicates that the stabilizer of two points is sharply primitive (hence, also regular) on $d-2$ points. A notation such as 3t! means that the group is sharply 3-transitive. Similarly, 3t indicates that the group is 3-transitive, 3* that the group is 3-homogeneous, while 3*! indicates that the group is sharply 3-homogeneous. If the group is 1-primitive but

not 2-primitive, then the stabilizer of a point is not primitive on $d-1$ points, and in these cases the orbit lengths for the action of the point-stabilizer are provided. For example, group 15.1 ($\mathcal{A}_6$ acting on 15 points) is just primitive but not 2-primitive. The stabilizer of a point, which happens to be isomorphic to $\mathcal{S}_4$, has 3 orbits on points, of lengths 1, 6, and 8. A superscript over an orbit length indicates the number of times that orbit length is encountered, so, for example, for group 16.1 column 4 contains $[1, 5^3]$, which means that the stabilizer of a point has 3 orbits of length 5, besides the fixed point.

Column 5 specifies generators of the group in the current primitive representation. When a generator is labeled in the form a_k, it is the *canonical* element of order k and degree d. This means that one starts writing cycles of length k, encompassing serially the points $1, 2, \cdots, d$ for as long as one can. If k does not divide d, then the last res points are left fixed, where res is the remainder of the division of d by k. For example, for group 10.8, $a_5 = (1,2,3,4,5)(6,7,8,9,10)$, while for group 15.5, $a_7 = (1,2,3,4,5,6,7)(8,9,10,11,12,13,14)(15)$. Other generators are listed in Table 9.63 under the relevant degree. The subscript of a generator indicates its order. An exponent over a specified generator, such as in a_{14}^2 for group 14.1, has the usual meaning. A generator listed in the form $ax+b$ simply indicates the element $x \mapsto ax+b$ over the Galois field $\mathbb{F}_p$ where $d = p$. Every primitive group listed has been given as a two-generator group except group 25.11, which is not a two-generator group.

Column 6 describes the structure of the stabilizer of a point for the specific group. If group G is at least 2-primitive on X, the point stabilizer G_x, $x \in X$, is primitive on $X - \{x\}$ and can be described by referring to an entry in Table 9.62. This is the case, for example, for all primitive groups of degree 12. When the stabilizer of a point G_x is not primitive on the remaining points $X - \{x\}$, it is sometimes possible to describe G_x as being isomorphic (as an abstract group) to an earlier group in the table. For example, the group $G = M_{21} \cong L_3(4)$, of index 21.4, is doubly transitive, with point stabilizer G_x which is imprimitive on 20 points. Here, a nontrivial system of imprimitivity consists of a set of 5 blocks, each of size 4, and G_x is a split extension of the kernel of imprimitivity V_{16}, by the image of imprimitivity $\mathcal{A}_5$. If G_x is represented on the cosets of (maximal) $\mathcal{A}_5$, then G_x is a primitive group of degree 16, and is isomorphic to the group 16.11. Similar is the meaning of symbol $\approx$ in column 6 for groups 21.5, 21.6, and 21.7.

Column 7 describes the lattice of the groups appearing as primitive groups for a specific degree, under *conjugate subgroup inclusion*. In most cases groups are represented so that any conjugate subgroup inclusion is in fact a *subgroup inclusion*. The indices that appear in this column refer to groups under the same degree. For example, group 37.1 is contained in groups 37.2 and 37.3 and Group 37.2 is in groups 37.4 and 37.5, and so on. In a few cases, a specific conjugate inclusion is given, as for group 16.12.

In the eighth column, examples of combinatorial structures are given whose full automorphism group is the group listed in the second column of the same row. A *strongly regular graph* with parameters v, k, λ, μ is denoted by $\mathrm{srg}(v, k, \lambda, \mu)$. A t-(v, k, λ) design is denoted by $S_\lambda(t, k, v)$. All t-(v, k, λ) designs listed are simple. $PG_n(q)$ denotes the *projective space* of (projective) dimension n over the field of q elements. This list of combinatorial structures is by no means complete!

Table 9.63 displays generators for the groups of Table 9.62. The amount of data needed to specify group generators is minimized, by listing as few permutations as possible in Table 9.63 for each specific degree, and by generating various groups by powers of elements listed in Table 9.63, or powers of canonical elements. This provides economy in representation of the data. For example, although there are 22 primitive groups of degree 16, only six permutations of degree 16 need be listed in Table 9.63.

9.62 Table Primitive groups of degree at most 50.

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
5.1	$\mathbb{Z}_5$	5	$[1^5]$	$a_5 : x+1$	1	2	
.2	D_5	10	$[1,2^2]$	$x+1, -x$	$\mathbb{Z}_2$	3, 4	
.3	$\mathrm{AGL}_1(5)$	20	2t!	$x+1, 2x$	$\mathbb{Z}_4$	5	
.4	$\mathcal{A}_5$	60	3p!	a_3, a_5	$\mathcal{A}_4$	5	
.5	$\mathcal{S}_5$	120	5p!	a_4, a_5	$\mathcal{S}_4$		
6.1	$L_2(5) \cong \mathcal{A}_5$	60	2p	a_5, b_3	5.2	2, 3	
.2	$\mathrm{PGL}_2(5) \cong \mathcal{S}_5$	120	3t!	a_5, b_6	5.3	4	
.3	$\mathcal{A}_6$	360	4p!	a_3, a_5	5.4	4	
.4	$\mathcal{S}_6$	720	6p!	a_5, a_6	5.5		
7.1	$\mathbb{Z}_7$	7	$[1^7]$	$a_7 : x+1$	1	2, 3	
.2	D_7	14	$[1,2^3]$	$x+1, -x$	$\mathbb{Z}_2$	4	
.3	$F_{7,3}$	21	2*!	$x+1, 2x$	$\mathbb{Z}_3$	4, 5	
.4	$\mathrm{AGL}_1(7)$	42	2t!	$x+1, 3x$	$\mathbb{Z}_6$	7	
.5	$L_3(2)$	168	2t	a_7, b_7	$\mathcal{S}_4$	6	$S_1(2,3,7)$
.6	$\mathcal{A}_7$	2520	5p!	a_3, a_7	6.3	7	
.7	$\mathcal{S}_7$	5040	7p!	a_6, a_7	6.4		
8.1	$\mathrm{AGL}_1(8)$	56	2p!	a_7, b_7	7.1	2	
.2	$V_8 \cdot F_{7,3}$	168	3*	a_7, b_6	7.3	5	
.3	$L_2(7) \cong L_3(2)$	168	3*	a_7, c_7	7.3	4, 6	
.4	$\mathrm{PGL}_2(7)$	336	3t!	a_7, b_8	7.4	7	
.5	$\mathrm{AGL}_3(2)$	1344	3t	a_7, d_7	7.5	7	$S_1(3,4,8)$
.6	$\mathcal{A}_8$	20160	6p!	a_4, a_7	7.6	7	
.7	$\mathcal{S}_8$	40320	8p!	a_7, a_8	7.7		
9.1	$F_{9,4}$	36	$[1,4^2]$	d_4, e_4	$\mathbb{Z}_4$	2,3,4	
.2	$V_9 \cdot D_4$	72	$[1,4^2]$	f_6, g_6	D_4	5	
.3	$\mathrm{AGL}_1(9)$	72	2t!	b_3, c_8	$\mathbb{Z}_8$	5	
.4	$V_9 \cdot Q_8$	72	2t!	b_4, c_4	Q_8	5, 6	
.5	$V_9 \cdot (\mathbb{Z}_8 \cdot_3 \mathbb{Z}_2)$	144	2t	c_8, e_6	$\mathbb{Z}_8 \cdot_3 \mathbb{Z}_2$	7	
.6	$V_9 \cdot (Q_8 \cdot \mathbb{Z}_3)$	216	2t	c_6, d_6	$Q_8 \cdot \mathbb{Z}_3$	7, 10	
.7	$\mathrm{AGL}_2(3)$	432	2t	a_8, b_8	$\mathrm{GL}_2(3)$	11	$S_1(2,3,9)$
.8	$L_2(8)$	504	4*	a_9, b_9	8.1	9	
.9	$\mathrm{P\Gamma L}_2(8)$	1512	4*	a_9, b_6	8.2	10	
.10	$\mathcal{A}_9$	9!/2	7p!	a_4, a_9	8.6	11	
.11	$\mathcal{S}_9$	9!	9p!	a_8, a_9	8.7		

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
10.1	$\mathcal{A}_5$	60	[1,3,6]	b_3, d_5	$\mathcal{S}_3$	2, 3	$S_2(2,3,10)$
.2	$\mathcal{S}_5$	120	[1,3,6]	b_6, d_5	D_6	4	srg$(10,3,0,1)$
.3	$L_2(9) \cong \mathcal{A}_6$	360	2p	b_5, c_5	9.1	4, 5, 6	
.4	$\mathrm{P\Sigma L}_2(9) \cong \mathcal{S}_6$	720	2p	b_6, c_6	9.2	7	$S_2(2,4,10)$
.5	$\mathrm{P\Delta L}_2(9) \cong M_{10}$	720	3t!	c_8, d_8	9.4	7	$S_3(3,5,10)$
.6	$\mathrm{PGL}_2(9)$	720	3t!	a_{10}, b_{10}	9.3	7	
.7	$\mathrm{P\Gamma L}_2(9)$	1440	3t	a_{10}, b_8	9.5	9	$S_1(3,4,10)$
.8	$\mathcal{A}_{10}$	10!/2	8p!	a_5, a_9	9.10	9	
.9	$\mathcal{S}_{10}$	10!	10p!	a_9, a_{10}	9.11		
11.1	$\mathbb{Z}_{11}$	11	$[1^{11}]$	$a_{11} : x+1$	1	2, 3	
.2	$F_{11,2}$	22	$[1,2^5]$	$x+1,\ -x$	$\mathbb{Z}_2$	4	
.3	$F_{11,5}$	55	2*!	$x+1,\ 4x$	$\mathbb{Z}_5$	4, 5	
.4	$\mathrm{AGL}_1(11)$	110	2t	$x+1,\ 2x$	$\mathbb{Z}_{10}$	8	
.5	$L_2(11)$	660	2p	a_{11}, b_5	10.1	6	$S_2(2,5,11)$
.6	M_{11}	7920	4t!	a_{11}, b_{11}	10.5	7	$S_1(4,5,11)$
.7	$\mathcal{A}_{11}$	11!/2	9p!	a_5, a_{11}	10.8	8	
.8	$\mathcal{S}_{11}$	11!	11p!	a_{10}, a_{11}	10.9		
12.1	$L_2(11)$	660	3*	a_{11}, d_{11}	11.3	2,3	
.2	$\mathrm{PGL}_2(11)$	1320	3t!	a_{12}, b_{12}	11.4	6	
.3	M_{11}	7920	3p	a_{11}, c_{11}	11.5	4	
.4	M_{12}	95040	5t!	a_{11}, b_{11}	11.6	5	$S_1(5,6,12)$
.5	$\mathcal{A}_{12}$	12!/2	10p!	a_6, a_{11}	11.7	6	
.6	$\mathcal{S}_{12}$	12!	12p!	a_{11}, a_{12}	11.8		
13.1	$\mathbb{Z}_{13}$	13	$[1^{13}]$	$a_{13} : x+1$	1	2, 3	$S_5(2,6,13)$
.2	$F_{13,2}$	26	$[1,2^6]$	$x+1, -x$	$\mathbb{Z}_2$	4, 5	$S_2(3,4,13)$
.3	$F_{13,3}$	39	$[1,3^4]$	$x+1, 3x$	$\mathbb{Z}_3$	5, 7	$S_1(2,3,13)$
.4	$F_{13,4}$	52	$[1,4^3]$	$x+1, 8x$	$\mathbb{Z}_4$	6	$S_2(3,4,13)$
.5	$F_{13,6}$	78	$[1,6^2]$	$x+1, 4x$	$\mathbb{Z}_6$	6, 8	
.6	$\mathrm{AGL}_1(13)$	156	2t!	$x+1, 2x$	$\mathbb{Z}_{12}$	9	$S_2(2,3,13)$,$S_5(2,5,13)$
.7	$L_3(3)$	5616	2t	a_{13}, b_{13}	≈ 9.7	8	$\mathrm{PG}_2(3)$
.8	$\mathcal{A}_{13}$	13!/2	11p!	a_6, a_{13}	12.5	9	
.9	$\mathcal{S}_{13}$	13!	13p!	a_{12}, a_{13}	12.6		
14.1	$L_2(13)$	1092	2p	a_{14}^2, b_{13}	13.5	2, 3	
.2	$\mathrm{PGL}_2(13)$	2184	3t!	a_{14}, b_{13}	13.6	4	$S_2(3,4,14)$

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
14.3	$\mathcal{A}_{14}$	14!/2	12p!	a_7, a_{13}	13.8	4	
.4	$\mathcal{S}_{14}$	14!	14p!	a_{13}, a_{14}	13.9		
15.1	$\mathcal{A}_6$	360	[1,6,8]	a_{15}^3, b_2	$\mathcal{S}_4$	2, 3	
.2	$\mathcal{S}_6$	720	[1,6,8]	a_{15}^3, c_2	$\mathcal{S}_4 \times \mathbb{Z}_2$	4	
.3	$\mathcal{A}_7$	2520	2t	a_{15}^3, b_7	$L_3(2)$	4	
.4	$L_4(2) \cong \mathcal{A}_8$	20160	2t	a_{15}, c_2	$\mathrm{AGL}_3(2)$	5	$\mathrm{PG}_3(2)$
.5	$\mathcal{A}_{15}$	15!/2	13p!	a_7, a_{15}	14.3	6	
.6	$\mathcal{S}_{15}$	15!	15p!	a_{14}, a_{15}	14.4		
16.1	$V_{16} \cdot \mathbb{Z}_5$	80	$[1,5^3]$	a_{16}^8, b_{15}^3	$\mathbb{Z}_5$	2, 3	$S_1(3,4,16)$
.2	$V_{16} \cdot D_5$	160	$[1,5^3]$	a_{16}^4, b_{15}^3	D_5	5, 6, 9, 11	
.3	$\mathrm{AGL}_1(16)$	240	2t!	a_{16}^8, b_{15}	$\mathbb{Z}_{15}$	6	
.4	$V_{16} \cdot (S_3 \times \mathbb{Z}_3)$	288	[1,6,9]	b_6^2, c_6	$S_3 \times \mathbb{Z}_3$	8, 15	
.5	$V_{16} \cdot F_{5,4}$	320	[1,5,10]	a_{16}^2, b_{15}^3	$F_{5,4}$	10, 13, 14	
.6	$V_{16} \cdot (D_5 \times \mathbb{Z}_3)$	480	2t	a_{16}^4, b_{15}	$D_5 \times \mathbb{Z}_3$	10, 15	
.7	$V_{16} \cdot (F_{9,4})$	576	[1,6,9]	b_4, b_6^2	9.1	12, 17	
.8	$V_{16} \cdot (\mathcal{S}_3 \times \mathcal{S}_3)$	576	[1,6,9]	b_4^2, c_6	$S_3 \times S_3$	12, 16	
.9	$V_{16} \cdot \mathcal{A}_5$	960	[1,5,10]	a_{16}^4, b_3	10.1	13, 17	
.10	$V_{16} \cdot G_\alpha$	960	2t	a_{16}^2, b_{15}	$A_8 \cap (F_{5,4} \times \mathcal{S}_3)$	16	
.11	$V_{16} \cdot \mathcal{A}_5$	960	2t	a_{16}^4, b_6^2	$\mathcal{A}_5$	14, 15, 17	
.12	$S_4 \wr S_2$	1152	[1,6,9]	b_4, c_6	9.2	$18^{b_4 b_3}$	
.13	$V_{16} \cdot \mathcal{S}_5$	1920	[1,5,10]	a_{16}^2, b_3	$\mathcal{S}_5$	18	$\mathrm{srg}(16,5,0,2)$
.14	$V_{16} \cdot \mathcal{S}_5$	1920	2t	a_{16}^2, b_6	10.2	16, 18, 19	
.15	$\mathrm{AGL}_2(4)$	2880	2t	b_6^2, b_{15}	$\mathcal{A}_5 \times \mathbb{Z}_3$	16	
.16	$\mathrm{A\Gamma L}_2(4)$	5760	2t	b_6, b_{15}	$A_8 \cap (\mathcal{S}_5 \times \mathcal{S}_3)$	20	$S_1(2,4,16)$
.17	$V_{16} \cdot \mathcal{A}_6$	5760	2p	b_3, b_6^2	15.1	$18, 19^{b_{15}}$	
.18	$V_{16} \cdot \mathcal{S}_6$	11520	2p	b_3, b_6	15.2	20	
.19	$V_{16} \cdot \mathcal{A}_7$	40320	3t	a_{16}^2, b_7	15.3	20	
.20	$\mathrm{AGL}_4(2)$	322560	3t	b_3, b_{15}	15.4	21	$S_1(3,4,16)$
.21	$\mathcal{A}_{16}$	16!/2	14p!	a_8, a_{15}	15.5	22	
.22	$\mathcal{S}_{16}$	16!	16p!	a_{15}, a_{16}	15.6		
17.1	$\mathbb{Z}_{17}$	17	$[1^{17}]$	$a_{17} : x+1$	1	2	
.2	D_{17}	34	$[1,2^8]$	$x+1, -x$	$\mathbb{Z}_2$	3, 6	
.3	$F_{17,4}$	68	$[1,4^4]$	$x+1, 13x$	$\mathbb{Z}_4$	4, 7	
.4	$F_{17,8}$	136	$[1,8^2]$	$x+1, 9x$	$\mathbb{Z}_8$	5, 8	

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
17.5	$\mathrm{AGL}_1(17)$	272	2t!	$x+1, 3x$	$\mathbb{Z}_{16}$	10	$S_4(4,5,17)$
.6	$L_2(16)$	4080	3t!	a_{17}, b_8^4	16.3	7	$S_6(4,7,17)$
.7	$\mathrm{PZL}_2(16)$	8160	3t	a_{17}, b_8^2	16.6	8	
.8	$\mathrm{P\Gamma L}_2(16)$	16320	3t	a_{17}, b_8	16.10	9	$S_1(3,5,17)$
.9	$\mathcal{A}_{17}$	17!/2	15p!	a_8, a_{17}	16.21	10	
.10	$\mathcal{S}_{17}$	17!	17p!	a_{16}, a_{17}	16.22		
18.1	$L_2(17)$	2448	2p	b_{17}, a_{18}^2	17.4	2, 3	
.2	$\mathrm{PGL}_2(17)$	4896	3t!	a_{18}, b_{17}	17.5	4	
.3	$\mathcal{A}_{18}$	18!/2	16p!	a_9, a_{17}	17.9	4	
.4	$\mathcal{S}_{18}$	18!	18p!	a_{17}, a_{18}	17.10		
19.1	$\mathbb{Z}_{19}$	19	$[1^{19}]$	$a_{19} : x+1$	1	2, 3	$S_1(2,3,19)$
.2	D_{19}	38	$[1,2^9]$	$x+1, -x$	$\mathbb{Z}_2$	4	
.3	$F_{19,3}$	57	$[1,3^6]$	$x+1, 7x$	$\mathbb{Z}_3$	4, 5	$S_1(2,3,19)$
.4	$F_{19,6}$	114	$[1,6^3]$	$x+1, 8x$	$\mathbb{Z}_6$	6	
.5	$F_{19,9}$	171	2*!	$x+1, 4x$	$\mathbb{Z}_9$	6, 7	$S_{112}(5,8,19)$
.6	$\mathrm{AGL}_1(19)$	342	2t!	$x+1, 2x$	$\mathbb{Z}_{18}$	8	
.7	$\mathcal{A}_{19}$	19!/2	17p!	a_9, a_{19}	18.3	8	
.8	$\mathcal{S}_{19}$	19!	19p!	a_{18}, a_{19}	18.4		
20.1	$L_2(19)$	3420	3*	a_{19}, b_{20}^2	19.5	2, 3	$S_{112}(6,9,20)$
.2	$\mathrm{PGL}_2(19)$	6840	3t!	a_{19}, b_{20}	19.6	4	
.3	$\mathcal{A}_{20}$	20!/2	18p!	a_{10}, a_{19}	19.7	4	
.4	$\mathcal{S}_{20}$	20!	20p!	a_{19}, a_{20}	19.8		
21.1	$\mathrm{PGL}_2(7)$	336	$[1,4,8^2]$	a_7, b_2	D_8	9	
.2	$\mathcal{A}_7$	2520	$[1,10^2]$	a_7, c_4^2	10.2	3, 8	
.3	$\mathcal{S}_7$	5040	$[1,10^2]$	a_7, c_4	$\mathcal{S}_5 \times \mathcal{S}_2$	9	
.4	$M_{21} \cong L_3(4)$	20160	2t	a_{21}^3, b_4^2	≈ 16.11	5, 6	
.5	$\mathrm{P\Sigma L}_3(4)$	40320	2t	a_{21}^3, b_4	≈ 16.14	7	
.6	$\mathrm{PGL}_3(4)$	60480	2t	a_{21}, b_4^2	≈ 16.15	7, 8	
.7	$\mathrm{P\Gamma L}_3(4)$	120960	2t	a_{21}, b_4	≈ 16.16	9	$\mathrm{PG}_2(4)$
.8	$\mathcal{A}_{21}$	21!/2	19p!	a_{10}, a_{21}	20.3	9	
.9	$\mathcal{S}_{21}$	21!	21p!	a_{20}, a_{21}	20.4		
22.1	M_{22}	443520	3t	a_{11}, b_{10}^2	21.4	2, 3	$S_1(3,6,22)$
.2	$M_{22} \cdot \mathbb{Z}_2$	887040	3t	a_{11}, b_{10}	21.5	4	
.3	$\mathcal{A}_{22}$	22!/2	20p!	a_{11}, a_{21}	21.8	4	

Degree $n.i$	Group G	Order $\lvert G\rvert$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
22.4	$\mathcal{S}_{22}$	22!	22p!	a_{21}, a_{22}	21.9		
23.1	$\mathbb{Z}_{23}$	23	$[1^{23}]$	$a_{23} : x+1$	1	2, 3	
.2	D_{23}	46	$[1,2^{11}]$	$x+1, -x$	$\mathbb{Z}_2$	4	
.3	$F_{23,11}$	253	2*	$x+1, 2x$	$\mathbb{Z}_{11}$	4, 5	$S_1(4,5,23)$
.4	$\mathrm{AGL}_1(23)$	506	2t!	$x+1, 5x$	$\mathbb{Z}_{22}$	7	
.5	M_{23}	10200960	4t	a_{23}, b_2	22.1	6	$S_1(4,7,23)$
.6	$\mathcal{A}_{23}$	23!/2	21p!	a_{11}, a_{23}	22.3	7	
.7	$\mathcal{S}_{23}$	23!	23p!	a_{22}, a_{23}	22.4		
24.1	$L_2(23)$	6072	3*	a_{23}, b_{24}^2	23.3	2, 3	$S_1(5,6,24)$
.2	$\mathrm{PGL}_2(23)$	12144	3t!	a_{23}, b_{24}	23.4	5	
.3	M_{24}	244823040	5t	a_{23}, b_2	23.5	4	$S_1(5,8,24)$
.4	$\mathcal{A}_{24}$	24!/2	22p!	a_{12}, a_{23}	23.6	5	
.5	$\mathcal{S}_{24}$	24!	24p!	a_{23}, a_{24}	23.7		
25.1	$F_{25,3}$	75	$[1,3^8]$	a_5, b_{24}^8	$\mathbb{Z}_3$	2, 3	
.2	$F_{25,6}$	150	$[1,6^4]$	a_5, b_{24}^4	$\mathbb{Z}_6$	7,8,9,13	
.3	$V_{25} \cdot \mathcal{S}_3$	150	$[1,3^4,6^2]$	b_{10}, b_{24}^8	$\mathcal{S}_3$	9	
.4	$D_5 \wr \mathcal{S}_2$	200	$[1,4^4,8]$	b_2, b_{20}^2	D_4	11, 22	
.5	$F_{25,8}$	200	$[1,8^3]$	b_{24}^6, c_8	$\mathbb{Z}_8$	10, $14^{c_{10}}$, 15	
.6	$V_{25} \cdot Q_8$	200	$[1,8^3]$	b_4, d_4	Q_8	11, 13	
.7	$F_{25,12}$	300	$[1,12^2]$	a_5, b_{24}^2	$\mathbb{Z}_{12}$	12, 14, 15, 17	
.8	$V_{25} \cdot (\mathbb{Z}_3 \cdot \mathbb{Z}_4)$	300	$[1,12^2]$	b_{24}^4, c_4	$\mathbb{Z}_3 \cdot \mathbb{Z}_4$	12, 20	
.9	$V_{25} \cdot D_6$	300	$[1,6^4]$	b_{24}^4, b_{10}	D_6	12	
.10	$V_{25} \cdot (\mathbb{Z}_8 \cdot_5 \mathbb{Z}_2)$	400	[1,8,16]	b_{20}^2, c_8	$\mathbb{Z}_8 \cdot_5 \mathbb{Z}_2$	16, $18^{c_{20}}$, 25	
.11	$V_{25} \cdot (Q_8 \cdot \mathbb{Z}_2)$	400	$[1,8^3]$	b_{24}^6, b_4, b_2	$Q_8 \cdot \mathbb{Z}_2$	16, 17, 24	
.12	$V_{25} \cdot (\mathcal{S}_3 \times \mathbb{Z}_4)$	600	$[1,12^2]$	b_{24}^2, b_{10}	$\mathcal{S}_3 \times \mathbb{Z}_4$	18, 21	
.13	$V_{25} \cdot (Q_8 \cdot \mathbb{Z}_3)$	600	2t!	b_{24}^4, b_4	$Q_8 \cdot \mathbb{Z}_3$	17, 20	
.14	$\mathrm{AGL}_1(25)$	600	2t!	b_{24}, a_5	$\mathbb{Z}_{24}$	18	
.15	$V_{25} \cdot (\mathbb{Z}_3 \cdot \mathbb{Z}_8)$	600	2t!	b_{24}^2, c_8	$\mathbb{Z}_3 \cdot \mathbb{Z}_8$	18, 19	
.16	$\mathrm{AGL}_1(5) \wr \mathcal{S}_2$	800	[1,8,16]	b_{20}, b_8	$\mathbb{Z}_4 \wr \mathbb{Z}_2$	19, 26	
.17	$V_{25} \cdot G_\alpha$	1200	2t	b_{24}^2, b_{20}^2	$(Q_8 \cdot \mathbb{Z}_2) \cdot \mathbb{Z}_3$	19, 21	
.18	$V_{25} \cdot (\mathbb{Z}_{24} \cdot_5 \mathbb{Z}_2)$	1200	2t	b_{24}, b_{10}	$\mathbb{Z}_{24} \cdot_5 \mathbb{Z}_2$	23	
.19	$V_{25} \cdot G_\alpha$	2400	2t	b_{24}^2, b_{20}	$(Q_8 \cdot \mathbb{Z}_3) \cdot \mathbb{Z}_4$	23	
.20	$\mathrm{ASL}_2(5)$	3000	2t	b_{24}^4, c_{20}^2	$\approx \mathbb{Z}_2 \backslash 6.1$	21	
.21	$\mathcal{A}_{25} \cap \mathrm{AGL}_2(5)$	6000	2t	b_{24}^2, c_{20}	$\approx \mathbb{Z}_4 \backslash 6.1$	23, 27	

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
25.22	$\mathcal{A}_5 \wr \mathcal{S}_2$	7200	[1,8,16]	b_6, b_{12}^4	16.4	24	
.23	$\mathrm{AGL}_2(5)$	12000	2t	b_{24}, b_{20}	$\mathrm{GL}_2(5)$	28	
.24	$\mathcal{A}_5^2 \cdot V_4$	14400	[1,8,16]	b_6, b_{12}^2	16.8	26, 27	
.25	$\mathcal{A}_5^2 \cdot \mathbb{Z}_4$	14400	[1,8,16]	b_6^2, b_{12}	16.7	26	
.26	$\mathcal{S}_5 \wr \mathcal{S}_2$	28800	[1,8,16]	b_6, b_{12}	16.12	28	
.27	$\mathcal{A}_{25}$	25!/2	23p!	a_{12}, a_{25}	24.4	28	
.28	$\mathcal{S}_{25}$	25!	25p!	a_{24}, a_{25}	24.5		
26.1	$L_2(25)$	7800	2p	a_{26}^2, b_{10}^2	25.7	2,3,4	
.2	$\mathrm{P\Sigma L}_2(25)$	15600	2p	a_{26}^2, b_{10}	25.12	5,6	
.3	$\mathrm{PGL}_2(25)$	15600	3t!	a_{26}, b_{10}^2	25.14	5	
.4	$\mathrm{P\Delta L}_2(25)$	15600	3t!	a_{26}^2, b_{12}	25.15	5	
.5	$\mathrm{P\Gamma L}_2(25)$	31200	3t	a_{26}, b_{10}	25.18	7	
.6	$\mathcal{A}_{26}$	26!/2	24p!	a_{13}, a_{25}	25.27	7	
.7	$\mathcal{S}_{26}$	26!	26p!	a_{25}, a_{26}	25.28		
27.1	$V_{27} \cdot \mathcal{A}_4$	324	[1,4^2,6,12]	a_9, b_6^2	$\mathcal{A}_4$	3,4,5	
.2	$F_{27,13}$	351	[1,13^2]	a_9^3, b_{26}^2	$\mathbb{Z}_{13}$	6,7	$S_1(4, 6, 27)$
.3	$V_{27} \cdot \mathcal{S}_4$	648	[1,6,8,12]	a_9, b_4	$\mathcal{S}_4$	8,12	
.4	$V_{27} \cdot \mathcal{S}_4$	648	[1,4^2,6,12]	a_9, c_4	$\mathcal{S}_4$	8	
.5	$V_{27} \cdot (V8 \cdot \mathbb{Z}_3)$	648	[1,6,8,12]	a_9, b_6	$V_8 \cdot \mathbb{Z}_3$	8	
.6	$\mathrm{AGL}_1(27)$	702	2t!	a_9^3, b_{26}	$\mathbb{Z}_{26}$	9	
.7	$V_{27} \cdot F_{13,3}$	1053	[1,13^2]	a_9, d_6^2	13.3	9,12	
.8	$V_{27} \cdot (\mathcal{S}_4 \times \mathbb{Z}_2)$	1296	[1,6,8,12]	b_4, c_6	$\mathcal{S}_4 \times \mathbb{Z}_2$	13	
.9	$\mathrm{A\Gamma L}_1(27)$	2106	2t	a_9, d_6	$\mathbb{Z}_{26} \cdot \mathbb{Z}_3$	13	
.10	$U_4(2) \cong S_4(3)$	25920	[1,10,16]	a_9, b_{12}^2	16.9	11	
.11	$U_4(2) \cdot \mathbb{Z}_2$	51840	[1,10,16]	a_9, b_{12}	16.13	14	$\mathrm{srg}(27, 10, 1, 5)$
.12	$\mathrm{ASL}_3(3)$	151632	2t	a_9, b_{24}^2	$\approx$ 13.7	13,14	
.13	$\mathrm{AGL}(3, 3)$	303264	2t	a_9, b_{24}	$\approx \mathbb{Z}_2 \backslash$13.7	15	
.14	$\mathcal{A}_{27}$	27!/2	25p!	a_{13}, a_{27}	26.6	15	
.15	$\mathcal{S}_{27}$	27!	27p!	a_{26}, a_{27}	26.7		
28.1	$\mathrm{PGL}_2(7)$	336	[1,3,6^2,12]	a_7, b_6	D_6	6, 10	
.2	$L_2(8)$	504	[1,9^3]	a_7, b_9^3	D_9	3	
.3	$\mathrm{P\Gamma L}_2(8)$	1512	2t	a_7, b_9	$D_9 \cdot \mathbb{Z}_3$	12	
.4	$U_3(3)$	6048	2t	a_7, b_{12}^2	$T_{27} \cdot \mathbb{Z}_8$	6	

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
28.5	$L_2(27)$	9828	2p	a_7, b_{26}^2	27.2	7,9	$S_1(5,7,28)$
.6	$\mathrm{P\Sigma U}_3(3)$	12096	2t	a_7, b_{12}	$T_{27} \cdot (\mathbb{Z}_8 \cdot_3 \mathbb{Z}_2)$	12	
.7	$\mathrm{PGL}_2(27)$	19656	3t!	a_7, b_{26}	27.6	11	
.8	$\mathcal{A}_8$	20160	[1,12,15]	a_7, c_6	$\mathcal{S}_6$	10	
.9	$\mathrm{P\Sigma L}_2(27)$	29484	2p	a_7, c_{12}^2	27.7	11,13	
.10	$\mathcal{S}_8$	40320	[1,12,15]	a_7, b_8	$\mathcal{S}_6 \times \mathbb{Z}_2$	12	
.11	$\mathrm{P\Gamma L}_2(27)$	58968	3t	a_7, c_{12}	27.9	14	
.12	$S_6(2)$	1451520	2p	a_7, d_{12}	27.11	13	
.13	$\mathcal{A}_{28}$	28!/2	26p!	a_{14}, a_{27}	27.14	14	
.14	$\mathcal{S}_{28}$	28!	28p!	a_{27}, a_{28}	27.15		
29.1	$\mathbb{Z}_{29}$	29	$[1^{29}]$	$a_{29} : x+1$	1	2,4	
.2	$F_{29,2}$	58	$[1,2^{14}]$	$x+1, 28x$	$\mathbb{Z}_2$	3,5	
.3	$F_{29,4}$	116	$[1,4^7]$	$x+1, 12x$	$\mathbb{Z}_4$	6	
.4	$F_{29,7}$	203	$[1,7^4]$	$x+1, 16x$	$\mathbb{Z}_7$	5	
.5	$F_{29,14}$	406	$[1,14^2]$	$x+1, 4x$	$\mathbb{Z}_{14}$	6,7	
.6	$\mathrm{AGL}_1(29)$	812	2t!	$x+1, 2x$	$\mathbb{Z}_{28}$	8	
.7	$\mathcal{A}_{29}$	29!/2	27p!	a_{14}, a_{29}	28.13	8	
.8	$\mathcal{S}_{29}$	29!	29p!	a_{28}, a_{29}	28.14		
30.1	$L_2(29)$	12180	2p	a_{29}, b_{30}^2	29.5	2,3	
.2	$\mathrm{PGL}_2(29)$	24360	3t!	a_{29}, b_{30}	29.6	4	
.3	$\mathcal{A}_{30}$	30!/2	28p!	a_{15}, a_{29}	29.7	4	
.4	$\mathcal{S}_{30}$	30!	30p!	a_{29}, a_{30}	29.8		
31.1	$\mathbb{Z}_{31}$	31	$[1^{31}]$	$a_{31} : x+1$	1	2, 3, 4	
.2	$F_{31,2}$	62	$[1,2^{15}]$	$x+1, \ -x$	$\mathbb{Z}_2$	5, 6	
.3	$F_{31,3}$	93	$[1,3^{10}]$	$x+1, \ 5x$	$\mathbb{Z}_3$	5, 7, 9	
.4	$F_{31,5}$	155	$[1,5^6]$	$x+1, \ 2x$	$\mathbb{Z}_5$	6, 7, 10	$S_{36}(4,6,31),\ S_{10}(5,6,31)$
.5	$F_{31,6}$	186	$[1,6^5]$	$x+1, \ 6x$	$\mathbb{Z}_6$	8	
.6	$F_{31,10}$	310	$[1,10^3]$	$x+1, \ 15x$	$\mathbb{Z}_{10}$	8	
.7	$F_{31,15}$	465	$[1,15^2]$	$x+1, \ 7x$	$\mathbb{Z}_{15}$	8, 11	
.8	$\mathrm{AGL}_1(31)$	930	2t!	$x+1, \ 3x$	$\mathbb{Z}_{30}$	12	
.9	$L_3(5)$	372000	2t	$a_{31}, \ b_{31}$	$\mathrm{AGL}_2(5)$	11	
.10	$L_5(2)$	9999360	2t	$a_{31}, \ c_{31}$	$\mathrm{AGL}_4(2)$	11	
.11	$\mathcal{A}_{31}$	31!/2	29p!	$a_{15}, \ a_{31}$	30.3	12	

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
31.12	$\mathcal{S}_{31}$	31!	31p!	$a_{30},\ a_{31}$	30.4		
32.1	$\mathrm{AGL}_1(32)$	992	2p!	a_{31}, b_{10}^5	31.1	2	
.2	$\mathrm{A\Gamma L}_1(32)$	4960	3*!	a_{31}, b_{10}	31.4	5	$S_{36}(5,7,32)$,$S_{10}(6,7,32)$
.3	$L_2(31)$	14880	3*	a_{31}, b_{32}^2	31.7	4, 6	
.4	$\mathrm{PGL}_2(31)$	29760	3t!	a_{31}, b_{32}	31.8	7	
.5	$\mathrm{AGL}_5(2)$	319979520	3t	a_{31}, b_{31}	31.10	6	
.6	$\mathcal{A}_{32}$	32!/2	30p!	a_{16}, a_{31}	31.11	7	
.7	$\mathcal{S}_{32}$	32!	32p!	a_{31}, a_{32}	31.12		
33.1	$L_2(32)$	32736	3p!	a_{33}, b_{15}^5	32.1	2	
.2	$\mathrm{P\Gamma L}_2(32)$	163680	4*	a_{33}, b_{15}	32.2	3	$S_{36}(6,8,33)$,$S_{10}(7,8,33)$
.3	$\mathcal{A}_{33}$	33!/2	31p!	a_{16}, a_{33}	32.6	4	
.4	$\mathcal{S}_{33}$	33!	33p!	a_{32}, a_{33}	32.7		
34.1	$\mathcal{A}_{34}$	34!/2	32p!	a_{17}, a_{33}	33.3	2	
.2	$\mathcal{S}_{34}$	34!	34p!	a_{33}, a_{34}	33.4		
35.1	$\mathcal{A}_7$	2520	[1,4,12,18]	$a_{15,5}^3, b_{12}^2$	$\approx \mathbb{Z}_2 \backslash 9.1$	2, 3	
.2	$\mathcal{S}_7$	5040	[1,4,12,18]	$a_{15,5}^3, b_{12}$	≈ 9.5	4	
.3	$\mathcal{A}_8$	20160	[1,16,18]	$a_{15,5}, b_{12}^2$	16.8	4	
.4	$\mathcal{S}_8$	40320	[1,16,18]	$a_{15,5}, b_{12}$	16.12	5	srg(35, 16, 6, 8)
.5	$\mathcal{A}_{35}$	35!/2	33p!	a_{17}, a_{35}	34.1	6	
.6	$\mathcal{S}_{35}$	35!	35p!	a_{34}, a_{35}	34.2		
36.1	$L_2(8)$	504	$[1,7^3,14]$	a_{36}^{12}, b_8^4	D_7	5	
.2	$\mathrm{PGL}_2(9)$	720	$[1,5,10^3]$	b_{10}, c_8^2	D_{10}	4,15	
.3	M_{10}	720	[1,5,10,20]	b_{10}^2, c_8	$F_{5,4}$	$4,15^{b_{12}}$	
.4	$\mathrm{P\Gamma L}_2(9)$	1440	[1,5,10,20]	b_{10}, c_8	$F_{5,4} \times \mathbb{Z}_2$	17	
.5	$\mathrm{P\Gamma L}_2(8)$	1512	[1,14,21]	a_{36}^4, b_8^4	≈ 7.4	14,20	
.6	$U_3(3)$	6048	$[1,7^2,21]$	a_{36}^{12}, c_{12}^2	7.5	8	
.7	$\mathcal{A}_5 \wr \mathcal{S}_2$	7200	[1,10,25]	b_{10}, b_{12}^4	25.4	9,15	
.8	$\mathrm{P\Sigma U}_3(3)$	12096	[1,14,21]	a_{36}^{12}, c_{12}	21.1	20	srg(36, 14, 4, 6)
.9	$\mathcal{A}_5^2 \cdot V_4$	14400	[1,10,25]	b_{10}, b_{12}^2	25.11	12,17	
.10	$\mathcal{A}_5^2 \cdot \mathbb{Z}_4$	14400	[1,10,25]	b_{10}^2, b_{12}	25.10	12,18	
.11	$S_4(3) \cong U_4(2)$	25920	[1,15,20]	a_{36}^4, b_6^2	15.2	13	
.12	$\mathcal{S}_5 \wr \mathcal{S}_2$	28800	[1,10,25]	b_{10}, b_{12}	25.16	19	
.13	$U_4(2) \cdot \mathbb{Z}_2$	51840	[1,15,20]	a_{36}^4, b_6	$\mathcal{S}_6 \times \mathcal{S}_2$	20	srg(36, 15, 6, 6)

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
36.14	$\mathcal{A}_9$	181440	[1,14,21]	a_{36}^4, b_8^2	21.3	16, 21	
.15	$\mathcal{A}_6 \wr \mathcal{S}_2$	259200	[1,10,25]	a_{36}^{12}, b_{10}	25.22	17	
.16	$\mathcal{S}_9$	362880	[1,14,21]	a_{36}^4, b_8	$\mathcal{S}_7 \times \mathcal{S}_2$	22	
.17	$\mathcal{A}_6^2 \cdot V_4$	518400	[1,10,25]	a_{36}^6, b_{10}	25.24	19	
.18	$\mathcal{A}_6^2 \cdot \mathbb{Z}_4$	518400	[1,10,25]	a_{36}^3, b_{10}^2	25.25	19	
.19	$\mathcal{S}_6 \wr \mathcal{S}_2$	1036800	[1,10,25]	a_{36}^3, b_{10}	25.26	22	
.20	$S_6(2)$	1451520	2p	a_{36}^4, c_{12}	35.4	21	
.21	$\mathcal{A}_{36}$	36!/2	34p!	a_{18}, a_{35}	35.5	22	
.22	$\mathcal{S}_{36}$	36!	36p!	a_{35}, a_{36}	35.6		
37.1	$\mathbb{Z}_{37}$	37	$[1^{37}]$	$a_{37} : x+1$	1	2,3	
.2	$F_{37,2}$	74	$[1, 2^{18}]$	$x+1, -x$	$\mathbb{Z}_2$	4,5	
.3	$F_{37,3}$	111	$[1, 3^{12}]$	$x+1, 26x$	$\mathbb{Z}_3$	5,6	
.4	$F_{37,4}$	148	$[1, 4^9]$	$x+1, 31x$	$\mathbb{Z}_4$	7	
.5	$F_{37,6}$	222	$[1, 6^6]$	$x+1, 27x$	$\mathbb{Z}_6$	7,8	
.6	$F_{37,9}$	333	$[1, 9^4]$	$x+1, 16x$	$\mathbb{Z}_9$	8,11	
.7	$F_{37,12}$	444	$[1, 12^3]$	$x+1, 8x$	$\mathbb{Z}_{12}$	9	
.8	$F_{37,18}$	666	$[1, 18^2]$	$x+1, 4x$	$\mathbb{Z}_{18}$	9,10	
.9	$\mathrm{AGL}_1(37)$	1332	2t!	$x+1, 2x$	$\mathbb{Z}_{36}$	11	
.10	$\mathcal{A}_{37}$	37!/2	35p!	a_{18}, a_{37}	36.21	11	
.11	$\mathcal{S}_{37}$	37!	37p!	a_{36}, a_{37}	36.22		
38.1	$L_2(37)$	25308	2p	a_{37}, b_{38}^2	37.8	2,3	
.2	$\mathrm{PGL}_2(37)$	50616	3t!	a_{37}, b_{38}	37.9	4	
.3	$\mathcal{A}_{38}$	38!/2	36p!	a_{19}, a_{37}	37.10	4	
.4	$\mathcal{S}_{38}$	38!	38p!	a_{36}, a_{37}	37.11		
39.1	$\mathcal{A}_{39}$	39!/2	37p!	a_{19}, a_{39}	38.3	2	
.2	$\mathcal{S}_{39}$	39!	39p!	a_{38}, a_{39}	38.4		
40.1	$S_4(3) \cong U_4(2)$	25920	[1,12,27]	a_{40}^8, b_5	$T_{27} \cdot (Q_8 \cdot \mathbb{Z}_3)$	3	
.2	$S_4(3) \cong U_4(2)$	25920	[1,12,27]	a_{40}^8, b_{10}^2	27.4	4	
.3	$U_4(2) \cdot \mathbb{Z}_2$	51840	[1,12,27]	a_{40}^4, b_5	$T_{27} \cdot (Q_8 \cdot \mathcal{S}_3)$	5	
.4	$U_4(2) \cdot \mathbb{Z}_2$	51840	[1,12,27]	a_{40}^8, b_{10}	27.8	8	
.5	$L_4(3)$	6065280	2t	a_{40}^2, b_5	$\mathrm{ASL}_3(3)$	6,7	
.6	$\mathrm{PGL}_4(3)$	12130560	2t	a_{40}, b_5	$\mathrm{AGL}_3(3)$	8	
.7	$\mathcal{A}_{40}$	40!/2	38p!	a_{20}, a_{39}	39.1	8	

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
40.8	$\mathcal{S}_{40}$	40!	40p!	a_{39}, a_{40}	39.2		
41.1	$\mathbb{Z}_{41}$	41	$[1^{41}]$	$a_{41} : x+1$	1	2,4	
.2	$F_{41,2}$	82	$[1,2^{20}]$	$x+1, 40x$	$\mathbb{Z}_2$	3,6	
.3	$F_{41,4}$	164	$[1,4^{10}]$	$x+1, 32x$	$\mathbb{Z}_4$	5,7	
.4	$F_{41,5}$	205	$[1,5^8]$	$x+1, 10x$	$\mathbb{Z}_5$	6	
.5	$F_{41,8}$	328	$[1,8^5]$	$x+1, 27x$	$\mathbb{Z}_8$	8	
.6	$F_{41,10}$	410	$[1,10^4]$	$x+1, 25x$	$\mathbb{Z}_{10}$	7	
.7	$F_{41,20}$	820	$[1,20^2]$	$x+1, 36x$	$\mathbb{Z}_{20}$	8,9	
.8	$\mathrm{AGL}_1(41)$	1640	2t!	$x+1, 6x$	$\mathbb{Z}_{40}$	10	
.9	$\mathcal{A}_{41}$	41!/2	39p!	a_{20}, a_{41}	40.7	10	
.10	$\mathcal{S}_{41}$	41!	41p!	a_{40}, a_{41}	40.8		
42.1	$L_2(41)$	34440	2p	a_{41}, b_{42}^2	41.7	2,3	
.2	$\mathrm{PGL}_2(41)$	68880	3t!	a_{41}, b_{42}	41.8	4	
.3	$\mathcal{A}_{42}$	42!/2	40p!	a_{21}, a_{41}	41.9	4	
.4	$\mathcal{S}_{42}$	42!	42p!	a_{41}, a_{42}	41.10		
43.1	$\mathbb{Z}_{43}$	43	$[1^{43}]$	$a_{43} : x+1$	1	2,3,5	
.2	$F_{43,2}$	86	$[1,2^{21}]$	$x+1, 42x$	$\mathbb{Z}_2$	4,6	
.3	$F_{43,3}$	129	$[1,3^{14}]$	$x+1, 36x$	$\mathbb{Z}_3$	4,7	
.4	$F_{43,6}$	258	$[1,6^7]$	$x+1, 37x$	$\mathbb{Z}_6$	8	
.5	$F_{43,7}$	301	$[1,7^6]$	$x+1, 41x$	$\mathbb{Z}_7$	6,7	
.6	$F_{43,14}$	602	$[1,14^3]$	$x+1, 27x$	$\mathbb{Z}_{14}$	8	
.7	$F_{43,21}$	903	$[1,21^2]$	$x+1, 9x$	$\mathbb{Z}_{21}$	8,9	
.8	$\mathrm{AGL}_1(43)$	1806	2t!	$x+1, 3x$	$\mathbb{Z}_{42}$	10	
.9	$\mathcal{A}_{43}$	43!/2	41p!	a_{21}, a_{43}	42.3	10	
.10	$\mathcal{S}_{43}$	43!	43p!	a_{42}, a_{43}	42.4		
44.1	$L_2(43)$	39732	2p	a_{43}, b_{44}^2	43.7	2,3	
.2	$\mathrm{PGL}_2(43)$	79464	3t!	a_{43}, b_{44}	43.8	4	
.3	$\mathcal{A}_{44}$	44!/2	42p!	a_{22}, a_{43}	43.9	4	
.4	$\mathcal{S}_{44}$	44!	44p!	a_{43}, a_{44}	43.10		
45.1	$\mathrm{PGL}_2(9)$	720	$[1,4,8^3,16]$	b_8^2, b_{10}	D_8	3	
.2	M_{10}	720	$[1,4,8,16^2]$	b_8, b_{10}^2	$\mathbb{Z}_8 \cdot_3 \mathbb{Z}_2$	3, 6	
.3	$\mathrm{P\Gamma L}_2(9)$	1440	$[1,4,8,16^2]$	b_8, b_{10}	$\mathbb{Z}_8 \cdot Aut\ \mathbb{Z}_8$	7	
.4	$S_4(3) \cong U_4(2)$	25920	[1,12,32]	b_{10}^2, d_8^2	$\mathbb{Z}_2 \backslash 16.4$	5, 8	

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
45.5	$U_4(2) \cdot \mathbb{Z}_2$	51840	[1,12,32]	b_{10}^2, d_8	$\mathbb{Z}_2 \backslash 16.8$	9	srg(45, 12, 3, 3)
.6	$\mathcal{A}_{10}$	1814400	[1,16,28]	b_{10}^2, c_8^2	28.10	7	
.7	$\mathcal{S}_{10}$	3628800	[1,16,28]	b_{10}, c_8	$\mathcal{S}_8 \times \mathcal{S}_2$	8	
.8	$\mathcal{A}_{45}$	45!/2	43p!	a_{22}, a_{45}	44.3	9	
.9	$\mathcal{S}_{45}$	45!	45p!	a_{44}, a_{45}	44.4		
46.1	$\mathcal{A}_{46}$	46!/2	44p!	a_{23}, a_{45}	45.8	2	
.2	$\mathcal{S}_{46}$	46!	46p!	a_{45}, a_{46}	45.9		
47.1	$\mathbb{Z}_{47}$	47	$[1^{47}]$	$a_{47} : x + 1$	1	2, 3	
.2	$F_{47,2}$	94	$[1,2^{23}]$	$x + 1, 46x$	$\mathbb{Z}_2$	4	
.3	$F_{47,23}$	1081	$[1,23^2]$	$x + 1, 25x$	$\mathbb{Z}_{23}$	4, 5	$S_1(4, 5, 47)$
.4	$\mathrm{AGL}_1 47$	2162	2t!	$x + 1, 5x$	$\mathbb{Z}_{46}$	6	
.5	$\mathcal{A}_{47}$	47!/2	45p!	a_{23}, a_{47}	46.1	6	
.6	$\mathcal{S}_{47}$	47!	47p!	a_{46}, a_{47}	46.2		
48.1	$L_2(47)$	51888	2p	a_{48}^2, b_{47}	47.3	2,3	$S_1(5, 6, 48)$
.2	$\mathrm{PGL}_2(47)$	103776	3t!	a_{48}, b_{47}	47.4	4	
.3	$\mathcal{A}_{48}$	48!/2	46p!	a_{24}, a_{47}	47.5	4	
.4	$\mathcal{S}_{48}$	48!	48p!	a_{47}, a_{48}	47.6		
49.1	$F_{49,4}$	196	$[1,4^{12}]$	a_7, b_{48}^{12}	$\mathbb{Z}_4$	3,4,5,6,7	
.2	$V_{49} \cdot \mathcal{S}_3$	294	$[1,3^6,6^5]$	b_{42}^3, b_{14}	$\mathcal{S}_3$	8, 12	
.3	$F_{49,8}$	392	$[1,8^6]$	a_7, b_{48}^6	$\mathbb{Z}_8$	9,10,11,13	
.4	$V_{49} \cdot Q_8$	392	$[1,8^6]$	b_{48}^{12}, b_{12}^3	Q_8	9,14,15,16	
.5	$D_7 \wr \mathcal{S}_2$	392	$[1,4^6,8^3]$	b_{14}, b_{48}^{12}	D_4	11,17,18	
.6	$V_{49} \cdot (\mathbb{Z}_3 \cdot \mathbb{Z}_4)$	588	$[1,12^4]$	b_{48}^{12}, d_6	$\mathbb{Z}_3 \cdot \mathbb{Z}_4$	$17, 20, 22^{b_{42}}, 30$	
.7	$F_{49,12}$	588	$[1,12^4]$	a_7, b_{48}^4	$\mathbb{Z}_{12}$	13,14,18,20	
.8	$V_{49} \cdot D_6$	588	$[1,6^6,12]$	b_{42}^3, d_6	D_6	17,21	
.9	$V_{49} \cdot (\mathbb{Z}_2 \backslash D_4)$	784	$[1,16^3]$	b_{48}^6, b_{12}^3	$\mathbb{Z}_2 \backslash D_4$	19,22,23	
.10	$F_{49,16}$	784	$[1,16^3]$	a_7, b_{48}^3	$\mathbb{Z}_{16}$	19,24	
.11	$V_{49} \cdot D_8$	784	$[1,8^6]$	b_{14}, b_{48}^6	D_8	19, 25	
.12	$V_{49} \cdot G_\alpha \cong 7.3 \wr \mathcal{S}_2$	882	$[1,6^2,9^2,18]$	b_{14}, c_6^2	$\mathbb{Z}_3 \wr \mathcal{S}_2$	21, 33	
.13	$F_{49,24}$	1176	$[1,24^2]$	a_7, b_{48}^2	$\mathbb{Z}_{24}$	23, 24, 25	
.14	$V_{49} \cdot (Q_8 \times \mathbb{Z}_3)$	1176	$[1,24^2]$	b_{48}^4, b_{12}	$Q_8 \times \mathbb{Z}_3$	23, 26	
.15	$V_{49} \cdot (Q_8 \cdot \mathbb{Z}_3)$	1176	$[1,24^2]$	b_{48}^{12}, b_3	$Q_8 \cdot \mathbb{Z}_3$	22,26	
.16	$V_{49} \cdot (Q_8 \cdot \mathbb{Z}_3)$	1176	$[1,8^3,24]$	b_{48}^{12}, b_6	$Q_8 \cdot \mathbb{Z}_3$	26	

Degree $n.i$	Group G	Order $\|G\|$	Trans/Rank	Generators	G_α	min H, $G < H \leq \mathcal{S}_n$	Combinatorial Structures
49.17	$V_{49} \cdot (\mathbb{Z}_3 \cdot D_4)$	1176	[1,12^4]	b_{48}^{12}, b_{42}^3	$\mathbb{Z}_3 \cdot D_4$	27,31	
.18	$V_{49} \cdot (D_4 \times \mathbb{Z}_3)$	1176	[1,12^2,24]	b_{14}, b_{48}^4	$D_4 \times \mathbb{Z}_3$	25,27	
.19	$V_{49} \cdot (\mathbb{Z}_{16} \cdot_7 \mathbb{Z}_2)$	1568	[1,16^3]	b_{14}, b_{48}^3	$\mathbb{Z}_{16} \cdot_7 \mathbb{Z}_2$	28,31	
.20	$V_{49} \cdot G_\alpha$	1764	[1,12,36]	b_{48}^4, c_6	$\mathbb{Z}_3 \times (\mathbb{Z}_3 \cdot \mathbb{Z}_4)$	27,29$^{b_{42}}$, 32, 37	
.21	$V_{49} \cdot (\mathcal{S}_3 \times \mathbb{Z}_6)$	1764	[1,12,18^2]	b_{14}, c_6	$\mathcal{S}_3 \times \mathbb{Z}_6$	27,36	
.22	$V_{49} \cdot (\mathbb{Z}_2 \backslash \mathcal{S}_4)$	2352	2t!	b_{48}^6, b_8^2	$\mathbb{Z}_2 \backslash \mathcal{S}_4$	29,30	
.23	$V_{49} \cdot G_\alpha$	2352	2t!	b_{48}^2, b_{12}	$\mathbb{Z}_3 \times (\mathbb{Z}_2 \backslash D_4)$	28,29	
.24	$\mathrm{AGL}_1(49)$	2352	2t!	a_7, b_{48}	$\mathbb{Z}_{48}$	28	
.25	$\mathrm{A\Sigma L}_1(49)$	2352	[1,24^2]	b_{48}^2, b_{14}	$\mathbb{Z}_{24} \cdot_7 \mathbb{Z}_2$	28	
.26	$V_{49} \cdot G_\alpha$	3528	[1,24^2]	b_{48}^4, b_6	$(Q_8 \cdot \mathbb{Z}_3) \times \mathbb{Z}_3$	29	
.27	$7.4 \wr \mathcal{S}_2$	3528	[1,12,36]	b_{48}^4, b_{42}^3	$\mathbb{Z}_6 \wr \mathcal{S}_2$	34,38	
.28	$\mathrm{A\Gamma L}_1(49)$	4704	2t	b_{48}, b_{14}	$\mathbb{Z}_{48} \cdot_7 \mathbb{Z}_2$	34	
.29	$V_{49} \cdot G_\alpha$	7056	2t	b_{48}^2, b_8^2	$(\mathbb{Z}_2 \backslash \mathcal{S}_4) \times \mathbb{Z}_3$	32	
.30	$\mathrm{ASL}_2(7)$	16464	2t	b_{48}^6, b_8	$\mathrm{SL}_2(7)$	31,32	
.31	$\mathrm{AS}^{\pm} L_2(7)$	32928	2t	b_{48}^3, b_{42}^3	$(\pm 1) \cdot SL_2(7)$	34	
.32	$\mathrm{AS}^2 L_2(7)$	49392	2t	b_{48}^2, b_{42}^2	$\langle 2 \rangle \times SL_2(7)$	34,39	
.33	$L_3(2) \wr \mathcal{S}_2 \cong 7.5 \wr \mathcal{S}_2$	56448	[1,12,36]	b_{24}^{12}, b_{42}^3	$\mathcal{S}_4 \wr \mathcal{S}_2$	35	
.34	$\mathrm{AGL}_2(7)$	98784	2t	b_{48}, b_{42}	$\mathrm{GL}_2(7)$	40	
.35	$\mathcal{A}_7 \wr \mathcal{S}_2$	12700800	[1,12,36]	b_{24}^4, b_{42}^3	36.15	36	
.36	$(\mathcal{A}_7 \times \mathcal{A}_7) \cdot V_4$	25401600	[1,12,36]	b_{24}^2, b_{42}^3	36.17	38	
.37	$(\mathcal{A}_7 \times \mathcal{A}_7) \cdot \mathbb{Z}_4$	25401600	[1,12,36]	b_{24}, b_{42}^6	36.18	38,39	
.38	$\mathcal{S}_7 \wr \mathcal{S}_2$	50803200	[1,12,36]	b_{24}, b_{42}^3	36.19	40	
.39	$\mathcal{A}_{49}$	49!/2	47p!	a_{24}, a_{49}	48.3	40	
.40	$\mathcal{S}_{49}$	49!	49p!	a_{48}, a_{49}	48.4		
50.1	$L_2(49)$	58800	2p	a_7, b_{50}^2	49.13	2,3,4	
.2	$\mathrm{P\Delta L}_2(49)$	117600	3t!	a_7, b_{16}	49.23	6,8	
.3	$\mathrm{PGL}_2(49)$	117600	3t!	a_7, b_{50}	49.24	6	
.4	$\mathrm{P\Sigma L}_2(49)$	117600	2p	b_{14}, b_{50}^2	49.25	6	
.5	$\mathrm{PSU}_3(5^2)$	126000	[1,7,42]	a_7, b_8^2	7.6	7	
.6	$\mathrm{P\Gamma L}_2(49)$	235200	3t	b_{14}, b_{50}	49.28	9	
.7	$\mathrm{P\Sigma U}_3(5^2)$	252000	[1,7,42]	a_7, b_8	7.7	8	srg$(50, 7, 0, 1)$
.8	$\mathcal{A}_{50}$	50!/2	48p!	a_{25}, a_{49}	49.39	9	
.9	$\mathcal{S}_{50}$	50!	50p!	a_{49}, a_{50}	49.40		

9.63 Table Generators for primitive groups of degree at most 50.

Deg	Elt	Permutation	Elt	Permutation	Elt	Permutation	Elt	Permutation
6	b_3	(1 3 4)(2 5 6)	b_6	(1 5 2 4 3 6)				
7	b_7	(1 4 6 2 3 7 5)						
8	b_6	(1 2 8 5 7 6)(3 4)	b_7	(1 5 6 8 2 4 3)	b_8	(1 2 8 3 4 7 6 5)	c_7	(1 8 7 2 5 3 6)
	d_7	(1 8 2 7 5 4 6)						
9	b_3	(1 5 9)(2 3 8)(4 7 6)	b_4	(1 6 4 5)(2 9 8 7)	b_6	(1 9 3 4 7 5)(2 8)	b_8	(1 7 5 2 8 4 3 9)
	b_9	(1 8 5 2 9 4 7 3 6)	c_4	(1 9 8 2)(3 7 5 4)	c_6	(1 2 4 6 3 9)(5 7)	c_8	(2 9 3 6 7 5 4 8)
	d_4	(1 6 4 5)(2 9 8 7)	d_6	(1 5 6 2 8 4)(3 9)	e_4	(1 3 6 2)(4 5 9 7)	e_6	(1 7 5 6 9 4)(2 8 3)
	f_6	(1 4 3)(2 8 6 7 9 5)	g_6	(1 7 8 9 6 3)(2 5 4)				
10	b_3	(1 6 8)(2 7 10)(3 9 5)	b_5	(1 10 4 7 5)(2 8 6 9 3)	b_6	(1 8 6)(2 3 7 9 10 5)	b_8	(1 8 6 2 9 5 3 10)(4 7)
	b_{10}	(1 2 5 8 9 7 4 10 6 3)	c_5	(1 3 4 5 7)(2 10 9 8 6)	c_6	(1 8 9 3 5 6)(2 7 4)	c_8	(1 6 10 9 3 8 4 5)(2 7)
	d_5	(1 10 9 6 4)(2 8 3 5 7)	d_8	(1 7 2 6 5 9 4 10)(3 8)				

Deg	Elt	Permutation	Elt	Permutation
11	b_5	(1 11 10 3 6)(2 5 4 9 7)	b_{11}	(1 2 7 9 4 3 6 11 5 8 10)
12	b_{11}	(1 12 10 3 7 5 8 4 2 11 9)	c_{11}	(2 3 7 8 10 4 5 9 6 11 12)
	d_{11}	(1 2 10 11 9 5 4 12 8 7 3)	b_{12}	(1 7 2 5 12 6 3 11 9 10 8 4)
13	b_{13}	(1 3 4 6 8 10 7 13 2 5 12 11 9)		
14	b_{13}	(1 9 4 3 8 10 13 5 11 14 2 7 6)		
15	b_2	(1 9)(2 5)(4 15)(8 13)(10 11)(12 14)	b_7	(2 6 3 8 12 4 9)(5 7 13 11 10 14 15)
	c_2	(1 5)(6 13)(7 8)(10 12)		
16	b_3	(2 16 4)(3 14 9)(5 6 11)(7 12 8)	b_4	(2 5)(3 9 8 13)(4 6 11 16)(7 14 10 12)
	b_6	(1 8 10 15 7 3)(2 11 4)(6 9 13 16 14 12)	b_7	(1 2 11 12 7 16 13)(3 15 10 9 8 6 5)
	b_{15}	(1 2 10 14 11 8 5 12 3 13 9 6 15 4 7)	c_6	(1 3 13)(2 14 16 7 5 15)(4 11 10 8 9 12)
17	b_8	(1 15 13 10 16 12 17 6)(2 8 7 4 9 11 5 14)	b_{10}	(1 16 8 4 2 14 9 12 5 7)(3 6 15 11 13)(10 17)
	b_{17}	(1 11 6 12 17 4 7 10 14 2 8 3 13 5 16 15 9)		
18	b_{17}	(1 12 13 8 2 15 16 9 7 11 10 6 14 4 18 17 3)		
20	b_{20}	(1 3 5 17 18 10 16 19 13 11 2 20 4 14 12 6 9 15 7 8)		
21	b_2	(2 17)(3 12)(4 19)(5 16)(6 13)(7 18)(9 21)(11 14)(15 20)	b_4	(1 14 8 12)(3 21 7 18)(4 20 16 19)(5 11)(9 17 10 15)
	c_4	(1 21 4 10)(2 9 11 3)(5 12 15 14)(7 13 20 8)(17 18)		
22	b_{10}	(1 15 17 2 21 14 7 3 22 10)(4 12 11 6 16 13 9 19 20 5)(8 18)		
23	b_2	(1 4)(2 6)(8 23)(9 10)(11 16)(12 19)(13 21)(14 20)		
24	b_2	(6 7)(8 19)(9 14)(10 22)(11 12)(13 24)(15 17)(20 23)		
	b_{24}	(1 2 24 3 4 15 19 22 18 16 8 7 17 23 14 5 11 21 20 12 10 6 9 13)		
25	b_2	(1 18)(2 23)(4 8)(5 13)(6 19)(7 24)(10 14)(11 20)(12 25)(17 21)		

Deg	Elt	Permutation
25	b_4	(2 3 5 4)(6 16 21 11)(7 18 25 14)(8 20 24 12)(9 17 23 15)(10 19 22 13)
	b_6	(1 9 25)(2 14 22 11 7 15)(3 19 23 16 8 20)(4 24 21 6 10 5)(13 17)
	b_8	(1 2 7 9 19 18 13 11)(3 12 6 4 17 8 14 16)(5 22 10 24 20 23 15 21)
	b_{10}	(1 3 5 2 4)(6 22 10 21 9 25 8 24 7 23)(11 16 15 20 14 19 13 18 12 17)
	b_{12}	(1 10 17)(2 5 20 16 6 7)(3 15 19 21 8 12 4 25 18 11 9 22)(13 14 24 23)
	b_{20}	(1 9 17 15 3 6 19 12 5 8 16 14 2 10 18 11 4 7 20 13)(21 24 22 25 23)
	b_{24}	(1 4 17 9 20 22 7 8 14 18 15 24 19 16 3 11 5 23 13 12 6 2 10 21)
25	c_4	(2 3 5 4)(6 19 21 13)(7 16 25 11)(8 18 24 14)(9 20 23 12)(10 17 22 15)
	c_8	(2 6 3 11 5 21 4 16)(7 8 13 15 25 24 19 17)(9 18 12 10 23 14 20 22)
	c_{20}	(2 7 21 12 15 3 13 16 23 24 5 25 6 20 17 4 19 11 9 8)(10 14 22 18)
	d_4	(1 7 3 22)(4 17 5 12)(6 8 23 21)(9 18 25 11)(10 13 24 16)(14 19 20 15)
26	b_{10}	(1 17 16 9 21 15 12 18 14 6)(2 13 19 26 24)(3 25 10 5 4 23 11 8 20 22)
	b_{12}	(1 22 14 25 11 23 17 7 18 5 10 8)(2 16 9 3 4 20 15 12 26 13 21 19)(6 24)
27	b_4	(1 18 5 3)(6 17 26 12)(7 11 21 20)(8 19 27 16)(9 15 22 10)(13 25 23 14)
	b_6	(1 5 17 22 15 6)(2 10 14 18 13 9)(3 27 12 11 26 8)(4 21 25 19 23 7)(20 24)
	b_{12}	(1 25 27 5 13 21)(2 15 18 16)(3 23 17 12)(4 19 8 9 20 14 6 26 11 10 7 22)
	b_{24}	(1 27 21 13 4 10 18 19 9 14 17 15 3 12 2 24 26 22 25 8 20 5 16 11)(6 7 23)
	b_{26}	(1 10 18 5 20 2 27 23 25 3 4 24 21 16 7 26 6 15 9 14 12 19 8 13 17 11)
	c_4	(1 2 18 15)(3 22 13 7)(4 19 26 8)(5 11 23 9)(10 14)(12 17 27 16)(20 25 21 24)
27	c_6	(1 11 26 19 9 24)(2 14 21 15 6 20)(3 16 27 17 13 23)(4 18 22 25 8 7)(5 12)
	d_6	(1 27 19 14 9 20)(2 17 21 16 7 6)(3 11 15 24 4 12)(5 8 26 13 10 22)(23 25)
28	b_6	(1 23 24 4 18 19)(2 8 7 20 21 22)(3 25 16 17 5 14)(6 9 28 15 26 13)(10 12 27)
	b_8	(1 13 26 20 16 23 7 17)(2 25 21 5 12 19 4 28)(3 9 18 6 10 24 22 11)(8 14 15 27)
	b_9	(1 27 22 26 10 23 13 12 3)(2 21 7 24 15 14 25 16 19)(4 5 17 9 18 6 28 8 20)
	b_{12}	(1 11 5 15 14 19 28 10 17 24 2 6)(3 18 13 22 16 7 25 23 4 21 20 8)(9 26 27)
	b_{26}	(1 22 4 27 23 24 5 3 7 8 21 9 25 2 26 16 20 18 10 11 14 19 12 15 17 6)
	c_6	(1 3 14)(2 27)(4 26)(5 20 9 11 19 21)(6 12 17)(8 18)(10 23 16 28 15 25)(13 22)
	c_{12}	(1 24 13 8 10 15 16 7 19 14 4 27)(2 18 11 17 23 21 6 3 9 20 22 12)(5 28 25 26)
	d_{12}	(1 14 21 20 23 4 19 22 7 25 27 9)(3 28 5 11)(6 17 26 10 16 24)(12 13 15 18)
30	b_{30}	(1 20 19 6 28 8 3 15 23 12 13 11 16 27 4 10 21 26 24 25 14 22 5 29 9 2 18 17 7 30)
31	b_{31}	(1 13 15 7 30 10 19 23 3 18 29 6 9 14 25 2 27 28 26 4 21 24 16 5 17 22 12 20 31 11 8)
	c_{31}	(1 26 4 24 19 13 10 20 23 6 17 16 15 7 22 11 12 21 9 8 14 18 5 25 3 2 27 31 30 29 28)
32	b_{10}	(1 21 25 13 6 14 10 26 32 8)(2 12 19 29 30 5 31 4 7 3)(9 16 11 27 15 23 24 18 17 20)(22 28)
	b_{31}	(1 5 19 9 23 3 24 15 2 21 12 25 6 20 28 8 11 17 14 22 7 26 29 32 4 30 31 13 10 16 18)

Deg	Elt	Permutation
32	b_{32}	(1 29 23 21 13 25 27 11 12 31 30 6 14 9 32 7 2 10 17 16 4 5 20 22 3 26 24 18 15 19 8 28)
33	b_{15}	(1 20 29 24 7 32 17 16 8 18 30 6 10 13 23)(2 22 14 33 4 21 31 11 9 28 15 19 25 12 5)(3 26 27)
35	b_{12}	(1 21 31 28 9 12 29 15 3 25 33 27)(2 5 30 10 26 34 16 22 35 17 7 18)(4 14 6 8 13 32)(11 20 19 23)
	$a_{15,5}$	(a_{15} for degree 30) · (31 32 33 34 35)
36	b_6	(1 10 16 20 28 29)(2 15 35 13 12 3)(4 19 27)(6 26 34)(7 31 25)(8 14)(9 17 24 21 22 23)(11 32 30)
	b_8	(1 17 33 30 2 28 25 24)(3 22 31 10 4 6 36 27)(5 35 11 34 7 23 20 13)(8 29 15 9 18 26 32 19)
	b_{10}	(1 11 33 28 22 15 23 14 20 13)(2 25 31 30 9)(3 8 6 26 18 19 36 16 21 32)(4 27 17 34 35 12 10 29 7 5)
	b_{12}	(1 36 6 21 14 22 26 2 34 31 8 28)(3 35 32 10 11 24 23 4 19 17 18 7)(5 30 16 9 29 12 13 33 25 15 20 27)
	c_8	(1 14 30 5 35 27 21 6)(2 16 17 19)(3 18 34 4 12 31 20 15)(7 9 36 25 10 33 24 28)(8 32 23 11 29 22 13 26)
	c_{12}	(1 35 2 8 7 26)(3 10 28 13 23 34 17 27 30 21 5 12)(4 18 11 20 29 24 36 15 16 14 19 31)(6 9 32 22 25 33)
38	b_{38}	(1 20 4 18 29 38 12 23 37 21 3 32 36 17 6 33 30 10 16 15 28 14 22 7 2 34 19 27 13 26 25 31 11 8 35 24 5 9)
40	b_5	(1 29 26 4 13)(2 28 38 30 22)(3 8 39 16 32)(5 7 27 14 15)(6 25 23 37 9)(10 17 11 40 35)(12 34 18 24 31)(19 36 21 33 20)
	b_{10}	(1 2 3 4 27 20 12 5 6 25)(7 26 17 9 8)(10 13 11 24 33 38 22 31 18 30)(14 34 21 36 37 2315 35 16 29)(19 40 39 32 28)
42	b_{42}	(1 38 15 6 25 14 16 18 7 26 17 35 31 24 12 19 41 4 39 9 40 37 11 3 27 22 30 42 2 10 5 29 21 36 33 23 34 28 32 13 20 8)
44	b_{44}	(1 41 29 9 42 43 8 22 15 26 31 13 2 34 16 21 32 25 39 4 5 38 18 6 3 12 36 10 28 27 14 30 40 24 44 23 7 17 33 20 19 37 11 35)
45	b_8	(1 9 20 37 41 45 34 12)(2 11 8 31 26 5 27 40)(3 39 32 7)(4 6 25 42 36 35 44 28)(13 33 38 19 23 22 21 30)(14 29 43 24 18 17 16 15)
	b_{10}	(1 2 3 4 5 6 7 8 9 10)(11 12 13 14 15 16 17 18 19 20)(21 22 23 24 25 26 27 28 29 30)(31 32 33 34 35 36 37 38 39 40)(41 42 43 44 45)
	c_8	(1 5 16 11 33 13 32 19)(2 15 3 36 12 23 25 40)(4 29 22 41)(6 24 18 37 21 45 34 14)(7 35 28 31 8 30 20 17)(9 10 38 27 42 39 26 44)
	d_8	(1 45 18 31)(2 21 12 34 13 39 22 4)(3 41 35 40)(5 38 10 37 32 16 14 25)(6 9 8 29 26 28 17 27)(7 43 11 19 15 44 36 24)(20 23 42 30)
48	b_{47}	(1 32 48 12 4 43 30 45 20 27 34 9 24 11 2 42 6 22 5 37 23 13 33 38 46 39 19 25 7 18 44 14 28 26 40 10 36 47 29 35 15 8 16 21 41 31 17)
49	b_3	(2 3 5)(4 7 6)(8 35 16)(9 30 20)(10 32 17)(11 34 21)(12 29 18)(13 31 15)(14 33 19)(22 40 46)(23 42 43)(24 37 47)(25 39 44)(26 41 48)(27 36 45)(28 38 49)
	b_6	(2 4 3 7 5 6)(8 45 12 43 13 46)(9 48 14 49 10 44)(11 47)(15 40 16 36 18 42)(17 39 20 41 19 38)(21 37)(22 35 27 29 23 31)(24 34)(25 30 26 33 28 32)
	b_8	(2 16 11 19 7 42 47 39)(3 31 21 30 6 27 37 28)(4 46 24 48 5 12 34 10)(8 23 33 44 43 35 25 14)(9 38 36 13 49 20 15 45)(17 26 22 18 41 32 29 40)
	b_{12}	(2 12 4 27 3 16 7 46 5 31 6 42)(8 23 22 18 15 45 43 35 29 40 36 13)(9 34 25 37 17 11 49 24 33 21 41 47)(10 38 28 14 19 26 48 20 30 44 39 32)
	b_{14}	(1 7 49 48 41 40 33 32 25 24 17 16 9 8)(2 14 43 6 42 47 34 39 26 31 18 23 10 15)(3 21 44 13 36 5 35 46 27 38 19 30 11 22)(4 28 45 20 37 12 29)
	b_{24}	(1 33 14 23 38 48 15 32 7 26 10 44 36 34 21 25 3 47 8 30 42 27 17 46)(2 40 13 16 39 6 19 11)(4 5 12 9 37 41 20 18)(22 31 49)(24 45 43 29 35 28)
	b_{42}	(1 6 14 2 23 41 16 21 22 17 38 7 31 29 37 32 4 15 46 44 3 47 19 30 12 10 18 13 34 45 27 25 33 28 49 11 42 40 48 36 8 26)(5 39 24 9 43 35 20)
	b_{48}	(1 3 42 34 24 31 46 15 33 29 14 23 36 22 48 5 25 26 21 38 12 40 44 32 41 39 7 8 18 11 45 27 9 13 35 19 6 20 43 37 17 16 28 4 30 2 47 10)
	c_6	(2 4 3 7 5 6)(8 43)(9 46 10 49 12 48)(11 45 14 47 13 44)(15 36)(16 39 17 42 19 41)(18 38 21 40 20 37)(22 29)(23 32 24 35 26 34)(25 31 28 33 27 30)
	d_6	(2 4 3 7 5 6)(8 36 29 43 15 22)(9 39 31 49 19 27)(10 42 33 48 16 25)(11 38 35 47 20 23)(12 41 30 46 17 28)(13 37 32 45 21 26)(14 40 34 44 18 24)
50	b_8	(1 27 15 19)(2 37 40 43 34 33 32 14)(3 38)(4 7 16 25 28 18 35 49)(5 22 6 23 45 36 30 47)(8 48 17 9)(10 41 11 42 24 46 31 26)(12 21 13 50 20 44 29 39)
	b_{14}	(1 26 2 27 3 28 4 22 5 23 6 24 7 25)(8 12 9 13 10 14 11)(15 33 16 34 17 35 18 29 19 30 20 31 21 32)(36 43 37 44 38 45 39 46 40 47 41 48 42 49)
	b_{16}	(1 6 11 4 7 8 38 39 10 44 24 37 36 45 26 35)(2 21 19 47 18 20 22 28 49 32 9 23 25 48 3 30)(5 17 46 15 27 40 12 13 16 31 34 14 50 29 41 43)(33 42)
	b_{50}	(1 34 30 17 7 10 44 37 41 18 39 25 26 28 40 20 43 8 32 31 16 47 29 48 14 49 24 12 11 35 46 27 3 19 21 15 4 22 2 6 45 33 36 23 13 9 42 5 50 38)

9.5 Simple Groups

9.64 Remark The classification of all finite simple groups has been a major accomplishment of modern group theory. As a result of a remarkable effort by mathematicians from all continents, spanning about two and a half decades (1955–1980), all finite simple groups have been classified. See [935] for an introduction to the proof.

Apart from the cyclic groups $\mathbb{Z}_p$ of prime order, and the alternating groups $\mathcal{A}_n$, there are 16 infinite classes of simple groups of *Lie* type, and an additional 26 *sporadic simple groups* that do not fall in any of the other classes. The simple groups of Lie type consist of 6 classes of so-called *classical* groups, and another 10 classes of so-called *exceptional simple groups*. The classical simple groups consist of *linear, symplectic, orthogonal*, and *unitary* groups. The smallest sporadic simple group is the Mathieu group M_{11} of order 7920, and the largest is a group denoted by F_1, of order $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$. F_1 is the *Fischer–Griess* group or the (friendly) *giant*. Its existence was established by Griess, who based his construction on results by several other people notably on work of Norton, but also of Conway, Fischer, Livingstone, Thorne, and Smith, and his own earlier work. The uniqueness of a simple group of "type F_1" [934] was established by Thompson and Norton. This remarkable giant is constructed as a group of complex matrices of degree $196,883$. It is worth noting that every finite simple group has a representation as a primitive permutation group of rank at most 8, where the stabilizer of a point is a (smaller) simple group.

9.65 Remark Data related to the simple groups of order less than 100 million are displayed in seven columns. (The 106 groups $L_2(q)$ for $q > 5^3$ are omitted; their structure is known and described fully by Dickson [702].) The first column gives the name of the simple group using the conventions in §9.3. Column 2 displays the order of the group. The third column, labeled $\Omega.\{\sigma, \mu\}$ gives information in the form $n.x$. Here, n is a positive integer indicating the order of the outer automorphism group of G, and x is one of the two Greek letters σ, μ. If a μ appears then the group is *minimal simple*; that is, the group is simple with all of its subgroups solvable. If a σ appears, then the simple group has nonsolvable subgroups, some of which are listed in column 6. In a few instances, as in the case of $L_3(7)$ and $U_4(3)$, in position n of column 3 the isomorphism type of the outer-automorphism group is listed instead of its order. The next column gives information about the conjugacy classes of the group. Only a *signature* that describes the number of conjugacy classes of nonidentity elements of a given order is given. As an example, for group $U_3(3)$ the signature $2^1 3^2 4^3 6^1 7^2 8^2 12^2$ says that there is a single conjugacy class of involutions, two classes of elements of order 3, three classes of elements of order 4, and so on.

Column 5 displays the *primitive spectrum* of the group. This is the list of degrees of the various (inequivalent) primitive permutation representations for the group. An exponent here denotes that there is more than one inequivalent primitive representation of a particular degree for the given group. For example, $\mathcal{A}_6$ has two inequivalent primitive representations of degree 6 (corresponding to two conjugacy classes of $\mathcal{A}_5$s in $\mathcal{A}_6$), one primitive representation of degree 10, and two inequivalent primitive representations of degree 15. Column 6 displays some nonsolvable subgroups that are contained in the given group. Here the existence of several conjugacy classes of a certain nonsolvable group is indicated by a *multiplicity index* positioned in front of the subgroup specified. For example, the simple group $U_3(5) \cong PSU_3(5^2)$ contains three conjugacy classes of $\mathcal{A}_7$s, three classes of M_{10}s, and a class of $\mathcal{S}_5$s. If a group G is generated as $G = \langle x, y \rangle$, where $|x| = \ell$, $|y| = m$, and $|xy| = n$, G is an (ℓ, m, n) group. The seventh column provides several ways in which G is an (ℓ, m, n) group.

9.66 Table Simple groups of order less than 100,000,000.

Group G	$\lvert G\rvert$	$\Omega.\{\sigma,\mu\}$	Conjugacy Classes	Primitive Spec.	n.s. $H<G$	Generated as (ℓ,m,n)
$\mathcal{A}_5\cong L_2(4)\cong L_2(5)$	60	$2.\mu$	$2^1 3^1 5^2$	$5,6,10$	-	(2,3,5)
$L_3(2)\cong L_2(7)$	168	$2.\mu$	$2^1 3^1 4^1 7^2$	$7^2,8$	-	(2,3,7),(2,4,7),(3,3,4),(2,7,7)
$\mathcal{A}_6\cong L_2(9)$	360	$4.\sigma$	$2^1 3^2 4^1 5^2$	$6^2,10,15^2$	${}_2\mathcal{A}_5$	(2,4,5),(3,3,4),(3,4,5),(2,5,5)
$L_2(8)$	504	$3.\mu$	$2^1 3^1 7^3 9^3$	$9,28,36$	-	(2,3,7),(2,3,9),(2,7,9),(2,7,7)
$L_2(11)$	660	$2.\sigma$	$2^1 3^1 5^2 6^1 11^2$	$11^2,12,55$	${}_2\mathcal{A}_5$	(2,3,11),(2,5,6),(2,5,11),(2,5,5)
$L_2(13)$	1092	$2.\mu$	$2^1 3^1 6^1 7^3 13^2$	$14,78,91^2$	-	(2,3,7),(2,3,13),(2,6,7),(2,7,13)
$L_2(17)$	2448	$2.\mu$	$2^1 3^1 4^1 8^2 9^3 17^2$	$18,136,153,102^2$	-	(2,3,8),(2,3,9),(2,3,17)
$\mathcal{A}_7$	2520	$2.\sigma$	$2^1 3^2 4^1 5^1 6^1 7^2$	$7,15^2,21,35$	$\mathcal{A}_6,\mathcal{A}_5$	(2,4,7),(2,5,7),(2,6,7),(2,7,7)
$L_2(19)$	3420	$2.\sigma$	$2^1 3^1 5^2 9^3 10^2 19^2$	$20,57^2,171,190$	${}_2\mathcal{A}_5$	(2,3,9),(2,3,19),(2,5,9),(2,5,5)
$L_2(16)$	4080	$4.\sigma$	$2^1 3^1 5^2 15^4 17^8$	$17,68,120,136$	$\mathcal{A}_5$	(2,3,17),(2,5,17),(2,3,15),(2,5,15)
$L_3(3)$	5616	$2.\mu$	$2^1 3^2 4^1 6^1 8^2 13^4$	$13^2,144,234$	-	(2,3,13),(2,4,13),(2,8,8),(3,4,13)
$U_3(3)$	6048	$2.\sigma$	$2^1 3^2 4^3 6^1 7^2 8^2 12^2$	$28,36,63^2$	$L_2(7)$	(2,7,17),(2,6,7),(3,4,7),(3,6,7)
$L_2(23)$	6072	$2.\mu$	$2^1 3^1 4^1 6^1 12^2 11^5 23^2$	$24,253^3,276$	-	(2,3,11),(2,3,12),(2,4,6),(2,6,11)
$L_2(25)$	7800	$4.\sigma$	$2^1 3^1 4^1 5^2 6^1 12^2 13^6$	$26,65^2,300,325$	S_5	(2,3,13),(2,3,12),(2,4,13),(2,5,13)
M_{11}	7920	$1.\sigma$	$2^1 3^1 4^1 5^1 6^1 8^2 11^2$	$11,12,55,66,165$	$L_2(11),\mathcal{S}_5,M_{10}$	(2,5,11),(2,5,8),(2,4,11),(3,4,5)
$L_2(27)$	9828	$6.\mu$	$2^1 3^2 7^3 14^3 13^6$	$28,351,378,819$	-	(2,3,7),(2,3,13),(2,7,13),(2,7,7)
$L_2(29)$	12180	$2.\sigma$	$2^1 3^1 5^2 7^3 14^3 15^4 29^2$	$30,203^2,406,435$	${}_2\mathcal{A}_5$	(2,3,7),(2,5,7),(2,3,15),(2,5,15)
$L_2(31)$	14880	$2.\sigma$	$2^1 3^1 4^1 5^2 8^2 15^4 16^4 31^2$	$32,248^2,465,496$	${}_2\mathcal{A}_5$	(2,3,15),(2,3,8),(2,4,5),(2,5,16)
$\mathcal{A}_8\cong L_4(2)$	20160	$2.\sigma$	$2^2 3^2 4^2 5^1 6^2 7^2 15^2$	$8,15^2,28,35,36$	$\mathcal{A}_7,L_2(7),\mathcal{S}_5$	(2,5,7),(2,7,15),(2,4,9),(3,4,15)
$L_3(4)\cong M_{21}$	20160	$12.\sigma$	$2^2 3^1 4^3 5^2 7^2$	$21^2,56^3,120^3,280$	$L_2(7),\mathcal{A}_6,\mathcal{A}_5$	(2,5,7),(2,5,5),(2,4,7),(3,4,7)
$L_2(37)$	25308	$2.\mu$	$2^1 3^1 9^3 6^1 18^3 19^9 37^2$	$38,666,703,2109$	-	(2,3,37),(2,3,9),(2,9,19),(2,18,19)
$U_4(2)\cong S_4(3)$	25920	$2.\sigma$	$2^2 3^4 4^2 5^1 6^6 9^2 12^2$	$27,36,40^2,45$	$\mathcal{S}_5,\mathcal{S}_6$	(2,4,9),(2,5,9),(3,4,9),(3,5,6)
$Sz(8)$	29120	$3.\mu$	$2^1 4^2 5^1 7^3 13^3$	$65,560,1456,2080$	-	(2,5,7),(2,5,13),(2,7,13),(2,4,5)
$L_2(32)$	32736	$5.\mu$	$2^1 3^1 11^5 33^{10} 31^{15}$	$33,496,528$	-	(2,3,11),(2,3,31),(2,11,31),(2,31,33)
$L_2(41)$	34440	$2.\mu$	$2^1 3^1 4^1 5^2 7^3 10^2$ $20^4 21^6 41^2$	$42,820,861,1435^2$	${}_2\mathcal{A}_5$	(2,3,7),(2,3,10),(2,5,20),(2,7,20)
$L_2(43)$	39732	$2.\mu$	$2^1 3^1 7^3 11^5 21^6$ $22^5 43^2$	$44,903,946,3311$	-	(2,3,7),(2,3,11),(2,7,11),(3,7,11)
$L_2(47)$	51888	$2.\mu$	$2^1 3^1 4^1 6^1 8^2 12^2$ $23^{11} 24^4 47^2$	$48,1081,1128,2162^2$	-	(2,3,8),(2,3,23),(2,3,47),(3,4,47)

Group G	$\lvert G\rvert$	$\Omega.\{\sigma,\mu\}$	Conjugacy Classes	Primitive Spec.	n.s. $H<G$	Generated as (ℓ,m,n)
$L_2(49)$	58800	$4.\sigma$	$2^1 3^1 4^1 5^2 6^1 7^2$ $8^2 12^2 24^4 25^{10}$	$50, 175^2, 400,$ $1176,\ 1225$	${}_2PGL_2(7)$ ${}_2\mathcal{A}_5$	(2,3,12),(2,7,25), (3,4,5),(3,4,6)
$U_3(4)$	62400	$4.\sigma$	$2^1 3^1 4^1 5^6 10^4 13^4 15^4$	$65, 208, 416, 1600$	$\mathcal{A}_5$	(2,3,13),(2,3,15),(2,10,13),(2,13,15)
$L_2(53)$	74412	$2.\mu$	$2^1 3^1 9^3 13^6 26^6 27^9 53^2$	$54, 1378, 1431, 6201$	-	(2,3,13),(2,3,9),(2,9,26),(2,13,27)
M_{12}	95040	$2.\sigma$	$2^2 3^2 4^2 5^1 6^2 8^2$ $10^1 11^2$	$12^2, 66^2, 144, 220^2,$ $396, 495^2, 1320$	${}_2M_{11},\ {}_2\mathcal{A}_6,$ ${}_3L_2(11),\ \mathcal{S}_5$	(2,3,11),(2,3,10) (2,5,6),(2,5,11)
$L_2(59)$	102660	$2.\sigma$	$2^1 3^1 5^2 6^1 10^2$ $15^4 29^{14} 30^4 59^2$	$60, 1711^3, 1770$	${}_2\mathcal{A}_5$	(2,3,29),(2,3,10), (2,3,15),(3,5,10)
$L_2(61)$	113460	$2.\sigma$	$2^1 3^1 5^2 6^1 10^2$ $15^4 30^4 31^{15} 61^2$	$62, 1891^3, 1830$	${}_2\mathcal{A}_5$	(2,3,31),(2,3,10) (2,5,31),(2,15,31)
$U_3(5)$	126000	$5.\sigma$	$2^1 3^1 4^1 5^4 6^1 7^2 8^2 10^1$	$50^3, 126, 175^3, 525$	${}_3\mathcal{A}_7, {}_3M_{10}, \mathcal{S}_5$	(2,5,7),(2,4,10),(3,5,7),(3,7,10)
$L_2(67)$	150348	$2.\mu$	$2^1 3^1 11^5 17^8 33^{10} 34^8 67^2$	$68, 2211, 2278, 12529$	-	(2,3,11),(2,3,17),(2,11,67),(2,17,33)
Ja_1	175560	$1.\sigma$	$2^1 3^1 5^2 6^1 7^1$ $10^2 11^1 15^2 19^3$	$266,\ 1045,\ 1463,$ $1540, 1596, 2926, 4180$	$L_2(11),\ \mathcal{A}_5$	(2,3,7),(2,3,11), (2,3,19),(5,7,19)
$L_2(71)$	178920	$2.\sigma$	$2^1 3^1 4^1 5^2 6^1 7^3 9^3$ $12^2 18^3 35^{12} 36^6 71^2$	$72,\ 2485,\ 2556,\ 2982^2$	${}_2\mathcal{A}_5$	(2,3,7),(2,3,71), (2,5,6), (2,6,36),(2,9,35),(5,12,71)
$\mathcal{A}_9$	181440	$2.\sigma$	$2^2 3^3 4^2 5^1 6^2 7^1$ $9^2 10^1 12^1 15^2$	$9, 36, 84, 120^2$ $126,\ 280,\ 840$	$\mathcal{A}_8, \mathcal{S}_7$	(2,3,15),(2,4,7), (3,7,9),(3,7,15)
$L_2(73)$	194472	$2.\mu$	$2^1 3^1 4^1 6^1 9^3$ $12^2 18^3 36^6 37^{18} 73^2$	$74, 2628, 2701,$ 8103^2	-	(2,3,37),(2,3,9), (2,3,73),(2,12,37),(3,6,37)
$L_2(79)$	246480	$2.\sigma$	$2^1 3^1 4^1 5^2 8^2$ $10^2 13^6 20^4 39^{12} 40^8 79^2$	$80, 3081, 3160,$ 4108^2	${}_2\mathcal{A}_5$	(2,3,8),(2,3,13), (2,3,79),(2,13,39),(3,8,13)
$L_2(64)$	262080	$6.\sigma$	$2^1 3^1 5^2 7^3 9^3 13^6 21^6 63^{18} 65^{24}$	$65, 520^2, 2016, 2080$	$\mathcal{A}_5,\ L_2(8)$	(2,3,13),(2,3,63),(2,5,63),(5,13,63)
$L_2(81)$	265680	$4.\sigma$	$2^1 3^2 4^1 5^2 8^2$ $10^2 20^4 40^8 41^{20}$	$82, 369^2, 3240,$ 3321^2	${}_2\mathcal{A}_5$ ${}_2\mathcal{A}_6$	(2,3,41),(2,5,41), (2,10,41),(3,5,8)
$L_2(83)$	285852	$2.\mu$	$2^1 3^1 6^1 7^3 14^3$ $21^6 41^{20} 42^5 83^2$	$84, 3403^2, 3486$ 22821	-	(2,3,7),(2,3,41), (2,41,83),(3,7,41)
$L_2(89)$	352440	$2.\sigma$	$2^1 3^1 4^1 5^2 9^3 11^5$ $15^4 22^5 44^{10} 45^{12} 89^2$	$90, 3916, 4005^2,$ $14685^2, 11748^2$	${}_2\mathcal{A}_5$	(2,3,11),(2,3,9), (2,3,89), (2,11,89),(3,5,45),(3,5,89)
$L_3(5)$	372000	$2.\sigma$	$2^1 3^1 4^3 5^2 6^1 8^2$ $10^1 12^2 20^2 24^4 31^{10}$	$31^2, 3100, 3875, 4000$	$\mathcal{S}_5$	(2,3,31),(2,5,31),(3,8,31), (3,10,24),(3,12,31),(3,20,24)
M_{22}	443520	$2.\sigma$	$2^1 3^1 4^2 5^1 6^1 7^2$ $8^1 11^2$	$22, 77, 176^2, 231,$ $330, 616, 672$	$M_{21},\ {}_2\mathcal{A}_7,$ $L_3(2), \mathcal{A}_6, L_2(11)$	(2,5,7),(2,5,11),(3,4,7), (3,4,11),(3,5,7),(3,5,8)

Group G	$\lvert G\rvert$	$\Omega.\{\sigma,\mu\}$	Conjugacy Classes	Primitive Spec.	n.s. $H<G$	Generated as (ℓ,m,n)
$L_2(97)$	456288	$2.\mu$	$2^1 3^1 4^1 6^1 7^3 8^2 12^2 16^4$ $24^4 48^8 49^{20} 97^2$	$98, 4656, 7453^2$, 19012^2	-	(2,3,7),(2,3,8),(2,3,49), (3,12,49),(3,7,24),(3,12,49)
$L_2(101)$	515100	$2.\sigma$	$2^1 3^1 5^2 10^2 17^8$ $25^{10} 50^{10} 51^{16} 101^2$	$102, 1717^2, 5050$, 5151^2	${}_2\mathcal{A}_5$	(2,3,17),(2,3,10), (2,17,25), (3,17,50),(5,17,51),(5,17,101)
$L_2(103)$	546312	$2.\mu$	$2^1 3^1 4^1 13^6 17^8$ $26^6 51^{16} 52^{12} 103^2$	$104, 5253^2$, $5356, 277823^2$	-	(2,3,13),(2,3,17),(2,51,52), (3,4,52),(4,13,51)
HaJ	604800	$2.\sigma$	$2^2 3^2 4^1 5^4 6^2 7^1$ $8^1 10^4 12^1 15^2$	100,280,315, 525, 840, 1008, 1800, 2016, 10080	$U_3(3), PGL_2(9)$ ${}_4\mathcal{A}_5, L_3(2)$	(2,3,7),(2,3,10),(2,5,7), (2,5,15),(2,6,7),(3,7,10)
$L_2(107)$	612468	$2.\mu$	$2^1 3^1 6^1 9^3 18^3$ $27^9 53^{26} 54^9 107^2$	$108, 5671^2$, 5778, 51039	-	(2,3,53),(2,3,9), (2,9,54),(3,9,27),(3,9,53)
$L_2(109)$	647460	$2.\mu$	$2^1 3^1 5^2 6^1 9^3 11^5 18^3$ $27^9 54^9 55^{20} 109^2$	110, 5886, $5995^2, 10791^2$	${}_2\mathcal{A}_5$	(2,3,11),(2,3,9),(2,11,55), (2,54,55),(5,6,27),(5,11,18)
$L_2(113)$	721392	$2.\mu$	$2^1 3^1 4^1 7^3 8^2 14^3 19^9$ $28^6 56^{12} 57^{18} 113^2$	114, 6328, $6441^2, 30058^2$	-	(2,3,7),(2,3,19),(2,7,7), (3,7,57),(2,57,57),(3,19,28)
$L_2(11^2)$	885720	$4.\sigma$	$2^1 3^1 4^1 5^2 6^1 10^2 11^2 12^2$ $15^4 20^4 30^4 60^8 61^{30}$	$122, 671^3, 7260$, $7381^2, 36905^2$	${}_2\mathcal{A}_5$ ${}_2L_2(11)$	(2,3,15),(2,3,61), (2,10,61),(3,5,61),(3,11,61),
$L_2(5^3)$	976500	$6.\sigma$	$2^1 3^1 5^2 7^3 9^3 21^5$ $31^{15} 62^{15} 63^{18}$	126, 7750, $7875^2, 16275$	$\mathcal{A}_5$	(2,3,7),(2,3,31), (2,31,63),(5,7,21)
$S_4(4)$	979200	$4.\sigma$	$2^3 3^2 4^2 5^5 6^2 10^4$ $15^4 17^4$	$85^2, 120^2, 136^2$, 1360	${}_2\mathcal{A}_5, \mathcal{S}_6$, ${}_2\mathcal{A}_5 \times \mathcal{A}_5, {}_2L_2(16)$	(2,5,17),(2,4,5), (2,10,15),(3,5,6),(3,10,17)
$S_6(2)$	1451520	$1.\sigma$	$2^4 3^3 4^5 5^1 6^7 7^1$ $8^2 9^1 10^1 12^3 15^1$	$28, 36, 63, 120$, $135, 315, 336, 960$	$U_4(2), U_3(3), \mathcal{S}_8$, ${}_2\mathcal{S}_6, L_3(2), L_2(8)$	(2,5,7),(2,3,15), (4,5,12),(5,6,7),(6,7,9)
$\mathcal{A}_{10}$	1814400	$2.\sigma$	$2^2 3^3 4^3 5^2 6^3 7^1$ $8^1 9^2 10^1 12^2 15^1$ 21^2	10,45,120,126, 210, 945, 2520	$\mathcal{S}_8, \mathcal{A}_9, \mathcal{A}_7 \times \mathbb{Z}_3$, $M_{10}, \mathcal{A}_5 \times \mathcal{A}_5$, $\mathcal{S}_5,\ \mathcal{A}_6 \times \mathcal{A}_4$	(2,3,8),(2,3,9) (3,4,9),(3,7,8) (4,5,9),(6,7,8)
$L_3(7)$	1876896	$\mathcal{S}_3.\sigma$	$2^1 3^1 4^1 6^1 7^4 8^2$ $14^1 16^4 19^6$	$57^2, 5586^3$, $26068^2, 32928$	$L_2(7)$	(2,3,19),(3,7,8), (3,7,19),(3,8,16)
$U_4(3)$	3265920	$D_8.\sigma$	$2^1 3^4 4^2 5^1 6^3 7^2$ $8^1 9^4 12^1$	$112, 126^2, 162^2, 280, 540$, $567^2, 1296^4$, $2835, 4536^2$	${}_3\mathcal{A}_6,\ {}_2U_4(2)$, ${}_2L_3(4),\ U_3(3)$ ${}_4\mathcal{A}_7,\ {}_2M_{10}$	(2,5,7),(3,7,7),(3,7,9), (4,5,6),(4,5,7),(4,5,9), (5,6,7),(6,7,8)
$G_2(3)$	4245696	$2.\sigma$	$2^1 3^5 4^2 6^4 7^1 8^2$ $9^3 12^2 13^2$	$351^2, 364^2, 378^2$, $2808, 3159, 3888, 7371$	${}_2U_3(3),\ {}_2L_3(3)$, $L_2(8),\ L_3(2), L_2(13)$	(2,3,17), (2,4,13)
$S_4(5)$	4680000	$2.\sigma$	$2^2 3^2 4^2 5^6 6^3 10^6$ $12^2 13^3 15^3 20^2 30^2$	$156^2, 300, 325, 4875$, $6500, 9750, 13000$	${}_4\mathcal{A}_5,\ \mathcal{A}_5 \times \mathcal{A}_5,\ L_2(25)$ $\mathcal{A}_6,\ \mathcal{S}_3 \times \mathcal{S}_5$	(2,5,13),(3,10,13),(4,13,15) (3,10,15),(4,5,13),

Group G	$\lvert G\rvert$	$\Omega.\{\sigma,\mu\}$	Conjugacy Classes	Primitive Spec.	n.s. $H<G$	Generated as (ℓ,m,n)
$U_3(8)$	5515776	$12.\sigma$	$2^1 3^3 4^3 6^2 7^3$ $9^3 19^6 21^6$	$513, 3648, 25536^3$, $34048, 96768$	$L_2(8)$	(2,7,19),(2,7,7),(6,19,19), (19,19,19), (19,19,21),(19,21,21)
$U_3(7)$	5663616	$2.\sigma$	$2^1 3^1 4^3 6^1 7^2 8^{10} 12^2 14^1$ $16^4 24^4 28^2 43^{14} 48^8 56^4$	$344, 2107, 14749,$ $16856, 43904$	${}_2L_2(7)$	(2,3,43),(3,8,43), (3,14,28),(6,8,16),(3,3,43)
$L_4(3)$	6065280	$4.\sigma$	$2^2 3^4 4^3 5^1 6^5 8^1 9^2$ $10^1 12^3 13^4 20^2$	$40^2, 117^2, 130,$ $2106, 8424, 10530$	${}_2L_3(3), {}_2U_4(2)$ $\mathcal{A}_6,\ \mathcal{S}_6$	(2,3,13),(2,13,13),(3,6,13), (3,8,13),(3,13,20),(4,12,13)
$L_5(2)$	9999360	$2.\sigma$	$2^2 3^2 3^3 5^1 6^2 7^2$ $8^1 12^1 14^2 15^2 21^2 31^6$	$31^2, 155^2,$ 64512	${}_2L_4(2),$ ${}_2\mathcal{S}_3 \times L_3(2)$	(2,3,31),(3,14,21),(4,5,6), (4,6,14),(4,7,14),(4,7,31)
M_{23}	10200960	$1.\sigma$	$2^1 3^1 4^1 5^1 6^1 7^2$ $8^1 11^2 14^2 15^2 23^2$	$23, 253^2, 506,$ $1288, 1771, 40320$	$M_{22}, L_3(4), \mathcal{A}_7,$ $\mathcal{A}_8, M_{11}, \mathcal{A}_5$	(2,5,11),(2,5,23),(4,8,14), (4,11,15),(5,6,23),(5,7,11)
$U_5(2)$	13685760	$2.\sigma$	$2^2 3^6 4^3 5^1 6^{14} 8^1$ $9^4 11^2 12^9 15^2 18^2$	$165, 176, 297,$ $1408, 3520, 20736$	$U_4(2),$ ${}_2\mathcal{A}_5, L_2(11)$	(3,9,15),(4,8,9),(5,6,12), (5,6,15),(5,8,11),(6,9,11)
$L_3(8)$	16482816	$6.\sigma$	$2^1 3^1 4^1 7^{11} 9^3$ $14^6 21^6 63^{18} 73^{24}$	$73^2, 5604,$ $75264, 98112$	${}_2L_2(8),$ $L_3(2)$	(3,4,63),(3,7,73) (4,7,63),(4,9,63),(7,9,14)
${}^2F_4(2)'$	17971200	$2.\sigma$	$2^2 3^1 4^3 5^1 6^1 8^4$ $10^1 12^2 13^2 16^4$	$1600^2, 1755, 2304,$ $2925, 12480^2, 14976$	${}_2L_3(3),$ $L_2(25), {}_2\mathcal{A}_6$	(2,3,13)
$\mathcal{A}_{11}$	19958400	$2.\sigma$	$2^2 3^3 4^3 5^2 6^5 7^1 8^1 9^1 10^1$ $11^2 12^3 14^1 15^2 20^1 21^2$	$11, 55, 165, 330,$ $462, 2520^2$	$\mathcal{A}_{10},\ \mathcal{A}_7 \times \mathcal{A}_4, \mathcal{A}_8,$ $\mathcal{S}_9,\ \mathcal{A}_6 \times \mathcal{A}_5, {}_2M_{11}$	(3,4,11),(3,8,11),(4,8,11), (5,8,20),(6,7,9),(6,8,9)
$Sz(32)$	32537600	$5.\mu$	$2^1 4^2 5^1 25^5$ $31^{15} 41^{10}$	$1025, 198400,$ $325376, 524800$	-	(2,4,25),(2,5,31) (2,5,41),(2,31,41)
$L_3(9)$	42456960	$4.\sigma$	$2^1 3^2 4^3 5^2 6^1 7^2$ $8^{10} 10^2 12^2 13^4$ $16^4 20^4 24^4 40^8 80^{16} 91^{24}$	$91^2, 7020, 7560,$ $58968, 110565,$ 155520	$U_3(3),$ $L_3(3)$ $\mathrm{PGL}_2(9),\ {}_2GL_2(9)$	(4,8,24),(4,16,91) (7,8,16),(8,10,12)
$U_3(9)$	42573600	$4.\sigma$	$2^1 3^2 4^1 5^6 6^1 8^2 10^{14} 15^4 16^4$ $20^4 30^4 40^8 73^{24} 80^{16}$	$730, 5913, 59130,$ $70956, 194400$	${}_2\mathcal{A}_6$	(2,5,73),(2,15,10), (2,4,20),(2,40,40)
HS	44352000	$2.\sigma$	$2^2 3^1 4^3 5^3 6^2 7^1$ $8^3 10^2 11^2 12^1$ $15^1 20^2$	$100, 176^2, 1100^2,$ $3850, 4125, 5600^2,$ $5775, 15400, 36960$	$M_{22}, L_3(2), \mathcal{S}_5, \mathcal{A}_6,$ ${}_2U_3(5), L_3(4), \mathcal{A}_5$ $\mathcal{S}_6, \mathcal{S}_8,\ {}_2M_{11}$	(4,5,6),(4,7,11) (5,7,8),(5,7,11) (5,8,10),(6,7,8)
J_3	50232960	$2.\sigma$		$6156, 14688^2, 17442,$ $20520, 23256, 25840,$ $26163, 43605$	$L_2(16),\ {}_2L_2(19)$ $L_2(17), \mathcal{A}_6$ ${}_2\mathcal{A}_5$	(2,3,19)
$U_3(11)$	70915680	$\mathcal{S}_3.\sigma$	$2^1 3^1 4^3 5^2 6^1 8^2$ $10^2 11^4 12^4 20^4$ $22^1 37^1 240^8 44^2$	$1332, 13431, 53724^3,$ $196988^3, 246235,$ $638880, 984940$	${}_4L_2(11),$ ${}_3\mathcal{A}_6$	(4,12,12),(8,37,44) (10,10,37),(37,37,37)

See Also

§II.5	Gives some Steiner systems with large automorphism groups.
§II.4	t-designs with large automorphism groups.
§III.2	Quasigroups are generalizations of groups.
§VII.6	Groups are used extensively to reduce the computation time in algorithms to produce designs.
[225]	A nice summary treatment of multiply transitive groups.
[933, 1014, 2137]	The fundamental standard references for permutation groups and group actions.

References Cited: [225, 434, 598, 702, 732, 772, 933, 934, 935, 1014, 1450, 1479, 1681, 1816, 2137, 2143]

10 Designs and Matroids

Peter J. Cameron
Michel M. Deza

10.1 Matroids

10.1 A *matroid* is a pair $(E, \mathcal{I})$, where E is a set and $\mathcal{I}$ a nonempty family of subsets of E (*independent sets*) satisfying the conditions:

- if $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$;
- (the *Exchange Axiom*) if $I_1, I_2 \in \mathcal{I}$ and $|I_2| > |I_1|$, then there exists $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

10.2 Examples

1. E is the edge set of a graph G; a set of edges is independent if and only if it is a forest. (Such a matroid is a *graphic matroid*.)
2. E is a set of vectors in a vector space V; a set of vectors is independent if and only if it is linearly independent. (Such a matroid is a *vector matroid*.)
3. E is a set with a family $\mathcal{A} = (A_i : i \in I)$ of subsets; a subset of E is independent if and only if it is a partial transversal of $\mathcal{A}$. (A *transversal matroid*.)

10.3 In a matroid $M = (E, \mathcal{I})$,

- a *basis* is a maximal element of $\mathcal{I}$;
- a *circuit* is a minimal element of $\mathcal{P}(E) \setminus \mathcal{I}$;
- the *rank* $\rho(A)$ of a subset A of E is the maximum cardinality of a member of $\mathcal{I}$ contained in A;
- a *flat* is a subset F of E with the property that, for any $e \in E$, $\rho(F \cup \{e\}) = \rho(F)$ implies $e \in F$;
- a *hyperplane* H is a maximal proper flat of M (a flat with $\rho(H) = \rho(E) - 1$).

10.4 Remarks

1. The Exchange Axiom shows that all bases of a matroid have the same cardinality; more generally, all maximal independent subsets of A have rank $\rho(A)$.
2. Matroids can also be defined and axiomatized in terms of their bases, circuits, rank function, flats, or hyperplanes.

3. The set of flats of a matroid is closed under intersection. Also, if F is a flat and x a point not in F, then there is a flat F' with $F \cup \{x\} \in F'$ and $\rho(F') = \rho(F)+1$.

10.5 A *loop* in a matroid M is an element e such that $\{e\} \notin \mathcal{I}$. Two nonloops e_1, e_2 are *parallel* if $\{e_1, e_2\} \notin \mathcal{I}$. A matroid is *geometric* if it has no loops and no pairs of parallel elements. A geometric matroid is also known as a *combinatorial geometry*.

10.6 Remark From any matroid M, one obtains a geometric matroid (the *geometrization* of M) by deleting loops and identifying parallel elements. The geometrization of a vector space is the corresponding projective space.

10.7 The *truncation* of $M = (E, \mathcal{I})$ to rank r is the matroid on E whose family of independent sets is $\{I \in \mathcal{I} : |I| \le r\}$. Its flats are the flats of M of rank less than r, together with E.

10.8 Example The *free matroid* F_n of rank n is the matroid with $|E| = n$ and $\mathcal{I} = \mathcal{P}(E)$. Its truncation to rank r is the *uniform matroid* $U_{n,r}$.

10.9 Remark For more information on matroids, see [1711, 2128].

10.2 Perfect Matroid Designs

10.10 A *perfect matroid design*, or *PMD*, is a matroid M, of rank r, say, for which there exist integers $f_0, f_1, \ldots, f_r$ such that, for $0 \le i \le r$, any flat of rank i has cardinality f_i. The tuple $(f_0, f_1, \ldots, f_r)$ is the *type* of M.

10.11 Remark If M is a PMD of type $(f_0, f_1, \ldots, f_r)$, then the geometrization of M is a PMD of type $(f'_0, f'_1, \ldots, f'_r)$, where $f'_i = (f_i - f_0)/(f_1 - f_0)$. Hence, $f'_0 = 0$, $f'_1 = 1$.

10.12 Theorem If there exists a PMD of type $(0, 1, f_2, \ldots, f_r)$, then

1. $\displaystyle\prod_{i \le k \le j-1} \frac{f_l - f_k}{f_j - f_k}$ is a nonnegative integer for $0 \le i < j \le l \le r$;
2. $f_i - f_{i-1}$ divides $f_{i+1} - f_i$ for $2 \le i \le r-1$;
3. $(f_i - f_{i-1})^2 \le (f_{i+1} - f_i)(f_{i-1} - f_{i-2})$ for $1 \le i \le r-1$.

10.13 Remark The necessary conditions of Theorem 10.12 are not sufficient; for example, Wilson showed that no PMD of type $(0, 1, 3, 7, 43)$ or $(0, 1, 3, 19, 307)$ exists.

10.14 Examples Not many PMDs are known. All known geometric PMDs are truncations of examples on the following list:

1. Free matroids, with $f_i = i$ for all i.
2. Finite projective spaces over a field $\mathbb{F}_q$, with $f_i = (q^i - 1)/(q - 1)$.
3. Finite affine spaces: the points are the vectors in a vector space of rank r over $\mathbb{F}_q$; the independent sets are those that are affine independent. (The set $\{v_1, \ldots, v_k\}$ is *affine independent* if $\{v_2 - v_1, \ldots, v_k - v_1\}$ is linearly independent.) These have $f_i = q^i$.
4. Steiner systems. (Given a Steiner system $S(t, k, v)$ on the set E, take the independent sets to be all sets of cardinality at most t together with all $(t+1)$-sets not contained in a block. Then the hyperplanes are the blocks of S.) These PMDs have rank $t+1$ and are characterized by the property that $f_i = i$ for $i < t$; also $f_t = k$ and $f_{t+1} = v$.
5. Hall triple systems (§10.3): these have rank 4, $f_2 = 3$, and $f_3 = 9$, and the number of points $|E|$ is a power of 3.

10.15 Remark A *line* (resp. *plane*) in a PMD is a flat of rank 2 (resp. 3). The points and lines of a geometric PMD form a Steiner system $S(2, f_2, f_r)$; the flats form subsystems, so that (for example) any three noncollinear points lie in a unique plane.

10.16 Theorem Let M be a geometric PMD of rank 4.

1. If the planes in M are projective planes (that is, if $f_3 = f_2^2 - f_2 + 1$ with $f_2 > 2$), then M is a truncation of a projective space.
2. If the planes in M are affine planes (that is, if $f_3 = f_2^2$) and if $f_2 > 3$, then M is a truncation of an affine space.

10.17 Remark There is a wide gap between the restrictions imposed by Theorem 10.12 and the known examples. For example, it is not known whether there is a PMD of type $(0, 1, 3, 13, 183)$, $(0, 1, 3, 13, 313)$, or $(0, 1, 3, 15, 183)$.

10.3 Hall Triple Systems and their Algebraic Siblings

10.18 Remark A *triffid* is any PMD of rank 4 with type $(0, 1, 3, 9, 3^n)$. There is an equivalence between those PMDs and each of following structures:

1. *Hall triple system*, Steiner triple system $S(2, 3, 3^n)$ on E, $|E| = 3^n$ such that for any point $a \in E$, there exists an involution that has a as unique fixed point. (See §VI.28.)
2. *Finite exponent 3 commutative Moufang loop* (*exp3-CML*), a finite commutative loop $(L, \cdot)$, such that for any $x, y, z \in L$, $(x \cdot x) \cdot (x \cdot z) = (x \cdot y) \cdot (x \cdot z)$ and $(x \cdot x) \cdot x = 1$ hold.
3. *Distributive Manin quasigroup*, a groupoid $(Q, \circ)$ such that for any $x, y, z \in Q$, $x \circ y = y \circ x$ and $x \circ (x \circ y) = y$ (i.e, any relation $x \circ y = z$ is preserved under permutation of the variables; in particular, $(Q, \circ)$ is a quasigroup) and all translations are automorphisms.
4. *Restricted Fischer pair* (G, F), a group G generated by a subset F, such that $x^2 = 1 = (xy)^3$ and $xyx \in F$ for any $x, y \in F$ and such that the commutative center of G is just $\{1\}$.

10.19 Remark The correspondences among these four definitions are straightforward to check. For example, a distributive Manin quasigroup arises from a Hall triple system by taking $Q = E$ and defining $x \circ y$, for $x \neq y$, being the unique 3rd point of the triple defined by x, y.

10.20 Remark A triffid is a truncation of an affine space over $\mathbb{F}_3$ if and only if corresponding exp3-CML is a group; then the group is Z_3^n. The first (and smallest) example of a nonassociative exp3-CML was given in 1937 by Zassenhaus, by defining, on the set of all 81 $(0, 1, 2)$-sequences $x = (x_1, x_2, x_3, x_4)$, the product as

$$x \cdot y = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4 + (x_3 - y_3)(x_1 y_2 - x_2 y_1))$$

(all sums are modulo 3). The number of nonassociative exp3-CMLs of order 3^n is $1, 1, 3, 12, > 41$ for $n = 4, 5, 6, 7, 8$, respectively.

10.21 Remark The *dimension* $d(L)$ of a exp3-CML L is the smallest number m such that there exist a $(m + 1)$-set generating it; it is usually the dimension of corresponding Steiner triple system. Denote by L_m the *free* exp3-CML of dimension m, that is, any exp3-CML of dimension m is its homeomorphic image. One has $|L_m| = 3^4$, 3^{12}, 3^{49}, 3^{220}, 3^{1028}, 3^{4592} for $m = 3, 4, 5, 6, 7, 8$ [1929]. Moreover, $d(L) \leq \log_3 |L|$, with equality only if L is associative (an abelian 3-group). The number of exp3-CMLs L with $|L| = 3^n$ and $d(L) = 4$ is $1, 1, 1, 1, 4$ for $n = 4, 5, 6, 7, 8$ [184].

10.22 Remark The associative center $Z(L)$ of a exp3-CML L is the abelian 3-group $\{z \in L : (x \cdot y) \cdot z = x \cdot (y \cdot z)\}$. The *central quotient* $L^{(1)} = L/Z(L)$ is again a exp3-CML; define $L^{(i)}$ as $L^{(i-1)}/Z(L^{(i-1)})$. The *nilpotency class* $k(L)$ of L is the smallest number k such that $L^{(k)}$ is associative. Then $k(L) \le d(L)$, with equality for the free loop L_m. All exp3-CMLs L with $k(L) = 2$ are classified in [1279, 1828].

10.23 Remark Infinite exp3-CMLs were connected by Manin with cubic hypersurfaces; see, for example, [185] for recent developments. For connections with differential geometry (3-webs) and topological algebra, see, for example, [1662].

10.4 Designs in PMDs

10.24 Let t, k, v, λ be integers with $0 \le t < k < v$ and $\lambda > 0$. Let M be a PMD of rank v. A t-(v, k, λ) *design in* M is a family $\mathcal{B}$ of k-flats of M with the property that every t-flat in M is contained in exactly λ members of $\mathcal{B}$.

10.25 Remarks

1. A t-(v, k, λ) design in the free matroid F_v is just a t-(v, k, λ) design in the usual sense.
2. A t-(v, k, λ) design in a PMD M is also a s-(v, k, λ_s) design in M for $s < t$, where
$$\lambda_s = \lambda \cdot \prod_{i=s+1}^{t} \frac{f_v - f_s}{f_k - f_s}.$$
3. A t-(v, k, λ) design in a PMD M of type $(f_0, f_1, \ldots, f_v)$ is an ordinary s-design, where $s = \min(t, \max\{i : f_i = i\})$.

10.26 Remark Apart from ordinary t-designs, the only case to have been studied is that of t-designs in projective spaces over $\mathbb{F}_q$. To simplify the notation, let $[n]_q = (q^n - 1)/(q - 1)$, so that the projective space has type $([0]_q, [1]_q, \ldots, [v]_q)$; and define the *gaussian coefficient*
$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{[v-i]_q}{[k-i]_q}$$
to be the number of k-flats. In this case, some theory has been developed. For example, the analogue of the theorem of Ray-Chaudhuri and Wilson (Theorem VI.1.47) holds that in a $2s$-design in M, the number of blocks is at least $\begin{bmatrix} v \\ s \end{bmatrix}_q$.

10.27 Examples

- The first examples were due to Thomas [2029]. They live in $\mathrm{PG}(n, 2)$, where $n+1$ is coprime to 6, blocks are planes, and any line is contained in seven blocks.
- Ray-Chaudhuri and Schram [1779] give a few more constructions.
- A recent investigation appears in [321].

10.28 Remark It is unknown whether the analogue of Teirlinck's theorem holds: Do t-designs (without repeated blocks, and such that not every k-flat is a block) exist for all t?

10.5 Permutation Groups

10.29 A *base* in a permutation group G is a sequence of points whose pointwise stabiliser in G is the identity. A base is *irredundant* if no point is fixed by the stabilizer of its predecessors.

10.30 Remark In general, the bases of a permutation group do not satisfy the matroid basis axioms!

10.31 An *IBIS group* is a permutation group satisfying the following three conditions (shown to be equivalent by Cameron and Fon-Der-Flaass):

- all irredundant bases contain the same number of points;
- the irredundant bases are preserved by reordering;
- the irredundant bases are the bases of a matroid.

The *rank* of an IBIS group is the rank of its associated matroid.

10.32 A permutation group is *base-transitive* if it permutes its ordered bases transitively. Clearly, every base-transitive group is an IBIS group; moreover, the associated matroid is a PMD. Define the *type* of the group to be the type of the PMD. A permutation group is base-transitive if and only if the pointwise stabilizer of any sequence of points is transitive on the points it doesn't fix (if any).

10.33 Remark The base-transitive permutation groups with rank greater than 1 have been classified in [1557] using the classification of finite simple groups (CFSG); the list is too long to give here. An "elementary" (but by no means easy) determination of base-transitive groups of rank at least 7, not using CFSG, was given by Zil'ber [2217].

10.34 Remark A definition of *permutation geometries*, the analogue in the semilattice of subpermutations (partial bijections) of a set, was given by Cameron and Deza. Following the matroid flat axioms, they defined a permutation geometry to be a family $\mathcal{F}$ of subpermutations, closed under intersections, and having the property that if $F \in \mathcal{F}$ and x and y are points with x not in the domain, and y not in the range, of F, there is a unique $F' \in \mathcal{F}$ with rank one greater than the rank of F, extending F and mapping x to y.

A *geometric set* of permutations is a set that consists of the maximal elements in a permutation geometry, and a *geometric group* is a geometric set that forms a group. Now, a geometric group is the same thing as a base-transitive group.

10.35 Theorem Let G be an IBIS group of rank $r > 1$ whose associated matroid is uniform. Then G is $(r-1)$-transitive (and the stabilizer of any r points is the identity).

10.36 Remark For $r = 2$, the groups in the conclusion of this theorem are precisely the *Frobenius groups*; a lot of information about their structure is known (Frobenius, Zassenhaus, Thompson). For $r = 3$, they are the *Zassenhaus groups*; these have been determined (Zassenhaus, Feit, Ito, Suzuki) without the use of CFSG. For $r > 3$, they were determined by Gorenstein and Hughes. In particular, the only ones with $r \geq 5$ are symmetric and alternating groups and the Mathieu group M_{12}.

10.6 Some Generalizations of PMD

10.37 Remark A *matroid design* is a matroid whose hyperplanes form a BIBD, a (b, v, r, k, λ)-configuration on 1-flats. Any PMD is an MD. Any BIBD is a PMD of rank 3 if $\lambda = 1$, but never an MD if $\lambda = 2$. The point-hyperplane design of $\mathrm{PG}(n, q)$ is the unique *symmetric* BIBD with $\lambda > 1$, which is an MD [1252]. Some necessary conditions for a BIBD to be an MD and information on *base designs*, matroids whose bases are the blocks of a BIBD, and *circuit designs*, matroids whose circuits are the blocks of a BIBD, are given in [2128].

10.38 Remark An *equicardinal matroid* is a matroid such that all its hyperplanes have the same cardinality k; they are classified for $|E| - k$ being prime or the square of a prime,

as well as for the case of rank 3 matroids (Kestenband and Young, 1978).

10.39 Remark The following notion generalizes all known PMD of rank 4. A *planar M-space* is a combinatorial geometry of rank 4 such that all its restictions on a 3-flat are isomorphic to the given combinatorial geometry M of rank 3. An example of planar M-space (with at least two 2-flats) having two different 2-flat sizes is known, but only one.

10.40 Remark Brylawski [368] considered *latticially uniform* (or latticially homogeneous) matroids, such that for all i-flats x, all upper intervals $[x, E]$ (or, respectively, all lower intervals $[\emptyset, x]$), in the lattice of the flats) are equal.

10.41 Remark PMDs are the extremal case for the families of k-subsets of given v-set intersecting pairwisely in $l_0, l_1 \ldots, l_t$ elements. It was shown in [698] that for $v > v_0(k)$, such family contains at most $\prod_{0\le i\le t} \frac{v-l_i}{k-l_i}$ sets with equality if and only if it is the hyperplane family of a PMD with type $(l_0, l_1, \ldots, l_t, k, v)$.

See Also

§VI.28	Hall triple systems are perfect matroid designs.
[1711, 2128]	Standard references on matroids.

References Cited: [184, 185, 321, 368, 698, 1252, 1279, 1557, 1662, 1711, 1779, 1828, 1929, 2029, 2128, 2217]

11 Strongly Regular Graphs

Andries E. Brouwer

11.1 Definition and Parameters

11.1 A *strongly regular graph* with parameters (v, k, λ, μ) is a finite graph on v vertices, without loops or multiple edges, regular of degree k (with $0 < k < v - 1$, so that there are both edges and nonedges), and such that any two distinct vertices have λ common neighbors when they are adjacent, and μ common neighbors when they are nonadjacent.

11.2 Remark The complement of a strongly regular graph with parameters (v, k, λ, μ) is again strongly regular, with parameters $(v, v - k - 1, v - 2k + \mu - 2, v - 2k + \lambda)$.

11.3 Proposition The 0–1 adjacency matrix A of a strongly regular graph satisfies the equation $A^2 = kI + \lambda A + \mu(J - I - A)$, where I is the identity matrix and J the all–1 matrix, both of size v.

11.4 Corollary A has eigenvalues k, r, s with multiplicities 1, f, g, where r, s are found as solutions of $x^2 + (\mu - \lambda)x + (\mu - k) = 0$ (assuming $r \ge 0$, $s \le -1$), and f, g are found as solutions of $1 + f + g = v$ and $k + fr + gs = 0$.

11.5 A parameter set (v, k, λ, μ) is *feasible* when v, k, λ, μ are nonnegative integers satisfying $\mu(v - k - 1) = k(k - 1 - \lambda)$, $0 < k < v - 1$, $v - 2k + \mu - 2 \ge 0$, $v - 2k + \lambda \ge 0$, and f, g are nonnegative integers.

11.6 Proposition If (v, k, λ, μ) is feasible, then either r, s are integral, or there is a t such that $v = 4t + 1$, $k = f = g = 2t$, $\lambda = t - 1$, $\mu = t$, and $r, s = (-1 \pm \sqrt{v})/2$ (the *half case*).

11.7 A strongly regular graph Γ is *imprimitive* when either it or its complement is disconnected.

11.8 Remark If a strongly regular graph Γ with parameters (v, k, λ, μ) is disconnected, then it is the disjoint union of complete graphs, so $v = a(k + 1)$, $\lambda = k - 1$, $\mu = 0$, $r = k$, $s = -1$, $f = a - 1$, $g = ak$ (so that the eigenvalue k has multiplicity a). These graphs exist and are uniquely determined given a and k; they are aK_{k+1}. If the complement of Γ is disconnected, then Γ is the complement of aK_m; that is, it is the complete multipartite graph $K_{a\times m}$ with parameters $v = am$, $k = \mu = (a - 1)m$, $\lambda = (a - 2)m$, $r = 0$, $s = -m$, $f = a(m - 1)$, $g = a - 1$.

11.9 Remark Henceforth, Γ is primitive, so that $k > \mu > 0$ and $k > r > 0$.

11.10 Remarks Table 11.12 gives feasible parameter sets for strongly regular graphs on at most 280 vertices. The spectrum, the known constructions, and the known nonexistence results are given. Space limitations have forced the omission of theory and explanations. All information about (semi)partial geometries, gamma and delta spaces, and so on has been omitted.

11.2 Table of Strongly Regular Graphs

11.11 Remarks The first column of Table 11.12 lists information about existence and enumeration; a minus sign "−" means that there is no such graph; a question mark "?" that no such graph is known; a plus sign "+" that there is at least one such graph; an exclamation mark "!" that there is precisely one such graph; a number n, that at least n such graphs are known; and a number n followed by an exclamation mark, that precisely n such graphs exist. Multiplicities are written as exponents. In the comments column, the (or at least some) known constructions are given. It may well happen that several constructions in fact produce the same graph.

Finite fields

Paley(q): For prime powers $q = 4t+1$, the graph with vertex set $\mathbb{F}_q$ where two vertices are adjacent when they differ by a square.

van Lint–Schrijver(u): a graph constructed by the cyclotomic construction in [2087], taking the union of u classes.

Combinatorial

$\binom{n}{2}$ or $T(n)$: the graph on the pairs of an n-set, two pairs being adjacent when they have an element in common. It is the *triangular graph*.

n^2**:** the cartesian product of two complete graphs of size n.

OA(k, n): $(k \geq 3)$ the block graph of an orthogonal array OA(k, n) ($k - 2$ MOLS of order n; see §III.3).

$S(2, k, v)$**:** the block graph of a Steiner system with these parameters (see §II.5). More generally, given a quasi-symmetric design (§VI.48), the graph on the blocks, adjacent when they meet in one of the two possible cardinalities, is strongly regular. Much is known; an old survey is [1674]. From the Witt design $S(5, 8, 24)$, one finds five quasi-symmetric designs: 2-(23,7,21), 2-(22,7,16), 2-(21,7,12), 2-(22,6,5), 2-(21,6,4). Tonchev constructed a quasi-symmetric 2-(45,9,8) design with intersection numbers 1, 3 from the extended binary quadratic residue code of length 48. See also [1151].

Goethals–Seidel(k, r): a graph constructed from a Steiner system $S(2, k, v)$ (with $r = (v-1)/(k-1)$) and a Hadamard matrix of order $r+1$ as in [920]. See also §V.1.

Pasechnik(h): graphs obtained from the tensor product of two nonsymmetric association schemes on h points obtained from a skew Hadamard matrix of order $h+1$; see [1718].

Regular two-graphs

two-graph: the graph belongs to the switching class of a regular two-graph (§VII.13).

two-graph$-*$: the graph with an isolated point added belongs to the switching class of a regular two-graph. (These are usually comments only, but the existence of a two-graph on $v+1$ points implies the existence of a strongly regular graph on v points.)

RSHCD$\pm$: regular two-graphs from regular symmetric Hadamard matrices with constant diagonal (see [348, 920]).

Taylor two-graph for $U_3(q)$: derived from Taylor's regular two-graphs (see [348, 2006, 2007]).

skewhad^2**:** derived from the tensor product of the cores of two skew Hadamard matrices of the same order (see [918]).

Projective graphs

$A_{n-1,2}(q)$ or $\begin{bmatrix} n \\ 2 \end{bmatrix}_q$: the graph on the lines in $\mathrm{PG}(n-1, q)$, adjacent when they have a point in common.

$Bilin_{2\times d}(q)$**:** the graph on the $2 \times d$ matrices over $\mathbb{F}_q$, adjacent when their difference has rank 1.

Polar graphs

$O^{\varepsilon}_{2d}(q)$**:** the graph on the isotropic points on a nondegenerate quadric in $\mathrm{PG}(2d-1, q)$, where two points are joined when the connecting line is totally singular.

$O_{2d+1}(q)$**:** such a graph in $\mathrm{PG}(2d, q)$.

$Sp_{2d}(q)$**:** the graph on the points of $\mathrm{PG}(2d-1, q)$ provided with a nondegenerate symplectic form, where two points are joined when the connecting line is totally isotropic.

$U_d(q)$**:** the graph on the isotropic points of $\mathrm{PG}(d-1, q^2)$ provided with a nondegenerate hermitian form, where two points are joined when the connecting line is totally isotropic.

$NO^{\varepsilon}_{2d}(2)$**:** the graph on the nonisotropic points of $\mathrm{PG}(2d-1, 2)$ provided with a nondegenerate quadratic form, where two points are joined when they are orthogonal (when the connecting line is a tangent).

$NO^{\varepsilon}_{2d}(3)$**:** the graph on one class of nonisotropic points of $\mathrm{PG}(2d-1, 3)$ provided with a nondegenerate quadratic form, where two points are joined when they are orthogonal (when the connecting line is elliptic).

$NO^{\varepsilon}_{2d+1}(q)$**:** the graph on one class of nondegenerate hyperplanes of $\mathrm{PG}(2d, q)$ provided with a nondegenerate quadratic form, where two hyperplanes are joined when their intersection is degenerate.

$NO^{\varepsilon\perp}_{2d+1}(5)$**:** the graph on one class of nonisotropic points of $\mathrm{PG}(2d, 5)$ provided with a nondegenerate quadratic form, where two points are joined when they are orthogonal.

$NU_n(q)$**:** the graph on the nonisotropic points of $\mathrm{PG}(n-1, q)$ provided with a nondegenerate hermitian form, where two points are joined when the connecting line is a tangent.

Affine polar graphs

$VO^{\varepsilon}_{2d}(q)$**:** the graph on the vectors of a vector space of dimension $2d$ over $\mathbb{F}_q$ provided with a nondegenerate quadratic form Q, where two vectors u and v are joined when $Q(v-u) = 0$.

$VNO^{\varepsilon}_{2d}(q)$**:** ($q$ odd) the graph on the vectors of a vector space of dimension $2d$ over $\mathbb{F}_q$ provided with a nondegenerate quadratic form Q, where two vectors u and v are joined when $Q(v-u)$ is a nonzero square.

Affine difference sets

Let V be an n-dimensional vector space over $\mathbb{F}_q$ and let X be a set of directions (a subset of the projective space PV). Two vectors are *adjacent* when the line joining them has a direction in X. Then $v = q^n$ and $k = (q-1)|X|$. This graph is strongly regular if and only if there are two integers w_1, w_2 such that all hyperplanes of PV miss either w_1 or w_2 points of X. If this is the case, then $r = k - qw_1$, $s = k - qw_2$ (assuming $w_1 < w_2$), and hence $\mu = k + (k - qw_1)(k - qw_2)$, $\lambda = k - 1 + (k - qw_1 + 1)(k - qw_2 + 1)$. On the other hand, one can view X as the set of columns of the generator matrix of a code, and then the requirement that hyperplanes meet X in one of two cardinalities translates into the requirement that one has a 2-weight code. Thus, projective 2-weight codes, projective sets that have two intersection sizes with hyperplanes, and strongly regular graphs defined by a multiplication invariant difference set on a vector space are equivalent objects. These observations are due to Delsarte [672]. For an extensive discussion, see [412]. One more infinite family is given in [342]. There are many sporadic examples—a full discussion is omitted for reasons of space. All constructions "from a Baer subplane", "from a hyperoval", "from a partial spread", and so on, refer to this situation, and specify the set X.

Geometric

GQ(s,t): (the collinearity graph of) a generalized quadrangle with $s+1$ points on each line, and $t+1$ lines on each point. See §VI.23 and [1723].

Haemers(q): the graph constructed from a GQ$(q+1, q-1)$ as described in [348, §8A].

Nonexistence: The Half Case and Conference Matrices

Conf: In the Half Case (parameters $(v,k,\lambda,\mu) = (4t+1, 2t, t-1, t)$ for some integer t), a strongly regular graph exists if and only if a conference matrix C of order $v+1$ exists. Thus, v must be a sum of two squares. See §V.6.

Nonexistence: The Krein Conditions A strongly regular graph carries a two-class association scheme, and the standard theory of association schemes applies. In particular, the Krein parameters q^k_{ij} are nonnegative (see [673, 1096, 1361, 1859]). See also §VI.1. Expressed in the parameters, this condition becomes

Krein$_1$**:** $(r+1)(k+r+2rs) \le (k+r)(s+1)^2$.

Krein$_2$**:** $(s+1)(k+s+2rs) \le (k+s)(r+1)^2$.

Nonexistence: The Absolute Bound One has $v \le \frac{1}{2}f(f+3)$ and even $v \le \frac{1}{2}f(f+1)$ if $q^1_{11} \neq 0$ (see [676, 1322, 1672, 1872]). This condition is noted by "Abs".

$\mu = 1$**:** If $\mu = 1$, then the set of neighbors of a point is a union of $(\lambda+1)$-cliques, so that $(\lambda+1)|k$. The total number of $(\lambda+2)$-cliques equals $vk/(\lambda+1)(\lambda+2)$ which must be an integer.

11.12 Table Strongly Regular Graphs on at most 280 vertices.

∃	v	k	λ	μ	r^f	s^g	Comments
!	5	2	0	1	0.618^2	-1.618^2	pentagon; Paley(5); Seidel 2-graph$-*$
!	9	4	1	2	1^4	-2^4	Paley(9); 3^2; 2-graph$-*$
!	10	3	0	1	1^5	-2^4	Petersen graph [1730]; $NO_4^-(2)$; $NO_3^{-\perp}(5)$; switch $OA(3,2)+*$; 2-graph
	6	3	4		1^4	-2^5	$\binom{5}{2}$; 2-graph
!	13	6	2	3	1.303^6	-2.303^6	Paley(13); 2-graph$-*$

∃	v	k	λ	μ	r^f	s^g	Comments
!	15	6	1	3	1^9	-3^5	$O_5(2)$ polar graph; $Sp_4(2)$ polar graph; $NO_4^-(3)$; 2-graph$-*$
		8	4	4	2^5	-2^9	$\binom{6}{2}$; 2-graph$-*$
!	16	5	0	2	1^{10}	-3^5	$q_{22}^2 = 0$; van Lint–Schrijver(1); $VO_4^-(2)$ affine polar graph; projective binary [5,4] code with weights 2, 4; $RSHCD-$; 2-graph
		10	6	6	2^5	-2^{10}	Clebsch graph [515, 610, 512, 1870]; $q_{11}^1 = 0$; van Lint–Schrijver(2); 2-graph
2!	16	6	2	2	2^6	-2^9	Shrikhande graph [1902]; 4^2; from a partial spread: projective binary [6,4] code with weights 2, 4; $RSHCD+$; 2-graph
		9	4	6	1^9	-3^6	OA(4,3); $\mathrm{Bilin}_{2\times 2}(2)$; Goethals–Seidel(2,3); $VO_4^+(2)$ affine polar graph; 2-graph
!	17	8	3	4	1.562^8	-2.562^8	Paley(17); 2-graph$-*$
!	21	10	3	6	1^{14}	-4^6	
		10	5	4	3^6	-2^{14}	$\binom{7}{2}$
−	21	10	4	5	1.791^{10}	-2.791^{10}	Conf
!	25	8	3	2	3^8	-2^{16}	5^2
		16	9	12	1^{16}	-4^8	OA(5,4)
15!	25	12	5	6	2^{12}	-3^{12}	complete enumeration by Paulus [1719]; Paley(25); OA(5,3); 2-graph$-*$
10!	26	10	3	4	2^{13}	-3^{12}	complete enumeration by Paulus [1719]; switch $OA(5,3)+*$; 2-graph
		15	8	9	2^{12}	-3^{13}	S(2,3,13); 2-graph
!	27	10	1	5	1^{20}	-5^6	$q_{22}^2 = 0$; $O_6^-(2)$ polar graph; $GQ(2,4)$; 2-graph$-*$
		16	10	8	4^6	-2^{20}	Schläfli graph; unique by Seidel [1870]; $q_{11}^1 = 0$; 2-graph$-*$
−	28	9	0	4	1^{21}	-5^6	Krein_2; Abs
		18	12	10	4^6	-2^{21}	Krein_1; Abs
4!	28	12	6	4	4^7	-2^{20}	Chang graphs [450]; $\binom{8}{2}$; 2-graph
		15	6	10	1^{20}	-5^7	$NO_6^+(2)$; Goethals–Seidel(3,3); Taylor 2-graph for $U_3(3)$
41!	29	14	6	7	2.193^{14}	-3.193^{14}	complete enumeration by Bussemaker & Spence [personal comm.]; Paley(29); 2-graph$-*$
−	33	16	7	8	2.372^{16}	-3.372^{16}	Conf
3854!	35	16	6	8	2^{20}	-4^{14}	complete enumeration by McKay & Spence [1577]; 2-graph$-*$
		18	9	9	3^{14}	-3^{20}	S(2,3,15); $A_{3,2}(2)$; $O_6^+(2)$ polar graph; 2-graph$-*$
!	36	10	4	2	4^{10}	-2^{25}	6^2
		25	16	20	1^{25}	-5^{10}	
180!	36	14	4	6	2^{21}	-4^{14}	$U_3(3).2/L_2(7).2$ - subconstituent of Hall–Janko graph; complete enumeration by McKay & Spence [1577]; $RSHCD-$; 2-graph
		21	12	12	3^{14}	-3^{21}	2-graph
!	36	14	7	4	5^8	-2^{27}	$\binom{9}{2}$
		21	10	15	1^{27}	-6^8	
32548!	36	15	6	6	3^{15}	-3^{20}	complete enumeration by McKay & Spence [1577]; OA(6,3); $NO_6^-(2)$; $RSHCD+$; 2-graph
		20	10	12	2^{20}	-4^{15}	$NO_5^-(3)$; 2-graph
+	37	18	8	9	2.541^{18}	-3.541^{18}	Paley(37); 2-graph$-*$
28!	40	12	2	4	2^{24}	-4^{15}	complete enumeration by Spence [1947]; $O_5(3)$ polar graph; $Sp_4(3)$ polar graph
		27	18	18	3^{15}	-3^{24}	$NU(4,2)$
+	41	20	9	10	2.702^{20}	-3.702^{20}	Paley(41); 2-graph$-*$
78!	45	12	3	3	3^{20}	-3^{24}	complete enumeration by Coolsaet, Degraer, & Spence [605]; $U_4(2)$ polar graph
		32	22	24	2^{24}	-4^{20}	$NO_5^+(3)$
!	45	16	8	4	6^9	-2^{35}	$\binom{10}{2}$
		28	15	21	1^{35}	-7^9	
+	45	22	10	11	2.854^{22}	-3.854^{22}	Mathon [1535]; 2-graph$-*$
!	49	12	5	2	5^{12}	-2^{36}	7^2
		36	25	30	1^{36}	-6^{12}	OA(7,6)

∃	v	k	λ	μ	r^f	s^g	Comments
−	49	16	3	6	2^{32}	-5^{16}	Bussemaker, Haemers, Mathon, & Wilbrink [403]
		32	21	20	4^{16}	-3^{32}	
+	49	18	7	6	4^{18}	-3^{30}	OA(7,3); Pasechnik(7)
		30	17	20	2^{30}	-5^{18}	OA(7,5)
+	49	24	11	12	3^{24}	-4^{24}	Paley(49); OA(7,4); 2-graph$-*$
!	50	7	0	1	2^{28}	-3^{21}	Hoffman–Singleton graph [1116]; $U_3(5^2).2$/Sym(7)
		42	35	36	2^{21}	-3^{28}	
−	50	21	4	12	1^{42}	-9^{7}	Abs
		28	18	12	8^{7}	-2^{42}	Abs
+	50	21	8	9	3^{25}	-4^{24}	switch $OA(7,4)+*$; switch skewhad$^2+*$; 2-graph
		28	15	16	3^{24}	-4^{25}	S(2,4,25); 2-graph
+	53	26	12	13	3.140^{26}	-4.140^{26}	Paley(53); 2-graph$-*$
!	55	18	9	4	7^{10}	-2^{44}	$\binom{11}{2}$
		36	21	28	1^{44}	-8^{10}	
!	56	10	0	2	2^{35}	-4^{20}	Sims–Gewirtz graph [893, 894, 346]; $L_3(4).2^2$/Alt(6).2^2
		45	36	36	3^{20}	-3^{35}	Witt: intersection 2 graph of a 2-(21,6,4) design with block intersections 0, 2
−	56	22	3	12	1^{48}	-10^{7}	Krein$_2$; Abs
		33	22	15	9^{7}	-2^{48}	Krein$_1$; Abs
−	57	14	1	4	2^{38}	-5^{18}	Wilbrink–Brouwer [2140]
		42	31	30	4^{18}	-3^{38}	
+	57	24	11	9	5^{18}	-3^{38}	S(2,3,19)
		32	16	20	2^{38}	-6^{18}	
−	57	28	13	14	3.275^{28}	-4.275^{28}	Conf
+	61	30	14	15	3.405^{30}	-4.405^{30}	Paley(61); 2-graph$-*$
−	63	22	1	11	1^{55}	-11^{7}	Krein$_2$; Abs
		40	28	20	10^{7}	-2^{55}	Krein$_1$; Abs
+	63	30	13	15	3^{35}	-5^{27}	$O_7(2)$ polar graph; $Sp_6(2)$ polar graph; 2-graph$-*$
		32	16	16	4^{27}	-4^{35}	S(2,4,28); $NU(3,3)$; 2-graph$-*$
!	64	14	6	2	6^{14}	-2^{49}	8^2; from a partial spread of 3-spaces: projective binary [14,6] code with weights 4, 8
		49	36	42	1^{49}	-7^{14}	OA(8,7)
167!	64	18	2	6	2^{45}	-6^{18}	complete enumeration by Haemers & Spence [1008]; $GQ(3,5)$; from a hyperoval: projective 4-ary [6,3] code with weights 4, 6
		45	32	30	5^{18}	-3^{45}	
−	64	21	0	10	1^{56}	-11^{7}	Krein$_2$; Abs
		42	30	22	10^{7}	-2^{56}	Krein$_1$; Abs
+	64	21	8	6	5^{21}	-3^{42}	OA(8,3); Bilin$_{2\times 3}$(2); from a Baer subplane: projective 4-ary [7,3] code with weights 4, 6; Brouwer [342]; from a partial spread of 3-spaces: projective binary [21,6] code with weights 8, 12
		42	26	30	2^{42}	-6^{21}	OA(8,6)
+	64	27	10	12	3^{36}	-5^{27}	from a unital: projective 4-ary [9,3] code with weights 6, 8; $VO_6^-(2)$ affine polar graph; $RSHCD-$; 2-graph
		36	20	20	4^{27}	-4^{36}	2-graph
+	64	28	12	12	4^{28}	-4^{35}	OA(8,4); from a partial spread of 3-spaces: projective binary [28,6] code with weights 12, 16; $RSHCD+$; 2-graph
		35	18	20	3^{35}	-5^{28}	OA(8,5); Goethals–Seidel(2,7); $VO_6^+(2)$ affine polar graph; 2-graph
−	64	30	18	10	10^{8}	-2^{55}	Abs
		33	12	22	1^{55}	-11^{8}	Abs
?	65	32	15	16	3.531^{32}	-4.531^{32}	2-graph$-*$?
!	66	20	10	4	8^{11}	-2^{54}	$\binom{12}{2}$
		45	28	36	1^{54}	-9^{11}	
?	69	20	7	5	5^{23}	-3^{45}	
		48	32	36	2^{45}	-6^{23}	S(2,6,46)?
−	69	34	16	17	3.653^{34}	-4.653^{34}	Conf
+	70	27	12	9	6^{20}	-3^{49}	S(2,3,21)
		42	23	28	2^{49}	-7^{20}	
+	73	36	17	18	3.772^{36}	-4.772^{36}	Paley(73); 2-graph$-*$

∃	v	k	λ	μ	r^f	s^g	Comments
?	75	32	10	16	2^{56}	-8^{18}	2-graph$-*$?
		42	25	21	7^{18}	-3^{56}	2-graph$-*$?
−	76	21	2	7	2^{56}	-7^{19}	Haemers [1007]
		54	39	36	6^{19}	-3^{56}	
?	76	30	8	14	2^{57}	-8^{18}	2-graph?
		45	28	24	7^{18}	-3^{57}	2-graph?
?	76	35	18	14	7^{19}	-3^{56}	2-graph?
		40	18	24	2^{56}	-8^{19}	2-graph?
!	77	16	0	4	2^{55}	-6^{21}	S(3,6,22); $M_{22}.2/2^4$: Sym(6); unique by Brouwer [340]; subconstituent of Higman–Sims graph
		60	47	45	5^{21}	-3^{55}	Witt 3-(22,6,1): intersection 2 graph of a 2-(22,6,5) design with block intersections 0, 2
−	77	38	18	19	3.887^{38}	-4.887^{38}	Conf
!	78	22	11	4	9^{12}	-2^{65}	$\binom{13}{2}$
		55	36	45	1^{65}	-10^{12}	
!	81	16	7	2	7^{16}	-2^{64}	9^2; Brouwer [342]; from a partial spread: projective ternary [8,4] code with weights 3, 6
		64	49	56	1^{64}	-8^{16}	OA(9,8)
!	81	20	1	6	2^{60}	-7^{20}	unique by Brouwer & Haemers [345]; $VO_4^-(3)$ affine polar graph; projective ternary [10,4] code with weights 6, 9
		60	45	42	6^{20}	-3^{60}	
+	81	24	9	6	6^{24}	-3^{56}	OA(9,3); $VNO_4^+(3)$ affine polar graph; from a partial spread: projective ternary [12,4] code with weights 6, 9
		56	37	42	2^{56}	-7^{24}	OA(9,7)
+	81	30	9	12	3^{50}	-6^{30}	$VNO_4^-(3)$ affine polar graph; Hamada–Helleseth [1024]: projective ternary [15,4] code with weights 9, 12
		50	31	30	5^{30}	-4^{50}	
+	81	32	13	12	5^{32}	-4^{48}	OA(9,4); $\mathrm{Bilin}_{2\times 2}(3)$; $VO_4^+(3)$ affine polar graph; from a partial spread: projective ternary [16,4] code with weights 9, 12
		48	27	30	3^{48}	-6^{32}	OA(9,6)
−	81	40	13	26	1^{72}	-14^8	Abs
		40	25	14	13^8	-2^{72}	Abs
+	81	40	19	20	4^{40}	-5^{40}	Paley(81); OA(9,5); projective ternary [20,4] code with weights 12, 15; 2-graph$-*$
+	82	36	15	16	4^{41}	-5^{40}	switch $OA(9,5)+*$; 2-graph
		45	24	25	4^{40}	-5^{41}	S(2,5,41); 2-graph
?	85	14	3	2	4^{34}	-3^{50}	
		70	57	60	2^{50}	-5^{34}	
+	85	20	3	5	3^{50}	-5^{34}	$O_5(4)$ polar graph; $Sp_4(4)$ polar graph
		64	48	48	4^{34}	-4^{50}	
?	85	30	11	10	5^{34}	-4^{50}	
		54	33	36	3^{50}	-6^{34}	S(2,6,51)?
?	85	42	20	21	4.110^{42}	-5.110^{42}	2-graph$-*$?
?	88	27	6	9	3^{55}	-6^{32}	
		60	41	40	5^{32}	-4^{55}	
+	89	44	21	22	4.217^{44}	-5.217^{44}	Paley(89); 2-graph$-*$
!	91	24	12	4	10^{13}	-2^{77}	$\binom{14}{2}$
		66	45	55	1^{77}	-11^{13}	
−	93	46	22	23	4.322^{46}	-5.322^{46}	Conf
?	95	40	12	20	2^{75}	-10^{19}	2-graph$-*$?
		54	33	27	9^{19}	-3^{75}	2-graph$-*$?
+	96	19	2	4	3^{57}	-5^{38}	Haemers(4)
		76	60	60	4^{38}	-4^{57}	
+	96	20	4	4	4^{45}	-4^{50}	$GQ(5,3)$
		75	58	60	3^{50}	-5^{45}	
?	96	35	10	14	3^{63}	-7^{32}	
		60	38	36	6^{32}	-4^{63}	
?	96	38	10	18	2^{76}	-10^{19}	2-graph?
		57	36	30	9^{19}	-3^{76}	2-graph?

∃	v	k	λ	μ	r^f	s^g	Comments
?	96	45	24	18	9^{20}	-3^{75}	2-graph?
		50	22	30	2^{75}	-10^{20}	2-graph?
+	97	48	23	24	4.424^{48}	-5.424^{48}	Paley(97); 2-graph$-*$
?	99	14	1	2	3^{54}	-4^{44}	
		84	71	72	3^{44}	-4^{54}	
?	99	42	21	15	9^{21}	-3^{77}	
		56	28	36	2^{77}	-10^{21}	
+	99	48	22	24	4^{54}	-6^{44}	2-graph$-*$
		50	25	25	5^{44}	-5^{54}	S(2,5,45); 2-graph$-*$
!	100	18	8	2	8^{18}	-2^{81}	10^2
		81	64	72	1^{81}	-9^{18}	
!	100	22	0	6	2^{77}	-8^{22}	Higman–Sims graph [1098]; $HS.2/M_{22}.2$; unique by Gewirtz [893]; $q^2_{22}=0$
		77	60	56	7^{22}	-3^{77}	$q^1_{11}=0$
+	100	27	10	6	7^{27}	-3^{72}	OA(10,3)
		72	50	56	2^{72}	-8^{27}	OA(10,8)?
?	100	33	8	12	3^{66}	-7^{33}	
		66	44	42	6^{33}	-4^{66}	
+	100	33	14	9	8^{24}	-3^{75}	S(2,3,25)
		66	41	48	2^{75}	-9^{24}	
−	100	33	18	7	13^{11}	-2^{88}	Abs
		66	39	52	1^{88}	-14^{11}	Abs
+	100	36	14	12	6^{36}	-4^{63}	Hall–Janko graph; $J_2.2/U_3(3).2$; subconstituent of $G_2(4)$ graph; OA(10,4)
		63	38	42	3^{63}	-7^{36}	OA(10,7)?
+	100	44	18	20	4^{55}	-6^{44}	Jørgensen–Klin graph [1217]; $RSHCD-$; 2-graph
		55	30	30	5^{44}	-5^{55}	2-graph
+	100	45	20	20	5^{45}	-5^{54}	OA(10,5)?; $RSHCD+$; 2-graph
		54	28	30	4^{54}	-6^{45}	OA(10,6)?; 2-graph
+	101	50	24	25	4.525^{50}	-5.525^{50}	Paley(101); 2-graph$-*$
!	105	26	13	4	11^{14}	-2^{90}	$\binom{15}{2}$
		78	55	66	1^{90}	-12^{14}	
!	105	32	4	12	2^{84}	-10^{20}	Aut$L_3(4)$ on flags (rk 4) [Goethals & Seidel], unique by Coolsaet & Degraer [604]
		72	51	45	9^{20}	-3^{84}	
?	105	40	15	15	5^{48}	-5^{56}	
		64	38	40	4^{56}	-6^{48}	
?	105	52	21	30	2^{84}	-11^{20}	
		52	29	22	10^{20}	-3^{84}	
−	105	52	25	26	4.623^{52}	-5.623^{52}	Conf
+	109	54	26	27	4.720^{54}	-5.720^{54}	Paley(109); 2-graph$-*$
?	111	30	5	9	3^{74}	-7^{36}	
		80	58	56	6^{36}	-4^{74}	
+	111	44	19	16	7^{36}	-4^{74}	S(2,4,37)
		66	37	42	3^{74}	-8^{36}	
!	112	30	2	10	2^{90}	-10^{21}	unique by Cameron, Goethals, & Seidel [420]; subconstituent of McLaughlin graph; $q^2_{22}=0$; $O_6^-(3)$ polar graph
		81	60	54	9^{21}	-3^{90}	$q^1_{11}=0$
?	112	36	10	12	4^{63}	-6^{48}	
		75	50	50	5^{48}	-5^{63}	
+	113	56	27	28	4.815^{56}	-5.815^{56}	Paley(113); 2-graph$-*$
?	115	18	1	3	3^{69}	-5^{45}	
		96	80	80	4^{45}	-4^{69}	
+	117	36	15	9	9^{26}	-3^{90}	Wallis; S(2,3,27); $NO_3^+(3)$; Lines in $AG(3,3)$ (rk 4)
		80	52	60	2^{90}	-10^{26}	
?	117	58	28	29	4.908^{58}	-5.908^{58}	2-graph$-*$?
+	119	54	21	27	3^{84}	-9^{34}	$O_8^-(2)$ polar graph; 2-graph$-*$
		64	36	32	8^{34}	-4^{84}	2-graph$-*$
!	120	28	14	4	12^{15}	-2^{104}	$\binom{16}{2}$
		91	66	78	1^{104}	-13^{15}	
?	120	34	8	10	4^{68}	-6^{51}	
		85	60	60	5^{51}	-5^{68}	

∃	v	k	λ	μ	r^f	s^g	Comments
?	120	35	10	10	5^{56}	-5^{63}	
		84	58	60	4^{63}	-6^{56}	
!	120	42	8	18	2^{99}	-12^{20}	$L_3(4)$ on Baer subplanes (rk 5), unique by Coolsaet & Degraer [604]
		77	52	44	11^{20}	-3^{99}	Witt: intersection 3 graph of a 2-(21,7,12) design with block intersections 1, 3
+	120	51	18	24	3^{85}	-9^{34}	$NO_5^-(4)$; 2-graph
		68	40	36	8^{34}	-4^{85}	2-graph
+	120	56	28	24	8^{35}	-4^{84}	2-graph
		63	30	36	3^{84}	-9^{35}	dist. 2 in J(10,3) - Mathon; $NO_8^+(2)$; Goethals–Seidel(3,7); 2-graph
!	121	20	9	2	9^{20}	-2^{100}	11^2
		100	81	90	1^{100}	-10^{20}	OA(11,10)
+	121	30	11	6	8^{30}	-3^{90}	OA(11,3)
		90	65	72	2^{90}	-9^{30}	OA(11,9)
?	121	36	7	12	3^{84}	-8^{36}	
		84	59	56	7^{36}	-4^{84}	
+	121	40	15	12	7^{40}	-4^{80}	OA(11,4)
		80	51	56	3^{80}	-8^{40}	OA(11,8)
?	121	48	17	20	4^{72}	-7^{48}	
		72	43	42	6^{48}	-5^{72}	
+	121	50	21	20	6^{50}	-5^{70}	OA(11,5); Pasechnik(11)
		70	39	42	4^{70}	-7^{50}	OA(11,7)
−	121	56	15	35	1^{112}	-21^8	Abs
		64	42	24	20^8	-2^{112}	Abs
+	121	60	29	30	5^{60}	-6^{60}	Paley(121); $q_{11}^1=0$; OA(11,6); 2-graph$-*$
+	122	55	24	25	5^{61}	-6^{60}	switch $OA(11,6)+*$; switch skewhad$^2+*$; 2-graph
		66	35	36	5^{60}	-6^{61}	S(2,6,61)?; 2-graph
+	125	28	3	7	3^{84}	-7^{40}	$GQ(4,6)$
		96	74	72	6^{40}	-4^{84}	
−	125	48	28	12	18^{10}	-2^{114}	Abs
		76	39	57	1^{114}	-19^{10}	Abs
+	125	52	15	26	2^{104}	-13^{20}	2-graph$-*$
		72	45	36	12^{20}	-3^{104}	2-graph$-*$
+	125	62	30	31	5.090^{62}	-6.090^{62}	Paley(125); 2-graph$-*$
+	126	25	8	4	7^{35}	-3^{90}	dist. 1 or 4 in J(9,4) - Mathon, Buekenhout & Hubaut
		100	78	84	2^{90}	-8^{35}	
+	126	45	12	18	3^{90}	-9^{35}	$NO_6^-(3)$
		80	52	48	8^{35}	-4^{90}	
+	126	50	13	24	2^{105}	-13^{20}	Goethals; 2-graph
		75	48	39	12^{20}	-3^{105}	2-graph
+	126	60	33	24	12^{21}	-3^{104}	2-graph
		65	28	39	2^{104}	-13^{21}	Taylor 2-graph for $U_3(5)$
−	129	64	31	32	5.179^{64}	-6.179^{64}	Conf
+	130	48	20	16	8^{39}	-4^{90}	S(2,4,40); $A_{3,2}(3)$; $O_6^+(3)$ polar graph
		81	48	54	3^{90}	-9^{39}	
?	133	24	5	4	5^{56}	-4^{76}	
		108	87	90	3^{76}	-6^{56}	
?	133	32	6	8	4^{76}	-6^{56}	
		100	75	75	5^{56}	-5^{76}	
?	133	44	15	14	6^{56}	-5^{76}	
		88	57	60	4^{76}	-7^{56}	
−	133	66	32	33	5.266^{66}	-6.266^{66}	Conf
+	135	64	28	32	4^{84}	-8^{50}	2-graph$-*$
		70	37	35	7^{50}	-5^{84}	$O_8^+(2)$ polar graph; 2-graph$-*$
?	136	30	8	6	6^{51}	-4^{84}	
		105	80	84	3^{84}	-7^{51}	
!	136	30	15	4	13^{16}	-2^{119}	$\binom{17}{2}$
		105	78	91	1^{119}	-14^{16}	
+	136	60	24	28	4^{85}	-8^{50}	2-graph
		75	42	40	7^{50}	-5^{85}	$NO_5^+(4)$; 2-graph
+	136	63	30	28	7^{51}	-5^{84}	$NO_8^-(2)$; 2-graph
		72	36	40	4^{84}	-8^{51}	2-graph

∃	v	k	λ	μ	r^f	s^g	Comments
+	137	68	33	34	5.352^{68}	-6.352^{68}	Paley(137); 2-graph$-*$
−	141	70	34	35	5.437^{70}	-6.437^{70}	Conf
+	143	70	33	35	5^{77}	-7^{65}	2-graph$-*$
		72	36	36	6^{65}	-6^{77}	S(2,6,66); 2-graph$-*$
!	144	22	10	2	10^{22}	-2^{121}	12^2
		121	100	110	1^{121}	-11^{22}	OA(12,11)?
+	144	33	12	6	9^{33}	-3^{110}	OA(12,3)
		110	82	90	2^{110}	-10^{33}	OA(12,10)?
+	144	39	6	12	3^{104}	-9^{39}	$L_3(3)$ (rk 8)
		104	76	72	8^{39}	-4^{104}	
+	144	44	16	12	8^{44}	-4^{99}	OA(12,4)
		99	66	72	3^{99}	-9^{44}	OA(12,9)?
?	144	52	16	20	4^{91}	-8^{52}	
		91	58	56	7^{52}	-5^{91}	
+	144	55	22	20	7^{55}	-5^{88}	OA(12,5)
		88	52	56	4^{88}	-8^{55}	OA(12,8)?
−	144	65	16	40	1^{135}	-25^{8}	Krein_2; Abs
		78	52	30	24^{8}	-2^{135}	Krein_1; Abs
+	144	65	28	30	5^{78}	-7^{65}	$RSHCD-$; 2-graph
		78	42	42	6^{65}	-6^{78}	2-graph
+	144	66	30	30	6^{66}	-6^{77}	OA(12,6); $RSHCD+$; 2-graph
		77	40	42	5^{77}	-7^{66}	OA(12,7); Goethals–Seidel(2,11); 2-graph
?	145	72	35	36	5.521^{72}	-6.521^{72}	2-graph$-*$?
?	147	66	25	33	3^{110}	-11^{36}	2-graph$-*$?
		80	46	40	10^{36}	-4^{110}	2-graph$-*$?
?	148	63	22	30	3^{111}	-11^{36}	2-graph?
		84	50	44	10^{36}	-4^{111}	2-graph?
?	148	70	36	30	10^{37}	-4^{110}	2-graph?
		77	36	44	3^{110}	-11^{37}	2-graph?
+	149	74	36	37	5.603^{74}	-6.603^{74}	Paley(149); 2-graph$-*$
!	153	32	16	4	14^{17}	-2^{135}	$\binom{18}{2}$
		120	91	105	1^{135}	-15^{17}	
?	153	56	19	21	5^{84}	-7^{68}	
		96	60	60	6^{68}	-6^{84}	
?	153	76	37	38	5.685^{76}	-6.685^{76}	2-graph$-*$?
?	154	48	12	16	4^{98}	-8^{55}	
		105	72	70	7^{55}	-5^{98}	
−	154	51	8	21	2^{132}	-15^{21}	Krein_2
		102	71	60	14^{21}	-3^{132}	Krein_1
?	154	72	26	40	2^{132}	-16^{21}	
		81	48	36	15^{21}	-3^{132}	
+	155	42	17	9	11^{30}	-3^{124}	S(2,3,31); $A_{4,2}(2)$
		112	78	88	2^{124}	-12^{30}	
+	156	30	4	6	4^{90}	-6^{65}	$O_5(5)$ polar graph; $Sp_4(5)$ polar graph
		125	100	100	5^{65}	-5^{90}	
+	157	78	38	39	5.765^{78}	-6.765^{78}	Paley(157); 2-graph$-*$
?	160	54	18	18	6^{75}	-6^{84}	
		105	68	70	5^{84}	-7^{75}	
−	161	80	39	40	5.844^{80}	-6.844^{80}	Conf
?	162	21	0	3	3^{105}	-6^{56}	
		140	121	120	5^{56}	-4^{105}	
?	162	23	4	3	5^{69}	-4^{92}	
		138	117	120	3^{92}	-6^{69}	
?	162	49	16	14	7^{63}	-5^{98}	
		112	76	80	4^{98}	-8^{63}	
!	162	56	10	24	2^{140}	-16^{21}	$q^2_{22} = 0$
		105	72	60	15^{21}	-3^{140}	$U_4(3)/L_3(4)$; unique by Cameron, Goethals, & Seidel [420]; subconstituent of McLaughlin graph; $q^1_{11} = 0$
?	162	69	36	24	15^{23}	-3^{138}	
		92	46	60	2^{138}	-16^{23}	
+	165	36	3	9	3^{120}	-9^{44}	$U_5(2)$ polar graph
		128	100	96	8^{44}	-4^{120}	
−	165	82	40	41	5.923^{82}	-6.923^{82}	Conf

∃	v	k	λ	μ	r^f	s^g	Comments
!	169	24	11	2	11^{24}	-2^{144}	13^2
		144	121	132	1^{144}	-12^{24}	OA(13,12)
+	169	36	13	6	10^{36}	-3^{132}	OA(13,3)
		132	101	110	2^{132}	-11^{36}	OA(13,11)
?	169	42	5	12	3^{126}	-10^{42}	
		126	95	90	9^{42}	-4^{126}	
+	169	48	17	12	9^{48}	-4^{120}	OA(13,4)
		120	83	90	3^{120}	-10^{48}	OA(13,10)
?	169	56	15	20	4^{112}	-9^{56}	
		112	75	72	8^{56}	-5^{112}	
+	169	60	23	20	8^{60}	-5^{108}	OA(13,5)
		108	67	72	4^{108}	-9^{60}	OA(13,9)
?	169	70	27	30	5^{98}	-8^{70}	
		98	57	56	7^{70}	-6^{98}	
+	169	72	31	30	7^{72}	-6^{96}	OA(13,6)
		96	53	56	5^{96}	-8^{72}	OA(13,8)
+	169	84	41	42	6^{84}	-7^{84}	Paley(169); OA(13,7); 2-graph$-*$
+	170	78	35	36	6^{85}	-7^{84}	switch $OA(13,7)+*$; 2-graph
		91	48	49	6^{84}	-7^{85}	S(2,7,85)?; 2-graph
!	171	34	17	4	15^{18}	-2^{152}	$\binom{19}{2}$
		136	105	120	1^{152}	-16^{18}	
?	171	50	13	15	5^{95}	-7^{75}	
		120	84	84	6^{75}	-6^{95}	
?	171	60	15	24	3^{132}	-12^{38}	
		110	73	66	11^{38}	-4^{132}	
+	173	86	42	43	6.076^{86}	-7.076^{86}	Paley(173); 2-graph$-*$
+	175	30	5	5	5^{84}	-5^{90}	$GQ(6,4)$
		144	118	120	4^{90}	-6^{84}	
?	175	66	29	22	11^{42}	-4^{132}	
		108	63	72	3^{132}	-12^{42}	
+	175	72	20	36	2^{153}	-18^{21}	edges of Hoffman–Singleton graph; 2-graph$-*$
		102	65	51	17^{21}	-3^{153}	2-graph$-*$
?	176	25	0	4	3^{120}	-7^{55}	
		150	128	126	6^{55}	-4^{120}	
+	176	40	12	8	8^{55}	-4^{120}	
		135	102	108	3^{120}	-9^{55}	$NU(5,2)$
+	176	45	18	9	12^{32}	-3^{143}	S(2,3,33)
		130	93	104	2^{143}	-13^{32}	
+	176	49	12	14	5^{98}	-7^{77}	Higman symmetric 2-design [1099, 1932, 1919, 338]
		126	90	90	6^{77}	-6^{98}	
!	176	70	18	34	2^{154}	-18^{21}	$S(4,7,23)\setminus S(3,6,22)$; M_{22}/Alt(7); unique by Coolsaet & Degraer [604]; 2-graph
		105	68	54	17^{21}	-3^{154}	Witt 3-(22,7,4): intersection 3 graph of a 2-(22,7,16) design with block intersections 1, 3; 2-graph
?	176	70	24	30	4^{120}	-10^{55}	
		105	64	60	9^{55}	-5^{120}	
−	176	70	42	18	26^{10}	-2^{165}	Abs
		105	52	78	1^{165}	-27^{10}	Abs
+	176	85	48	34	17^{22}	-3^{153}	Haemers; 2-graph
		90	38	54	2^{153}	-18^{22}	2-graph
−	177	88	43	44	6.152^{88}	-7.152^{88}	Conf
+	181	90	44	45	6.227^{90}	-7.227^{90}	Paley(181); 2-graph$-*$
?	183	52	11	16	4^{122}	-9^{60}	
		130	93	90	8^{60}	-5^{122}	
+	183	70	29	25	9^{60}	-5^{122}	S(2,5,61)
		112	66	72	4^{122}	-10^{60}	
−	184	48	2	16	2^{160}	-16^{23}	Krein_2
		135	102	90	15^{23}	-3^{160}	Krein_1
?	185	92	45	46	6.301^{92}	-7.301^{92}	2-graph$-*$?
?	189	48	12	12	6^{90}	-6^{98}	
		140	103	105	5^{98}	-7^{90}	
?	189	60	27	15	15^{28}	-3^{160}	
		128	82	96	2^{160}	-16^{28}	

∃	v	k	λ	μ	r^f	s^g	Comments
?	189	88	37	44	4^{132}	-11^{56}	2-graph$-*$?
		100	55	50	10^{56}	-5^{132}	2-graph$-*$?
−	189	94	46	47	6.374^{94}	-7.374^{94}	Conf
!	190	36	18	4	16^{19}	-2^{170}	$\binom{20}{2}$
		153	120	136	1^{170}	-17^{19}	
?	190	45	12	10	7^{75}	-5^{114}	
		144	108	112	4^{114}	-8^{75}	
?	190	84	33	40	4^{133}	-11^{56}	2-graph?
		105	60	55	10^{56}	-5^{133}	2-graph?
+	190	84	38	36	8^{75}	-6^{114}	S(2,6,76)
		105	56	60	5^{114}	-9^{75}	
?	190	90	45	40	10^{57}	-5^{132}	2-graph?
		99	48	55	4^{132}	-11^{57}	2-graph?
+	193	96	47	48	6.446^{96}	-7.446^{96}	Paley(193); 2-graph$-*$
+	195	96	46	48	6^{104}	-8^{90}	2-graph$-*$
		98	49	49	7^{90}	-7^{104}	S(2,7,91); 2-graph$-*$
!	196	26	12	2	12^{26}	-2^{169}	14^2
		169	144	156	1^{169}	-13^{26}	OA(14,13)?
?	196	39	2	9	3^{147}	-10^{48}	
		156	125	120	9^{48}	-4^{147}	
+	196	39	14	6	11^{39}	-3^{156}	OA(14,3)
		156	122	132	2^{156}	-12^{39}	OA(14,12)?
?	196	45	4	12	3^{150}	-11^{45}	
		150	116	110	10^{45}	-4^{150}	
+	196	52	18	12	10^{52}	-4^{143}	OA(14,4)
		143	102	110	3^{143}	-11^{52}	OA(14,11)?
?	196	60	14	20	4^{135}	-10^{60}	
		135	94	90	9^{60}	-5^{135}	
+	196	60	23	16	11^{48}	-4^{147}	S(2,4,49); Huffman–Tonchev [1151]: intersection 3 graph of a 2-(49,9,6) design with block intersections 1, 3
		135	90	99	3^{147}	-12^{48}	
+	196	65	24	20	9^{65}	-5^{130}	OA(14,5)
		130	84	90	4^{130}	-10^{65}	OA(14,10)?
?	196	75	26	30	5^{120}	-9^{75}	
		120	74	72	8^{75}	-6^{120}	
?	196	78	32	30	8^{78}	-6^{117}	OA(14,6)?
		117	68	72	5^{117}	-9^{78}	OA(14,9)?
?	196	81	42	27	18^{24}	-3^{171}	
		114	59	76	2^{171}	-19^{24}	
−	196	85	18	51	1^{187}	-34^{8}	Krein_2; Abs
		110	75	44	33^{8}	-2^{187}	Krein_1; Abs
?	196	90	40	42	6^{105}	-8^{90}	$RSHCD-$?; 2-graph?
		105	56	56	7^{90}	-7^{105}	2-graph?
+	196	91	42	42	7^{91}	-7^{104}	OA(14,7)?; $RSHCD+$; 2-graph
		104	54	56	6^{104}	-8^{91}	OA(14,8)?; 2-graph
+	197	98	48	49	6.518^{98}	-7.518^{98}	Paley(197); 2-graph$-*$
−	201	100	49	50	6.589^{100}	-7.589^{100}	Conf
?	204	28	2	4	4^{119}	-6^{84}	
		175	150	150	5^{84}	-5^{119}	
?	204	63	22	18	9^{68}	-5^{135}	
		140	94	100	4^{135}	-10^{68}	S(2,10,136)?
?	205	68	15	26	3^{164}	-14^{40}	
		136	93	84	13^{40}	-4^{164}	
?	205	96	50	40	14^{40}	-4^{164}	
		108	51	63	3^{164}	-15^{40}	
?	205	102	50	51	6.659^{102}	-7.659^{102}	2-graph$-*$?
?	208	45	8	10	5^{117}	-7^{90}	
		162	126	126	6^{90}	-6^{117}	
+	208	75	30	25	10^{64}	-5^{143}	S(2,5,65); $NU(3,4)$
		132	81	88	4^{143}	-11^{64}	
?	208	81	24	36	3^{168}	-15^{39}	
		126	80	70	14^{39}	-4^{168}	

∃	v	k	λ	μ	r^f	s^g	Comments
−	209	16	3	1	5^{76}	-3^{132}	$\mu = 1$
		192	176	180	2^{132}	-6^{76}	
?	209	52	15	12	8^{76}	-5^{132}	
		156	115	120	4^{132}	-9^{76}	
+	209	100	45	50	5^{132}	-10^{76}	2-graph−∗
		108	57	54	9^{76}	-6^{132}	2-graph−∗
−	209	104	51	52	6.728^{104}	-7.728^{104}	Conf
?	210	33	0	6	3^{154}	-9^{55}	
		176	148	144	8^{55}	-4^{154}	
!	210	38	19	4	17^{20}	-2^{189}	$\binom{21}{2}$
		171	136	153	1^{189}	-18^{20}	
?	210	76	26	28	6^{114}	-8^{95}	
		133	84	84	7^{95}	-7^{114}	
?	210	77	28	28	7^{99}	-7^{110}	
		132	82	84	6^{110}	-8^{99}	
?	210	95	40	45	5^{133}	-10^{76}	2-graph?
		114	63	60	9^{76}	-6^{133}	2-graph?
+	210	99	48	45	9^{77}	-6^{132}	Sym(7); Klin; 2-graph
		110	55	60	5^{132}	-10^{77}	2-graph
−	213	106	52	53	6.797^{106}	-7.797^{106}	Conf
?	216	40	4	8	4^{140}	-8^{75}	
		175	142	140	7^{75}	-5^{140}	
?	216	43	10	8	7^{86}	-5^{129}	
		172	136	140	4^{129}	-8^{86}	
−	216	70	40	14	28^{12}	-2^{203}	Abs
		145	88	116	1^{203}	-29^{12}	Abs
?	216	75	18	30	3^{175}	-15^{40}	
		140	94	84	14^{40}	-4^{175}	
?	216	86	40	30	14^{43}	-4^{172}	
		129	72	84	3^{172}	-15^{43}	
?	216	90	39	36	9^{80}	-6^{135}	S(2,6,81)?
		125	70	75	5^{135}	-10^{80}	
?	217	66	15	22	4^{154}	-11^{62}	
		150	105	100	10^{62}	-5^{154}	
?	217	88	39	33	11^{62}	-5^{154}	
		128	72	80	4^{154}	-12^{62}	
−	217	108	53	54	6.865^{108}	-7.865^{108}	Conf
?	220	72	22	24	6^{120}	-8^{99}	
		147	98	98	7^{99}	-7^{120}	
+	220	84	38	28	14^{44}	-4^{175}	Tonchev: intersection 3 graph of a 2-(45,9,8) design with block intersections 1, 3
		135	78	90	3^{175}	-15^{44}	
+	221	64	24	16	12^{51}	-4^{169}	S(2,4,52)
		156	107	117	3^{169}	-13^{51}	
?	221	110	54	55	6.933^{110}	-7.933^{110}	2-graph−∗?
+	222	51	20	9	14^{36}	-3^{185}	S(2,3,37)
		170	127	140	2^{185}	-15^{36}	
!	225	28	13	2	13^{28}	-2^{196}	15^2
		196	169	182	1^{196}	-14^{28}	OA(15,14)?
+	225	42	15	6	12^{42}	-3^{182}	OA(15,3)
		182	145	156	2^{182}	-13^{42}	OA(15,13)?
?	225	48	3	12	3^{176}	-12^{48}	
		176	139	132	11^{48}	-4^{176}	
−	225	56	1	18	2^{200}	-19^{24}	Krein_2
		168	129	114	18^{24}	-3^{200}	Krein_1
+	225	56	19	12	11^{56}	-4^{168}	OA(15,4)
		168	123	132	3^{168}	-12^{56}	OA(15,12)?
?	225	64	13	20	4^{160}	-11^{64}	
		160	115	110	10^{64}	-5^{160}	
+	225	70	25	20	10^{70}	-5^{154}	OA(15,5)
		154	103	110	4^{154}	-11^{70}	OA(15,11)?
?	225	80	25	30	5^{144}	-10^{80}	
		144	93	90	9^{80}	-6^{144}	

∃	v	k	λ	μ	r^f	s^g	Comments
+	225	84	33	30	9^{84}	-6^{140}	OA(15,6)
		140	85	90	5^{140}	-10^{84}	OA(15,10)?
−	225	96	19	57	1^{216}	-39^{8}	Krein_2; Abs
		128	88	52	38^{8}	-2^{216}	Krein_1; Abs
?	225	96	39	42	6^{128}	-9^{96}	
		128	73	72	8^{96}	-7^{128}	
?	225	96	51	33	21^{24}	-3^{200}	
		128	64	84	2^{200}	-22^{24}	
+	225	98	43	42	8^{98}	-7^{126}	OA(15,7)?; Pasechnik(15)
		126	69	72	6^{126}	-9^{98}	OA(15,9)?
+	225	112	55	56	7^{112}	-8^{112}	skewhad^2; OA(15,8)?; 2-graph$-*$
+	226	105	48	49	7^{113}	-8^{112}	switch $\text{skewhad}^2 + *$; 2-graph
		120	63	64	7^{112}	-8^{113}	S(2,8,113)?; 2-graph
+	229	114	56	57	7.066^{114}	-8.066^{114}	Paley(229); 2-graph$-*$
+	231	30	9	3	9^{55}	-3^{175}	M_{22}; Cameron
		200	172	180	2^{175}	-10^{55}	
!	231	40	20	4	18^{21}	-2^{209}	$\binom{22}{2}$
		190	153	171	1^{209}	-19^{21}	
?	231	70	21	21	7^{110}	-7^{120}	
		160	110	112	6^{120}	-8^{110}	
?	231	90	33	36	6^{132}	-9^{98}	
		140	85	84	8^{98}	-7^{132}	
?	232	33	2	5	4^{144}	-7^{87}	
		198	169	168	6^{87}	-5^{144}	
?	232	63	14	18	5^{144}	-9^{87}	
		168	122	120	8^{87}	-6^{144}	
?	232	77	36	20	19^{28}	-3^{203}	
		154	96	114	2^{203}	-20^{28}	
?	232	81	30	27	9^{87}	-6^{144}	
		150	95	100	5^{144}	-10^{87}	S(2,10,145)?
+	233	116	57	58	7.132^{116}	-8.132^{116}	Paley(233); 2-graph$-*$
?	235	42	9	7	7^{94}	-5^{140}	
		192	156	160	4^{140}	-8^{94}	
?	235	52	9	12	5^{140}	-8^{94}	
		182	141	140	7^{94}	-6^{140}	
?	236	55	18	11	11^{59}	-4^{176}	
		180	135	144	3^{176}	-12^{59}	S(2,12,177)?
−	237	118	58	59	7.197^{118}	-8.197^{118}	Conf
?	238	75	20	25	5^{153}	-10^{84}	
		162	111	108	9^{84}	-6^{153}	
+	241	120	59	60	7.262^{120}	-8.262^{120}	Paley(241); 2-graph$-*$
+	243	22	1	2	4^{132}	-5^{110}	$3^5.2.M_{11}$ (rk 3); Berlekamp, van Lint, & Seidel [216]; Golay code: projective ternary [11,5] code with weights 6, 9
		220	199	200	4^{110}	-5^{132}	
?	243	66	9	21	3^{198}	-15^{44}	
		176	130	120	14^{44}	-4^{198}	
−	243	88	52	20	34^{11}	-2^{231}	Abs
		154	85	119	1^{231}	-35^{11}	Abs
+	243	110	37	60	2^{220}	-25^{22}	$3^5.2.M_{11}$ (rk 3); Delsarte; projective ternary [55,5] code with weights 36, 45
		132	81	60	24^{22}	-3^{220}	
?	243	112	46	56	4^{182}	-14^{60}	2-graph$-*$?
		130	73	65	13^{60}	-5^{182}	2-graph$-*$?
?	244	108	42	52	4^{183}	-14^{60}	2-graph?
		135	78	70	13^{60}	-5^{183}	2-graph?
?	244	117	60	52	13^{61}	-5^{182}	2-graph?
		126	60	70	4^{182}	-14^{61}	2-graph?
?	245	52	3	13	3^{195}	-13^{49}	
		192	152	144	12^{49}	-4^{195}	
?	245	64	18	16	8^{100}	-6^{144}	
		180	131	135	5^{144}	-9^{100}	

∃	v	k	λ	μ	r^f	s^g	Comments
?	245	108	39	54	3^{204}	-18^{40}	2-graph$-*$?
		136	81	68	17^{40}	-4^{204}	2-graph$-*$?
?	245	122	60	61	7.326^{122}	-8.326^{122}	2-graph$-*$?
?	246	85	20	34	3^{204}	-17^{41}	
		160	108	96	16^{41}	-4^{204}	
?	246	105	36	51	3^{205}	-18^{40}	2-graph?
		140	85	72	17^{40}	-4^{205}	2-graph?
?	246	119	64	51	17^{41}	-4^{204}	2-graph?
		126	57	72	3^{204}	-18^{41}	2-graph?
+	247	54	21	9	15^{38}	-3^{208}	S(2,3,39)
		192	146	160	2^{208}	-16^{38}	
?	249	88	27	33	5^{165}	-11^{83}	
		160	104	100	10^{83}	-6^{165}	
−	249	124	61	62	7.390^{124}	-8.390^{124}	Conf
?	250	81	24	27	6^{144}	-9^{105}	
		168	113	112	8^{105}	-7^{144}	
?	250	96	44	32	16^{45}	-4^{204}	
		153	88	102	3^{204}	-17^{45}	
!	253	42	21	4	19^{22}	-2^{230}	$\binom{23}{2}$
		210	171	190	1^{230}	-20^{22}	
−	253	90	17	40	2^{230}	-25^{22}	Krein_2
		162	111	90	24^{22}	-3^{230}	Krein_1
+	253	112	36	60	2^{230}	-26^{22}	$S(4,7,23)$; M_{23}
		140	87	65	25^{22}	-3^{230}	Witt 4-(23,7,1): intersection 3 graph of a 2-(23,7,21) design with block intersections 1, 3
−	253	126	62	63	7.453^{126}	-8.453^{126}	Conf
+	255	126	61	63	7^{135}	-9^{119}	$O_9(2)$ polar graph; $Sp_8(2)$ polar graph; 2-graph$-*$
		128	64	64	8^{119}	-8^{135}	S(2,8,120); 2-graph$-*$
!	256	30	14	2	14^{30}	-2^{225}	16^2; from a partial spread: projective 4-ary [10,4] code with weights 4, 8; from a partial spread of 4-spaces: projective binary [30,8] code with weights 8, 16
		225	196	210	1^{225}	-15^{30}	OA(16,15)
+	256	45	16	6	13^{45}	-3^{210}	OA(16,3); $\text{Bilin}_{2\times 4}(2)$; Brouwer [342]; from a partial spread: projective 4-ary [15,4] code with weights 8, 12; from a partial spread of 4-spaces: projective binary [45,8] code with weights 16, 24
		210	170	182	2^{210}	-14^{45}	OA(16,14)
+	256	51	2	12	3^{204}	-13^{51}	van Lint–Schrijver(1); $VO_4^-(4)$ affine polar graph; projective 4-ary [17,4] code with weights 12, 16
		204	164	156	12^{51}	-4^{204}	van Lint–Schrijver(4)
+	256	60	20	12	12^{60}	-4^{195}	OA(16,4); from a partial spread: projective 4-ary [20,4] code with weights 12, 16; Brouwer [342]; from a partial spread of 4-spaces: projective binary [60,8] code with weights 24, 32
		195	146	156	3^{195}	-13^{60}	OA(16,13)
−	256	66	2	22	2^{231}	-22^{24}	Krein_2
		189	144	126	21^{24}	-3^{231}	Krein_1
+	256	68	12	20	4^{187}	-12^{68}	Brouwer [342]; projective binary [68,8] code with weights 32, 40
		187	138	132	11^{68}	-5^{187}	
+	256	75	26	20	11^{75}	-5^{180}	OA(16,5); $\text{Bilin}_{2\times 2}(4)$; $VO_4^+(4)$ affine polar graph; from a partial spread: projective 4-ary [25,4] code with weights 16, 20; from a partial spread of 4-spaces: projective binary [75,8] code with weights 32, 40
		180	124	132	4^{180}	-12^{75}	OA(16,12)
+	256	85	24	30	5^{170}	-11^{85}	van Lint–Schrijver(1); possibly projective binary [85,8] code with weights 40, 48
		170	114	110	10^{85}	-6^{170}	van Lint–Schrijver(2)
+	256	90	34	30	10^{90}	-6^{165}	OA(16,6); from a partial spread: projective 4-ary [30,4] code with weights 20, 24; from a partial spread of 4-spaces: projective binary [90,8] code with weights 40, 48
		165	104	110	5^{165}	-11^{90}	OA(16,11)

∃	v	k	λ	μ	r^f	s^g	Comments
+	256	102	38	42	6^{153}	-10^{102}	$2^8.L_2(17)$ (rk 3); Liebeck; van Lint–Schrijver(2); possibly projective 4-ary [34,4] code with weights 24, 28
		153	92	90	9^{102}	-7^{153}	van Lint–Schrijver(3)
+	256	105	44	42	9^{105}	-7^{150}	OA(16,7); from a partial spread: projective 4-ary [35,4] code with weights 24, 28; Brouwer [342]; from a partial spread of 4-spaces: projective binary [105,8] code with weights 48, 56
		150	86	90	6^{150}	-10^{105}	OA(16,10)
+	256	119	54	56	7^{136}	-9^{119}	$VO_8^-(2)$ affine polar graph; projective binary [119,8] code with weights 56, 64; $RSHCD-$; 2-graph
		136	72	72	8^{119}	-8^{136}	2-graph
+	256	120	56	56	8^{120}	-8^{135}	OA(16,8); from a partial spread: projective 4-ary [40,4] code with weights 28, 32; from a partial spread of 4-spaces: projective binary [120,8] code with weights 56, 64; $RSHCD+$; 2-graph
		135	70	72	7^{135}	-9^{120}	OA(16,9); Goethals–Seidel(2,15); $VO_8^+(2)$ affine polar graph; 2-graph
+	257	128	63	64	7.516^{128}	-8.516^{128}	Paley(257); 2-graph$-*$
?	259	42	5	7	5^{147}	-7^{111}	
		216	180	180	6^{111}	-6^{147}	
?	260	70	15	20	5^{168}	-10^{91}	
		189	138	135	9^{91}	-6^{168}	
?	261	52	11	10	7^{116}	-6^{144}	
		208	165	168	5^{144}	-8^{116}	
?	261	64	14	16	6^{144}	-8^{116}	
		196	147	147	7^{116}	-7^{144}	
?	261	80	25	24	8^{116}	-7^{144}	
		180	123	126	6^{144}	-9^{116}	
?	261	84	39	21	21^{29}	-3^{231}	
		176	112	132	2^{231}	-22^{29}	
?	261	130	64	65	7.578^{130}	-8.578^{130}	2-graph$-*$?
?	265	96	32	36	6^{159}	-10^{105}	
		168	107	105	9^{105}	-7^{159}	
?	265	132	65	66	7.639^{132}	-8.639^{132}	2-graph$-*$?
?	266	45	0	9	3^{209}	-12^{56}	
		220	183	176	11^{56}	-4^{209}	
+	269	134	66	67	7.701^{134}	-8.701^{134}	Paley(269); 2-graph$-*$
?	273	72	21	18	9^{104}	-6^{168}	
		200	145	150	5^{168}	-10^{104}	
?	273	80	19	25	5^{182}	-11^{90}	
		192	136	132	10^{90}	-6^{182}	
+	273	102	41	36	11^{90}	-6^{182}	S(2,6,91)
		170	103	110	5^{182}	-12^{90}	
?	273	136	65	70	6^{168}	-11^{104}	
		136	69	66	10^{104}	-7^{168}	
−	273	136	67	68	7.761^{136}	-8.761^{136}	Conf
!	275	112	30	56	2^{252}	-28^{22}	$q_{22}^2=0$; 2-graph$-*$
		162	105	81	27^{22}	-3^{252}	$McL.2/U_4(3).2$; McLaughlin graph; unique by Goethals & Seidel [921]; $q_{11}^1=0$; 2-graph$-*$
!	276	44	22	4	20^{23}	-2^{252}	$\binom{24}{2}$
		231	190	210	1^{252}	-21^{23}	
?	276	75	10	24	3^{230}	-17^{45}	
		200	148	136	16^{45}	-4^{230}	
?	276	75	18	21	6^{160}	-9^{115}	
		200	145	144	8^{115}	-7^{160}	
−	276	110	28	54	2^{253}	-28^{22}	Krein_2; Abs
		165	108	84	27^{22}	-3^{253}	Krein_1; Abs
?	276	110	52	38	18^{45}	-4^{230}	
		165	92	108	3^{230}	-19^{45}	
+	276	135	78	54	27^{23}	-3^{252}	Conway, Goethals–Seidel; 2-graph
		140	58	84	2^{252}	-28^{23}	2-graph
+	277	138	68	69	7.822^{138}	-8.822^{138}	Paley(277); 2-graph$-*$

∃	v	k	λ	μ	r^f	s^g	Comments
+	279	128	52	64	4^{216}	-16^{62}	2-graph−∗
		150	85	75	15^{62}	-5^{216}	2-graph−∗
+	280	36	8	4	8^{90}	-4^{189}	$J_2/3.PGL_2(9)$ (rk 4); $U_4(3)$ polar graph
		243	210	216	3^{189}	-9^{90}	
?	280	62	12	14	6^{155}	-8^{124}	
		217	168	168	7^{124}	-7^{155}	
?	280	63	14	14	7^{135}	-7^{144}	
		216	166	168	6^{144}	-8^{135}	
+	280	117	44	52	5^{195}	-13^{84}	
		162	96	90	12^{84}	-6^{195}	Sym(9) (rk 5); Mathon & Rosa
?	280	124	48	60	4^{217}	-16^{62}	2-graph?
		155	90	80	15^{62}	-5^{217}	2-graph?
+	280	135	70	60	15^{63}	-5^{216}	$J_2/3.PGL_2(9)$ (rk 4); 2-graph
		144	68	80	4^{216}	-16^{63}	2-graph

See Also

§II.5	Steiner systems.
§III.3	Mutually orthogonal latin squares.
§V.1	Hadamard matrices.
§V.6	Conference matrices.
§VI.1	Association schemes.
§VI.23	Generalized quadrangles.
§VI.48	Quasi-symmetric designs.
§VII.13	Two-graphs.
[348, 1146]	Early surveys of the construction of strongly regular graphs.
[343]	Parameters of infinite series, the isomorphisms, and existence and nonexistence results.

References Cited: [216, 338, 340, 342, 343, 345, 346, 348, 403, 412, 420, 450, 512, 515, 604, 605, 610, 672, 673, 676, 893, 894, 918, 920, 921, 1007, 1008, 1024, 1096, 1098, 1099, 1116, 1146, 1151, 1217, 1322, 1361, 1535, 1577, 1672, 1674, 1718, 1719, 1723, 1730, 1859, 1870, 1872, 1902, 1919, 1932, 1947, 2006, 2007, 2087, 2140]

12 Directed Strongly Regular Graphs

Andries E. Brouwer
Sylvia A. Hobart

12.1 Definitions and Basics

12.1 A directed strongly regular graph (dsrg) is a (0,1)-matrix A with 0s on the diagonal such that the linear span of I, A and J is closed under matrix multiplication.

12.2 The (integral) parameters v, k, t, λ, μ are defined by: A is a matrix of order v, and $AJ = JA = kJ$, and $A^2 = tI + \lambda A + \mu(J - I - A)$. The object is a dsrg($v$,$k$,$t$,$\lambda$,$\mu$).

12.3 **Remark** Many authors use the parameter ordering (v, k, μ, λ, t).

12.4 The *complement* of a dsrg A is $J - I - A$. The complement is also a dsrg.

12.5 **Proposition** If A has parameters v, k, t, λ, μ then its complement $J - I - A$ has parameters v, $v - k - 1$, $v - 2k - 1 + t$, $v - 2k - 2 + \mu$, $v - 2k + \lambda$. In Table 12.47, complementary pairs are given together.

12.6 The *reverse* of a dsrg A is A^T. The reverse is also a dsrg.

12.7 Remark The concept of *directed* strongly regular graphs is due to Duval [763]. Hammersley [1030] studied the "love problem," a problem related to this present topic, and presented pictures of dsrg(8,3,2,1,1) and dsrg(15,4,2,1,1).

12.8 Remark Clearly, $0 \le t \le k$. In what follows it is assumed that $0 < t < k$. The case $t = k$ is that of strongly regular graphs, where A is symmetric (see §VII.11). The case $t = 0$ is that of Hadamard matrices H with 1s on the diagonal and skew symmetric off-diagonal. (See §V.1 and [1113].)

▷ Spectrum

12.9 Remark The algebra spanned by I, A, and J is 3-dimensional. The matrix A is diagonalizable and has precisely 3 distinct eigenvalues, say k, r, and s, with multiplicities 1, f, and g, respectively, with $f \ne g$. The eigenvalues r, s different from k are roots of $x^2 + (\mu - \lambda)x + \mu - t = 0$. They are integers, and r is chosen nonnegative while s is chosen negative. (One sees that $\mu \le t$.)

▷ The 2-Dimensional and 1-Dimensional Cases

12.10 Remark An important subclass is when the linear span of A and J is closed under matrix multiplication. This happens when $t = \mu$, and then $A^2 = (\lambda - \mu)A + \mu J$ so that the eigenvalues of A are k, $\lambda - \mu$, and 0. Conversely, when A has eigenvalue 0, one is in this case. Put $d = \mu - \lambda$. Then the multiplicities of the eigenvalues k, $-d$, 0 are 1, k/d, and $v - 1 - k/d$, respectively, and A has rank $1 + k/d$.

12.11 Remark If A is a 0-1 matrix, then $B = J - 2A$ is a ± 1 matrix, and it is possible that the 1-space generated by B is closed under matrix multiplication. This happens when $t = \mu$ and $v - 4k + 4t = d$ (with d as above—this is a subcase of the 2-dimensional case). Conversely, if B is a ± 1 matrix with constant row sums and 1s on the diagonal such that B^2 is a multiple of B, then $A = (J - B)/2$ is the adjacency matrix of a dsrg in this subcase. The set of such ± 1 matrices B is closed under taking tensor products.

▷ Combinatorial Parameter Conditions

12.12 Remark Remark 12.9 implies that $0 < \mu \le t$. (If $\mu = 0$, then $A = J - I$, which was excluded.) It also follows that $0 \le \lambda < t < k < v$. (Indeed, $\lambda < t$, since $\lambda + 1 - t = (r+1)(s+1) \le 0$.) The matrix equation immediately gives $k(k - \lambda + \mu) = \mu(v-1) + t$. Duval [763] gave one more condition, and parameter sets violating it are not mentioned in Table 12.47. The condition follows from counting the number of paths of length 2 between two points

12.13 Theorem If A is a dsrg(v,k,t,λ,μ), then $-2(k - t - 1) \le \mu - \lambda \le 2(k - t)$.

▷ Not a Cayley Graph of an Abelian Group

12.14 Theorem [1311] A directed strongly regular graph cannot be a Cayley graph of an abelian group.

12.15 Remark Theorem 12.14 is proved by observing that if A_s is the symmetric part of A (with row sums t), then A and A_s have real eigenvalues, while $A - A_s$ has a nonreal eigenvalue (since $(A - A_s)^2$ has zero trace and the positive eigenvalue $(k - t)^2$), so that A and A_s do not commute.

12.2 Constructions

12.16 Construction [C1] [763] For every $k > 2$, there exists a dsrg with $v = k(k+1)$, $k = k$, $t = 1$, $\lambda = 0$, $\mu = 1$.

12.17 Remark Construction C1 is a special case of C6(i) obtained by taking a 2-$(k+1, 2, 1)$ design.

12.18 Construction [C2] [763] Let q be a prime power, $q \equiv 1 \pmod 4$. Then there exists a dsrg with $v = 2q$, $k = q-1$, $t = \mu = \lambda + 1 = k/2$.

12.19 Construction [C3] [1215] Let μ, k be positive integers such that $\mu|(k-1)$. Then there exists a dsrg with $v = (k+1)(k-1)/\mu$, $t = \mu+1$, $\lambda = \mu$. The construction is as follows: Take as vertices the integers mod v and let $x \to y$ be an edge when $x + ky = 1, 2, ..., k \pmod v$.

12.20 Construction [C4] [1311] Let n be an odd integer. Then there exists a dsrg with $v = 2n$, $k = n-1$, $t = \mu = \lambda + 1 = k/2$.

12.21 Remark The graphs from Construction C4, and those of [1114] with parameters $(4t, 2t-1, t, t-1, t-1)$ (also covered by [C3]), are Cayley graphs of nonabelian groups.

12.22 Construction [C5] [1312] If there exists a generalized quadrangle GQ(a,b), then there exists a dsrg with $v = (a+1)(b+1)(ab+1)$, $k = ab+a+b$, $t = \lambda + 1 = a+b$, $\mu = 1$. This graph is obtained by looking at (point,line) flags, where $(p, L) \to (q, M)$ when the flags are distinct and q is on L.

12.23 Construction [C6] [814] If there exists a 2-(V, B, R, K, Λ) design, then (i) there exists a dsrg with $v = VR$, $k = R(K-1)$, $t = \mu = \Lambda(K-1)$, $\lambda = \Lambda(K-2)$ and also (ii) a dsrg with $v = VR$, $k = RK-1$, $t = \lambda + 1 = \Lambda(K-1) + R - 1$, $\mu = \Lambda K$. The former is obtained by looking at (point,block) flags, where $(p, B) \to (q, C)$ when p and q are distinct and q is on B. The latter is obtained by looking at (point,block) flags, where $(p, B) \to (q, C)$ when the flags are distinct and q is on B.

12.24 Construction [C7] [814] If there exists a partial geometry with parameters pg(K, R, T), then there exists a dsrg with $v = RK(1+(K-1)(R-1)/T)$, $k = RK-1$, $t = \lambda+1 = K+R-2$, $\mu = T$. This graph is obtained by looking at (point,line) flags, where $(p, L) \to (q, M)$ when the flags are distinct and q is on L. Of course C5 is the special case $T = 1$ of this.

12.25 Construction [C8] [763] If there exists a dsrg with parameters v, k, t, λ, μ, and $t = \mu$, then for each positive integer m there is also a dsrg with parameters mv, mk, mt, $m\lambda$, $m\mu$. Construction: given A, consider $A \otimes J$, with J of order m.

12.26 Construction [C9] [914] Suppose n, d, and c are positive integers such that $c < n-1$ and $c|d(n-1)$. Then there exists a dsrg with parameters $v = dn(n-1)/c$, $k = d(n-1)$, $t = \mu = cd$, $\lambda = (c-1)d$.

12.27 Construction [C10] [813] Let q be an odd prime power. Then there exists a dsrg with $v = (q-1)(q^2-1)$, $k = q^2-2$, $t = \lambda + 1 = 2q-2$, $\mu = q$.

12.28 Construction [C11] [813] Let q be an odd prime power. There there exists a dsrg with $v = 2q^2$, $k = 3q-2$, $t = 2q-1$, $\lambda = q-1$, $\mu = 3$.

12.29 Construction [C12] If there exists an srg with parameters v, k, λ, μ, and $\mu = \lambda + 1$, then there is a dsrg with parameters vk, $(v-k-1)k$, $(v-k-1)(k-\mu)$, $(v-k-2)(k-\mu)$, $(v-k-1)(k-\mu)$. Construction: take the edges of the srg, and let $xy \to uv$ when u is at distance 2 from y.

12.30 Example Using Construction C12, the Petersen graph produces a dsrg(30,18,12,10,12).

12.31 Construction [C13] Let r be an odd prime power. Then there exists a dsrg with parameters $2r^2$, $(r-1)(2r+1)/2$, $(r-1)(3r+1)/4$, $r(r-1)/2-1$, $r(r-1)/2$.

12.32 Remark Construction C13 is obtained as follows: Take two copies of the finite field of order r^2. Join vertices in one copy when they differ by a square, in the other when they differ by a nonsquare. Thus, both halves are undirected (Paley) graphs. View the field as AG(2,r) and pick two sets, B and C, each the union of $(r-1)/2$ mutually parallel lines, where B and C use different directions. Make an arrow from x in the first copy to y' in the second copy when $y-x$ is a member of B, and an arrow from y' to x when $y-x$ is a member of C.

12.33 Construction [C14] The tensor product of two ± 1 matrices belonging to dsrgs in the 1-dimensional case, is again a dsrg in the 1-dimensional case. Here one may also take I of order 2.

12.34 Construction [C15] [914] Given a dsrg with adjacency matrix A, where $\mu = \lambda$ and $v = 4(k-\mu)$, and a Hadamard matrix H of order c with constant row and column sums d, and ones on the diagonal, put $B = J - 2A$ and $B' = B \otimes H$. The parameter conditions say that B is a ± 1 matrix with 1s on the diagonal, constant row and column sums, and B^2 a multiple of I. Clearly, the same holds for B'. Hence A', given by $B' = J - 2A'$, is again the adjacency matrix of a dsrg. The parameters are $v' = vc$, $k' = 2c(k-\mu)+d(2\mu-k)$, $t' = c(k+t-2\mu)+d(2\mu-k)$, $\lambda' = \mu' = c(k-\mu)+d(2\mu-k)$. Note that $c = d^2$.

12.3 Nonexistence Conditions

12.35 Theorem [N1] [1216] If $g = 2$ then $(v,k,t,\lambda,\mu) = (6m, 2m, m, 0, m)$ or $(v,k,t,\lambda,\mu) = (8m, 4m, 3m, m, 3m)$.

12.36 Theorem [N2] [1216] For $g = 3$, $(v,k,t,\lambda,\mu) = (6m, 3m, 2m, m, 2m)$ or $(v,k,t,\lambda,\mu) = (12m, 3m, m, 0, m)$.

12.37 Theorem [N3] [1216] $(k-t)(\mu-k+t) \le \lambda t$.

12.38 Remark Theorem 12.37 is proved as follows: Fix a point x and look at triangles xyz where xy is a directed edge and xz is an undirected edge, and yz may be directed (in the yz direction) or undirected. The number of triangles is at least $(k-t)(\mu-k+t)$ and at most λt.

12.39 Theorem [N4] [1216] If $\lambda = 0$ and $\mu = k - t$, then v is a multiple of 3μ.

12.40 Remark Theorem 12.39 is proved as follows: Because $\lambda = 0$, the μ triangles on a directed edge contain directed edges only, and one sees that the directed edges form a graph where each connected component has 3μ vertices since it is the μ-coclique extension of a directed triangle.

12.41 Theorem (Absolute Bound [1216])
(i) If $s \ne -1$, then $v \le f(f+3)/2$. If $v(r+s^2) \ne 2(r-s)(k-s)$ also, then $v \le f(f+1)/2$.
(ii) If $r \ne 0$, then $v \le g(g+3)/2$. If $v(s+r^2) \ne 2(s-r)(k-r)$ also, then $v \le g(g+1)/2$.

12.4 Existence, Uniqueness, and Enumeration

12.42 Examples The two smallest dsrgs (with parameters (6,2,1,0,1) and (8,4,3,1,3)) are unique. Matrices for these dsrgs, A and B, respectively, are given below. The matrix

C is a dsrg with parameters (10,4,2,1,2) where points come in pairs with equal in-neighbors, but there is no such pairing for out-neighbors. There are 15 other examples with the same parameters. In a few cases uniqueness is known.

$$A = \begin{bmatrix} 0&0&1&1&0&0\\ 0&0&0&0&1&1\\ 0&0&0&0&1&1\\ 1&1&0&0&0&0\\ 1&1&0&0&0&0\\ 0&0&1&1&0&0 \end{bmatrix} \quad B = \begin{bmatrix} 0&0&0&0&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&1&0&1&0&1&0&1\\ 1&0&1&0&1&0&1&0\\ 0&1&0&1&0&1&0&1\\ 1&0&1&0&1&0&1&0\\ 1&1&1&1&0&0&0&0\\ 1&1&1&1&0&0&0&0 \end{bmatrix} \quad C = \begin{bmatrix} 0&0&0&0&0&0&1&1&1&1\\ 0&0&1&1&1&1&0&0&0&0\\ 1&1&0&0&1&1&0&0&0&0\\ 0&0&0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&1&1&1&1\\ 1&1&1&1&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0&1&1\\ 0&0&1&1&1&1&0&0&0&0\\ 0&0&1&1&1&1&0&0&0&0\\ 1&1&0&0&0&0&1&1&0&0 \end{bmatrix}.$$

12.43 Theorem [908] The dsrg($k(k+1)$,k,1,0,1) is unique for all positive integers k.

12.44 Theorem [1216] The dsrg($m(m+1)t$,mt,t,0,t) is unique for all positive integers m and t.

12.45 Theorem [1214] There are precisely 1292 nonisomorphic dsrg(15,5,2,1,2), namely, 1174, 100, 10, 5, 3 with full automorphism group of order 1, 2, 3, 4, 5, respectively.

12.46 Table Table of (mostly Jørgensen's) enumeration results (see also [1213]).

v	k	t	λ	μ	#	reference
6	2	1	0	1	1	
8	3	2	1	1	1	[1030]
10	4	2	1	2	16	[1214]
12	3	1	0	1	1	
12	4	2	0	2	1	
12	5	3	2	2	20	[1214]
14	6	3	2	3	16495	[1214]
15	4	2	1	1	5	[1214]
15	5	2	1	2	1292	[1214]
16	7	5	4	2	1	[1214]
18	4	3	0	1	1	[1214]
18	5	3	2	1	2	[1214]
18	6	3	0	3	1	
20	4	1	0	1	1	
24	6	2	0	2	1	

12.47 Table Directed strongly regular graphs with $v \le 32$. Online tables at [1113].

v	k	t	λ	μ	r^f	s^g	comments
6	2	1	0	1	0^3	-1^2	C1, C4, C6(i) for 2-(3,2,1), C9
	3	2	1	2	0^2	-1^3	C6(ii) for 2-(3,2,1), C7 for pg(2,2,2)
8	3	2	1	1	1^2	-1^5	C3, C5 for GQ(1,1)
	4	3	1	3	0^5	-2^2	
10	4	2	1	2	0^5	-1^4	C2, C4, C9, C12 from srg(5,2,0,1)
	5	3	2	3	0^4	-1^5	
12	3	1	0	1	0^8	-1^3	C1, C6(i) for 2-(4,2,1), C9
	8	6	5	6	0^3	-1^8	C6(ii) for 2-(4,3,2)
12	4	2	0	2	0^9	-2^2	C6(i) for 2-(3,2,2), C8 for m=2, C9
	7	5	4	4	1^2	-1^9	C6(ii) for 2-(3,2,2)
12	5	3	2	2	1^3	-1^8	C3, C6(ii) for 2-(4,2,1), C7 for pg(3,2,2)
	6	4	2	4	0^8	-2^3	C6(i) for 2-(4,3,2), C8 for m=2, C9

v	k	t	λ	μ	r^f	s^g	comments
14	5	4	1	2	1^7	-2^6	does not exist [1311]
	8	7	4	5	1^6	-2^7	
14	6	3	2	3	0^7	-1^6	C4, C9
	7	4	3	4	0^6	-1^7	
15	4	2	1	1	1^5	-1^9	C3
	10	8	6	8	0^9	-2^5	
15	5	2	1	2	0^9	-1^5	[1214]
	9	6	5	6	0^5	-1^9	
16	6	3	1	3	0^{12}	-2^3	does not exist ([813] or N2)
	9	6	5	5	1^3	-1^{12}	
16	7	4	3	3	1^4	-1^{11}	C3, C10
	8	5	3	5	0^{11}	-2^4	
16	7	5	4	2	3^2	-1^{13}	
	8	6	2	6	0^{13}	-4^2	C8 for m=2
18	4	3	0	1	1^{10}	-2^7	[763], Theorem 4.4.
	13	12	9	10	1^7	-2^{10}	
18	5	3	2	1	2^4	-1^{13}	C5 for GQ(1,2)
	12	10	7	10	0^{13}	-3^4	
18	6	3	0	3	0^{15}	-3^2	C6(i) for 2-(3,2,3), C8 for m=3, C9
	11	8	7	6	2^2	-1^{15}	C6(ii) for 2-(3,2,3)
18	7	5	2	3	1^9	-2^8	C11, C13
	10	8	5	6	1^8	-2^9	
18	8	4	3	4	0^9	-1^8	C2, C4, C9
	9	5	4	5	0^8	-1^9	
18	8	5	4	3	2^3	-1^{14}	
	9	6	3	6	0^{14}	-3^3	C8 for m=3
20	4	1	0	1	0^{15}	-1^4	C1, C6(i) for 2-(5,2,1), C9
	15	12	11	12	0^4	-1^{15}	C6(ii) for 2-(5,4,3)
20	7	4	3	2	2^4	-1^{15}	C6(ii) for 2-(5,2,1), C7 for pg(4,2,2)
	12	9	6	9	0^{15}	-3^4	C6(i) for 2-(5,4,3), C9
20	8	4	2	4	0^{15}	-2^4	C8 for m=2, C9
	11	7	6	6	1^4	-1^{15}	
20	9	5	4	4	1^5	-1^{14}	C3
	10	6	4	6	0^{14}	-2^5	C8 for m=2
21	6	2	1	2	0^{14}	-1^6	C6(i) for 2-(7,3,1), C9
	14	10	9	10	0^6	-1^{14}	
21	8	4	3	3	1^6	-1^{14}	C6(ii) for 2-(7,3,1), C7 for pg(3,3,3)
	12	8	6	8	0^{14}	-2^6	C9
22	9	6	3	4	1^{11}	-2^{10}	?
	12	9	6	7	1^{10}	-2^{11}	?
22	10	5	4	5	0^{11}	-1^{10}	C4, C9
	11	6	5	6	0^{10}	-1^{11}	
24	5	2	1	1	1^9	-1^{14}	C3
	18	15	13	15	0^{14}	-2^9	
24	6	2	0	2	0^{20}	-2^3	C6(i) for 2-(4,2,2), C8 for m=2, C9
	17	13	12	12	1^3	-1^{20}	C6(ii) for 2-(4,3,4)
24	7	3	2	2	1^8	-1^{15}	C3
	16	12	10	12	0^{15}	-2^8	C8 for m=2
24	8	4	0	4	0^{21}	-4^2	C6(i) for 2-(3,2,4), C8 for m=2, C9
	15	11	10	8	3^2	-1^{21}	C6(ii) for 2-(3,2,4)
24	8	3	2	3	0^{15}	-1^8	[1216]
	15	10	9	10	0^8	-1^{15}	
24	9	7	2	4	1^{15}	-3^8	[1216]
	14	12	8	8	2^8	-2^{15}	
24	10	5	3	5	0^{18}	-2^5	?
	13	8	7	7	1^5	-1^{18}	?
24	10	8	4	4	2^9	-2^{14}	[1216]
	13	11	6	8	1^{14}	-3^9	
24	11	6	5	5	1^6	-1^{17}	[1114], C3
	12	7	5	7	0^{17}	-2^6	
24	11	7	6	4	3^3	-1^{20}	C6(ii) for 2-(4,2,2)
	12	8	4	8	0^{20}	-4^3	C6(i) for 2-(4,3,4), C8 for m=2, C9

v	k	t	λ	μ	r^f	s^g	comments
24	11	8	7	3	5^2	-1^{21}	
	12	9	3	9	0^{21}	-6^2	C8 for m=3
25	9	6	5	2	4^3	-1^{21}	
	15	12	7	12	0^{21}	-5^3	does not exist by N2
25	10	6	1	6	0^{22}	-5^2	does not exist by N1
	14	10	9	6	4^2	-1^{22}	
26	11	7	4	5	1^{13}	-2^{12}	[1216]
	14	10	7	8	1^{12}	-2^{13}	
26	12	6	5	6	0^{13}	-1^{12}	C2, C4, C9
	13	7	6	7	0^{12}	-1^{13}	
27	7	4	1	2	1^{15}	-2^{11}	?
	19	16	13	14	1^{11}	-2^{15}	?
27	8	4	3	2	2^6	-1^{20}	C7 for pg(3,3,2)
	18	14	11	14	0^{20}	-3^6	
27	9	4	1	4	0^{23}	-3^3	does not exist by N2
	17	12	11	10	2^3	-1^{23}	
27	10	6	3	4	1^{14}	-2^{12}	?
	16	12	9	10	1^{12}	-2^{14}	?
27	11	6	5	4	2^5	-1^{21}	?
	15	10	7	10	0^{21}	-3^5	?
27	12	8	2	8	0^{24}	-6^2	does not exist by N1
	14	10	9	5	5^2	-1^{24}	
28	6	3	2	1	2^7	-1^{20}	does not exist (Brouwer, unpub.)
	21	18	15	18	0^{20}	-3^7	
28	7	2	1	2	0^{20}	-1^7	?
	20	15	14	15	0^7	-1^{20}	?
28	12	6	4	6	0^{21}	-2^6	C6(i) for 2-(7,4,2), C8 for m=2, C9
	15	9	8	8	1^6	-1^{21}	C6(ii) for 2-(7,4,2)
28	13	7	6	6	1^7	-1^{20}	C3
	14	8	6	8	0^{20}	-2^7	C8 for m=2
30	5	1	0	1	0^{24}	-1^5	C1, C6(i) for 2-(6,2,1), C9
	24	20	19	20	0^5	-1^{24}	C6(ii) for 2-(6,5,4)
30	7	5	0	2	1^{20}	-3^9	does not exist [1216]
	22	20	16	16	2^9	-2^{20}	
30	9	3	2	3	0^{20}	-1^9	C9
	20	14	13	14	0^9	-1^{20}	
30	9	5	4	2	3^5	-1^{24}	C6(ii) for 2-(6,2,1), C7 for pg(5,2,2)
	20	16	12	16	0^{24}	-4^5	C6(i) for 2-(6,5,4), C8 for m=2, C9
30	10	4	2	4	0^{24}	-2^5	C6(i) for 2-(6,3,2), C8 for m=2, C9
	19	13	12	12	1^5	-1^{24}	
30	10	5	0	5	0^{27}	-5^2	C6(i) for 2-(3,2,5), C8 for m=5, C9
	19	14	13	10	4^2	-1^{27}	C6(ii) for 2-(3,2,5)
30	11	5	4	4	1^9	-1^{20}	
	18	12	10	12	0^{20}	-2^9	C8 for m=2, C9, C12 from srg(10,3,0,1)
30	11	9	2	5	1^{21}	-4^8	?
	18	16	11	10	3^8	-2^{21}	?
30	12	6	3	6	0^{25}	-3^4	C6(i) for 2-(5,3,3), C8 for m=3, C9
	17	11	10	9	2^4	-1^{25}	C6(ii) for 2-(5,3,3)
30	12	11	4	5	2^{15}	-3^{14}	?
	17	16	9	10	2^{14}	-3^{15}	?
30	13	8	5	6	1^{15}	-2^{14}	?
	16	11	8	9	1^{14}	-2^{15}	?
30	13	11	6	5	3^9	-2^{20}	?
	16	14	7	10	1^{20}	-4^9	?
30	14	7	6	7	0^{15}	-1^{14}	C4, C9
	15	8	7	8	0^{14}	-1^{15}	
30	14	8	7	6	2^5	-1^{24}	C6(ii) for 2-(6,3,2)
	15	9	6	9	0^{24}	-3^5	C8 for m=3, C9
30	14	9	8	5	4^3	-1^{26}	
	15	10	5	10	0^{26}	-5^3	C8 for m=5
32	6	5	1	1	2^{14}	-2^{17}	does not exist [1215]
	25	24	19	21	1^{17}	-3^{14}	

v	k	t	λ	μ	r^f	s^g	comments
32	7	4	3	1	3^6	-1^{25}	C5 for GQ(1,3)
	24	21	17	21	0^{25}	-4^6	
32	9	6	1	3	1^{21}	-3^{10}	?
	22	19	15	15	2^{10}	-2^{21}	?
32	10	7	3	3	2^{13}	-2^{18}	?
	21	18	13	15	1^{18}	-3^{13}	?
32	11	6	5	3	3^5	-1^{26}	?
	20	15	11	15	0^{26}	-4^5	?
32	12	6	2	6	0^{28}	-4^3	does not exist by N2
	19	13	12	10	3^3	-1^{28}	
32	13	9	4	6	1^{20}	-3^{11}	
	18	14	10	10	2^{11}	-2^{20}	C15
32	14	7	5	7	0^{24}	-2^7	?
	17	10	9	9	1^7	-1^{24}	?
32	14	10	6	6	2^{12}	-2^{19}	C15
	17	13	8	10	1^{19}	-3^{12}	
32	15	8	7	7	1^8	-1^{23}	C3
	16	9	7	9	0^{23}	-2^8	
32	15	9	8	6	3^4	-1^{27}	
	16	10	6	10	0^{27}	-4^4	C8 for m=2
32	15	11	10	4	7^2	-1^{29}	
	16	12	4	12	0^{29}	-8^2	C8 for m=2

See Also

§II.6	More on Paley designs.
§V.1	Hadamard matrices.
§VI.23	Generalized quadrangles.
§VI.41	Partial geometries.
§VII.11	Strongly regular graphs.

References Cited: [763, 813, 814, 908, 914, 1030, 1113, 1114, 1213, 1214, 1215, 1216, 1311, 1312]

13 Two-Graphs

Edward Spence

13.1 Definitions and Examples

13.1

A *two-graph* (V, Δ) consists of a set V whose elements are the vertices, and a collection Δ of unordered triples of the vertices (the *odd triples*), such that each 4-tuple of V contains, as subsets, an even number of elements of Δ. If (V, Δ) is a two-graph, then so also is the pair $(V, V^3 \setminus \Delta)$; the *complement* of (V, Δ).

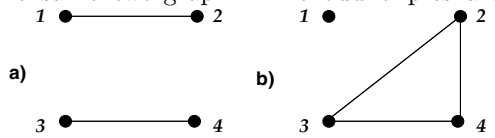
A *clique* of a two-graph (V, Δ) is a subset C of V such that every triple from C is in Δ.

The two-graphs (V, Δ) and (V', Δ') are *isomorphic* if there is a bijection $V \to V'$ that induces a bijection $\Delta \to \Delta'$.

The *automorphism group* $\mathrm{Aut}(V, \Delta)$ of a two-graph (V, Δ) is the group of permutations of V that preserve Δ.

13.2 Remark Given a (simple) graph $\Gamma = (V, E)$, the set Δ of triples of V whose induced subgraph in Γ contains an odd number of edges gives rise to a two-graph (V, Δ). In fact, every two-graph can be represented in this way.

13.3 Example The ladder graph on four vertices and a triangle extended by an isolated vertex give rise to the same two-graph. The odd triples are $\{123, 124, 134, 234\}$.



13.4 Remarks

1. In Example 13.3, (b) is obtained from (a) by *switching* the adjacencies of vertex 2. In general, switching with respect to a subset $X \subset V$ consists of interchanging adjacency and nonadjacency between X and its complement $V \setminus X$.
2. Graphs $\Gamma_1 = (V, E_1)$ and $\Gamma_2 = (V, E_2)$ represent the same two-graph if they are related by (the equivalence relation of) switching with respect to some $X \subset V$. Thus, a two-graph can be identified with the switching class of a graph.

13.5 The *switching class* of a graph Γ comprises those graphs with ∓ 1 adjacency matrices DAD, where D is a diagonal matrix with entries ± 1, and A is the ∓ 1 adjacency matrix of Γ (-1 for adjacency).

13.6 Remark Because$A$ and DAD (D as in the definition) have the same eigenvalues, the *eigenvalues of a two-graph* are the eigenvalues of the ∓ 1 adjacency matrix of any graph in its switching class.

13.7 Theorem [1517] Two-graphs, switching classes of graphs and the isomorphism classes of eulerian graphs (every vertex has even valency) on n vertices are equal in number.

13.8 Theorem [1871] Let $\Gamma = (V, E)$ be a graph in the switching class of a two-graph (V, Δ). Then $\mathrm{Aut}(\Gamma)$ is a subgroup of $\mathrm{Aut}(V, \Delta)$.

13.9 Theorem [1871] Let $\Gamma_i = (V, E_i)$, $i = 1, 2, \ldots, s$ denote the nonisomorphic graphs in the switching class of a two-graph (V, Δ), and let $|V| = n$, $|\mathrm{Aut}(V, \Delta)| = m$, $|\mathrm{Aut}\Gamma_i| = m_i$. Then $\sum_{i=1}^{s} \frac{m}{m_i} = 2^{n-1}$.

13.10 Remark Mallows and Sloane [1517] prove that every automorphism of a two-graph is also an automorphism of some graph in the switching class of the two-graph. However, there are two-graphs (V, Δ) each of whose switching classes contain graphs, all of which have automorphism group a *proper* subgroup of $\mathrm{Aut}(V, \Delta)$. All such two-graphs on $n \leq 10$ vertices are enumerated in [404].

13.11 Table The numbers $N_T(n)$ of pairwise nonisomorphic two-graphs on n vertices ($n \leq 10$). All two-graphs on $n \leq 9$ vertices are given in [404], together with their eigenvalues.

n	3	4	5	6	7	8	9	10
$N_T(n)$	2	3	7	16	54	243	2038	33120

13.2 Two-Graphs from Trees

13.12 Construction [417]

1. Let T be a tree with edge set E and let Δ be the set of 3-subsets of E not contained in paths in T. Then (E, Δ) is a two-graph.

2. Let X be the end vertices of a reduced vertex-2-colored (black and white) tree T (no divalent vertices) and let Δ comprise the triples of X whose vertices are pairwise joined by paths that meet in a black vertex. Then (X, Δ) is a two-graph. Use of the color white yields the complementary two-graph.

13.13 A two-graph Ω contains a graph Γ as an *induced substructure* if Γ is a subgraph of some graph in the switching class of Ω.

13.14 Theorem [417] A two-graph arises from a tree by Construction 13.12(1) if and only if the two-graph contains neither the pentagon nor the hexagon as an induced substructure. Only isomorphic trees yield isomorphic two-graphs.

13.15 Theorem [417] A two-graph arises from a tree by Construction 13.12(2) if and only if the two-graph does not contain the pentagon as an induced substructure. Only isomorphic colored reduced trees yield isomorphic two-graphs.

13.16 Remark Ishihara [1171] gives an alternative proof to Cameron's Theorem 13.15.

13.17 Remark Cameron [418] produces formulae for the numbers of labeled and labeled reduced two-graphs obtained by Construction 13.12. His proofs use various enumeration results for trees.

13.3 Groups Represented by Two-Graphs

13.18 Let $\Gamma = (V, E)$ be a graph with vertex set V. *The Coxeter group* of Γ, $\mathrm{Cox}(\Gamma)$ has a generator s_v for each $v \in V$ and defining relations $s_v^2 = 1, (s_v s_w)^3 = 1$ if $v \sim w$, and $(s_v s_w)^2 = 1$ if $v \not\sim w$. The set of all products of generators of even length forms a normal subgroup of index 2, denoted by $\mathrm{Cox}^+(\Gamma)$ [611]. Analogously [1876], the *Tsaranov group* of Γ has generators $t_v, v \in V$ and is given by
$$\mathrm{Ts}(\Gamma) := \langle t_v, v \in V \,:\, t_v^3 = 1,\ (t_v t_w^{-1})^2 = 1 \text{ if } v \sim w,\ (t_v t_w)^2 = 1 \text{ if } v \not\sim w \rangle.$$

13.19 Remark Switching Γ with respect to a set of vertices corresponds to replacing Tsaranov's generators for these vertices by their inverses. It follows that the Tsaranov group is an invariant of the two-graph (V, Δ) corresponding to the switching class of Γ. Thus, isomorphic two-graphs have isomorphic Tsaranov groups.

13.20 Theorem [1876] The group $\mathrm{Ts}(\Delta)$ of the two-graph (V, Δ) is finite if and only if its smallest eigenvalue is greater than -3. If this is the case, then $\mathrm{Ts}(\Delta) \cong \mathrm{Cox}^+(\Pi)$, where Π is a "Coxeter–Dynkin graph" of type A, D, or E.

13.21 Remark All two-graphs with smallest eigenvalue greater than -3 are identified in [1876].

13.22 Theorem [1876] Let $\Delta(T)$ be the two-graph arising from a tree T by means of Construction 13.12(1). Then $\mathrm{Ts}(\Delta(T)) \cong \mathrm{Cox}^+(T)$.

13.4 Regular Two-Graphs

13.23 Theorem Suppose the graph $\Gamma = (V, E)$ on n vertices has ∓ 1 adjacency matrix A with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_d$ and $-\rho$ of multiplicity $n - d$. Then using the values of $\mathrm{trace}(A)$ and $\mathrm{trace}(A^2)$,
$$\rho^2(n - d) \le d(n - 1) \text{ with equality if and only if } \lambda_1 = \lambda_2 = \ldots = \lambda_d.$$

13.24 Equality in Theorem 13.23 is of particular interest for the two-graph with Γ in its switching class. The following two definitions are equivalent [1871]:

1. A two-graph (V, Δ) is *regular* if each pair of vertices in V is contained in the same number of triples of Δ.
2. A two-graph (V, Δ) is *regular* if and only if it has two distinct eigenvalues $\rho_1 > 0 > \rho_2$, say, where $\rho_1\rho_2 = 1 - |V|$. The set $\{\rho_1, \rho_2\}$ is the *spectrum* of the two-graph.

13.25 Remark The switching class of a graph Γ, and hence any two-graph, can be represented geometrically as a set of *equiangular lines* [2088]. Let $-\rho = \lambda_{\min}$ be the smallest eigenvalue of the ∓ 1 adjacency matrix A of Γ (on n vertices) and suppose still that $-\rho$ has multiplicity $n - d$. Then $\rho I + A$ is positive semi-definite of rank d and so can be represented as the Gram matrix of the inner products of n vectors in euclidean d-space. Because these vectors have the same norm $\sqrt{\rho}$ and mutual inner products ± 1, any pair of the n lines spanned by them has the same angle ϕ with $\cos\phi = 1/\rho$. Conversely, given a set of n nonorthogonal equiangular lines in euclidean d-space there exists a two-graph from which it can be constructed by this method [1871]. Thus, from Theorem 13.23, the maximum cardinality n of such a set satisfies $n \le d(\rho^2-1)/(\rho^2-d)$ and this bound is achieved if and only if the corresponding two-graph is regular.

13.26 Remark In a regular two-graph with n vertices, the eigenvalues ρ_1 and ρ_2 are odd integers except possibly when $\rho_1 + \rho_2 = 0$. In this latter case the ∓ 1 adjacency matrix A of any graph in the switching class of the regular two-graph satisfies $A^2 = (n-1)I$ (the conference two-graph [1871]).

13.27 Theorem [1871] Suppose that (V, Δ) is a regular two-graph with spectrum $\{\rho_1, \rho_2\}$ and let $\Gamma = (V, E)$ be any graph in its switching class with an isolated vertex $v \in V$. Then $(V \setminus \{v\}, E)$ is a strongly regular graph (§VII.11) with Seidel spectrum (the eigenvalues of the ∓ 1 adjacency matrix) $\{\rho_0, \rho_1, \rho_2\}$, where $\rho_0 = \rho_1 + \rho_2$. This graph is a *descendant* of the two-graph.

13.28 Remark In the opposite direction, if Γ is a strongly regular graph (see §VII.11) with parameters (v, k, λ, μ), then the graph obtained from Γ by adjoining an isolated vertex belongs to the switching class of a regular two-graph if and only if $k = 2\mu$ [1871].

13.29 Theorem [1871] Given ρ_2 there are only finitely many possible ρ_1 such that there exists a regular two-graph with spectrum $\{\rho_1, \rho_2\}$ [1871].

13.30 Table The only possible spectra for regular two-graphs with $\rho_2 = -3$ or -5.

$-\rho_2$	3	3	3	3	3	5	5	5	5	5	5	5	5	5	5
ρ_1	1	3	5	9	21	1	3	5	7	15	19	25	35	55	115
n	4	10	16	28	64	6	16	26	36	76	96	126	176	276	576

13.31 Remark Of the pairs (ρ_1, ρ_2) listed in Table 13.30, it is known that $(21, -3)$ and $(115, -5)$ are impossible [1871] while the only ones remaining open are $(15, -5)$ and $(19, -5)$.

▷ Conference Two-Graphs

13.32 A *C-matrix* of order n is a square matrix C with zero diagonal and off-diagonal entries ± 1, such that $C^2 = (n-1)I$. C-matrices are essentially symmetric or skew according as $n \equiv 2$ or $0 \pmod 4$ [675]. Symmetric C-matrices (the ones of interest here) are *conference* matrices.

13.33 Remark Conference matrices are discussed in §V.2.

13.34 Theorem A conference matrix of order n is in the switching class of a regular two-graph with eigenvalues $\rho_1 = \sqrt{n-1}, \rho_2 = -\sqrt{n-1}$. The two-graph is a *conference* two-graph.

13.35 Theorem [1871] Necessary conditions for the existence of a conference two-graph with eigenvalues ρ_1, ρ_2 such that $\rho_1 + \rho_2 = 0$ are that $\rho_1^2 \equiv 1 \pmod 4$, and ρ_1^2 is a sum of squares of integers.

13.36 Theorem [1713] If $q \equiv 1 \pmod 4$ is a prime power, then there exists a conference two-graph of order $q+1$ (the Paley two-graph).

13.37 Theorem [2079] If a conference two-graph of order $m+1$ exists, then there also exists a conference two-graph of order $m^d + 1$ for all $d \geq 1$.

13.38 Theorem [1535] If $q = 4t - 1$ is a prime power and $p + 1 = 4t + 2$ is the order of a conference two-graph, then there exists a conference two-graph on $pq^2 + 1$ vertices.

13.39 Remark There are two further infinite families of conference two-graphs, known as the Möbius and Minkowski two-graphs, which are constructed in the setting of Möbius and Minkowski geometry (see [1875, 2139]). The Möbius two-graphs are isomorphic to the Paley two-graphs.

13.40 Construction (*Minkowski two-graphs* [1871]) Let $V = V(2, q)$ be the vector space of dimension 2 over $\mathbb{F}_q$, where q is an odd prime power. Suppose that the one-dimensional subspaces of V are partitioned into two disjoint sets P and N of equal size $(q+1)/2$. Then $(V \cup \{\infty\}, \Delta)$, where Δ comprises the set of triples $\{\infty, x, y\}$, with $x, y \in V$, such that $\langle x - y \rangle \in P$ is a self-complementary conference two-graph on $q^2 + 1$ vertices.

13.41 Remark The switching class of a two-graph from Construction 13.40 contains strongly regular graphs of degrees $q(q-1)/2$ and $q(q+1)/2$.

13.42 Theorem [1871] If there exist s mutually orthogonal latin squares of order $2s - 1$ or there exists a 2-$(2s^2 - 2s + 1, s, 1)$ design, then there exists a conference two-graph on $(2s-1)^2 + 1$ vertices.

▷ Symplectic and Orthogonal Two-Graphs

13.43

1. [1871] Let $V = V(2m, 2)$ denote the vector space of dimension $2m$ over $\mathbb{F}_2$ and let $B : V \times V \to \mathbb{F}_2$ be a nondegenerate, alternating bilinear form. The *symplectic* two-graph $\Sigma(2m, 2) = (V, \Delta)$ consists of the set V and the set $\Delta = \{\{u, v, w\} \subseteq V \ : \ u, v, w \text{ are distinct and } B(u, v) + B(v, w) + B(w, u) = 0\}$. Its eigenvalues are $\rho_1 = 1 + 2^m, \rho_2 = 1 - 2^m$.
2. [1871] There are essentially two quadratic forms on $V(2m, 2)$ defined by $Q^+(x) = x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m}$ and $Q^-(x) = x_1^2 + x_2^2 + x_1x_2 + \cdots + x_{2m-1}x_{2m}$. The *orthogonal* two-graph $\Omega^\epsilon(2m, 2)$, $\epsilon = \pm$, consists of the set of points $\Omega^\epsilon := \{x \in V \mid Q^\epsilon(x) = 0\}$, and the set of triples of distinct $u, v, w \in \Omega^\epsilon$ such that $B(u, v) + B(v, w) + B(w, u) = 0$. $\Omega^+(2m, 2)$ has eigenvalues $\rho_1 = 1 + 2^{m-1}, \rho_2 = 1 - 2^m$ and $\Omega^-(2m, 2)$ has eigenvalues $\rho_1 = 1 + 2^m, \rho_2 = 1 - 2^{m-1}$.

13.44 Remark [2007] The automorphism group of $\Omega^\epsilon(2m, 2)$ is the symplectic group, while $\Sigma(2m, 2)$ has automorphism group the symplectic group extended by the translations of $V(2m, 2)$. See §VII.9.

▷ Unitary Two-Graphs

13.45 Let H be a nondegenerate hermitian form on the projective plane $\mathrm{PG}(2, q^2)$, where q is an odd prime power, and let $U = \{x \mid H(x,x) = 0\}$ be the corresponding unital. Then $\mid U \mid = q^3 + 1$. The *unitary* two-graph $U(q) = (U, \Delta)$ consists of the set Δ of triples $\{x, y, z\}$, with $x, y, z \in U$, for which $H(x,y)H(y,z)H(z,x)$ is a square or nonsquare according as $q \equiv \mp 1 \pmod 4$. The Unitary group $\mathrm{P\Gamma U}(3, q^2)$ acts 2-transitively on Ω.

13.46 Proposition The eigenvalues of $U(q)$ are $\rho_1 = q^2, \rho_2 = -q$ [2007]. Its switching class contains a strongly regular graph of degree $q(q^2+1)/2$.

13.47 Remark Taylor [2006] proved that the automorphism group of $U(5)$ is $P\Gamma U(3, 5^2)$.

▷ Two Sporadic Regular Two-Graphs

13.48 Construction There is a unique 4-design with parameters 4-$(23, 7, 1)$ (it is a Witt design). Its residual design, a 3-$(22, 7, 4)$ design, is also unique. In each of these two designs distinct blocks meet in one or three points. The residual design has 176 blocks and its point-block incidence matrix M satisfies $MM^t = 40I + 16J$, $MJ = 56J$, $JM = 7J$. The eigenvalues of MM^t are 392 and 40, and hence, M^tM has eigenvalues $392, 40, 0$. Thus $A := M^tM - 5I - 2J$, a symmetric matrix of order 176 with zero diagonal and elements ± 1 elsewhere, has eigenvalues 35 and -5. It is therefore the adjacency matrix of a graph in the switching class of a regular two-graph on 176 vertices.

13.49 Construction If N is the point-block incidence matrix of the 4-$(23, 7, 1)$ design, then $NN^t = 56I + 21J$, $NJ = 77J$, $JN = 7J$. N^tN has eigenvalues $539, 56, 0$ and those of $B := N^tN - 5I - 2J$ are $28, 51, -5$. Hence, B satisfies $(B - 51I)(B + 5I) = -3J$, $BJ = 28J$, $NB = 51N - 7J$. A straightforward calculation shows that the symmetric matrix C of order 276, with zero diagonal and ± 1 elsewhere, given by $C = \begin{bmatrix} J - I & J - 2N \\ J - 2N^t & B \end{bmatrix}$ satisfies $(C - 55I)(C + 5I) = 0$ and, hence, is in the switching class of a regular two-graph on 276 vertices. This two-graph is unique [921].

▷ Symmetric Hadamard Matrices of Order 36

13.50 Remark Let E be the adjacency matrix of any graph in the switching class of a regular two-graph on 36 vertices. By complementation, if necessary, it may be assumed that the two-graph, and hence E, has eigenvalues 5 and -7, so that $(E - 5I)(E + 7I) = 0$. If $H := E + I$, then H is a symmetric Hadamard matrix of order 36 with constant diagonal (see §V.1). In [404] 91 such regular two-graphs are constructed, 11 from latin squares of order 6 and 80 from Steiner triple systems of order 15 (see also [920]). A further 136 were found using a computer and a backtracking algorithm [1944]. Subsequently, it was shown in [1577] that the $91 + 136 = 227$ regular two-graphs found in [404, 1944] make up the complete set. Many of these new two-graphs, and some of the older ones, have a particular shape. The corresponding Hadamard matrices contain, as a principal sub-matrix, the matrix A of order 20 defined by $A = \begin{bmatrix} I + P & I - P \\ I - P & I + P \end{bmatrix}$, where P is the ∓ 1 adjacency matrix of the Petersen graph. Assume this to be the case. Then for $\begin{bmatrix} A & N \\ N^t & B \end{bmatrix}$ to be a Hadamard matrix of order

36, it is necessary that $N = \begin{bmatrix} M \\ M \end{bmatrix}$, where M is of size 10×16 and is determined by Theorem 13.51.

13.51 Theorem [1944] There exist diagonal ± 1 matrices D_1, D_2 such that $M = D_1 \begin{bmatrix} C & \mathbf{j} \end{bmatrix} D_2$, where C is the ± 1 incidence matrix of a 2-$(10, 4, 2)$ design (Table II.1.25). Conversely, let C be the ± 1 incidence matrix of a 2-$(10, 4, 2)$ design and suppose that D_1 and D_2 are diagonal matrices of order 10, 16, respectively. If $M = D_1 \begin{bmatrix} C & \mathbf{j} \end{bmatrix} D_2$, and $B = 6I - \frac{1}{2}M^t M$, then $B - I$ is in the switching class of a regular two-graph of size 16,

$$H = \begin{bmatrix} I+P & I-P & M \\ I-P & I+P & M \\ M^t & M^t & B \end{bmatrix},$$

a symmetric Hadamard matrix of order 36 and $H - I$ is in the switching class of a regular two-graph on 36 vertices.

13.52 Remark There are three nonisomorphic 2-$(10, 4, 2)$ designs and each of them yields regular two-graphs on 36 vertices. In total 100 nonisomorphic regular two-graphs of order 36 are characterized by this method. See [1944] for the details.

13.53 Remark Grishukhin [972] investigated two-graphs from the even unimodular lattice $E_8 \oplus E_8$ and produced a further characterization of these 100 two-graphs.

▷ Completely Regular Two-Graphs

13.54 A regular two-graph is *completely regular* if, for all k, every k-clique is in a constant number α_k of $(k+1)$-cliques.

13.55 Theorem There are unique completely regular two-graphs on 10, 16, 28, 36, and 276 vertices. No others exist except possibly on 1128 or 3160 vertices.

13.56 Remark Neumaier [1673] allowed the further possibilities of 96, 288, and 640 vertices. These were shown subsequently not to exist [284, 287].

▷ Two-Graph Geometries

13.57 Theorem In a regular two-graph with eigenvalues $\rho_1 > \rho_2$, the maximum size of a clique c is given in terms of the smaller eigenvalue ρ_2 by $|c| \leq 1 - \rho_2$ [1873].

13.58 A *maximal* clique is one in which this upper bound of Theorem 13.57 is achieved.

13.59 A *two-graph geometry* is a set C of maximal cliques in a regular two-graph (V, Δ), such that each triple from Δ is in a unique clique from C.

13.60 Examples [1006]

1. In a regular two-graph, every odd triple is contained in $1 - \frac{1}{4}(\rho_1 + 3)(\rho_2 + 3)$ 4-cliques. When $\rho_2 = -3$, this number equals 1, and these cliques are maximal. Thus, by taking C to be the set of all 4-cliques, three two-graph geometries are obtained corresponding to the three regular two-graphs on 10, 16, and 28 vertices.
2. The known regular two-graph on 176 vertices has the Higman–Sims group acting as a 2-transitive group of automorphisms [2007] (see §VII.9). The subgroup M_{22} has an orbit C of size 18480 acting on the maximal 6-cliques of the two-graph and every odd triple is contained in exactly one 6-clique.

▷ Two-Graphs and Geometry

13.61 Remark Gunawardena and Moorhouse [994] associate a two-graph with an ovoid in finite orthogonal spaces of type $O_{2n+1}(q)$ (assuming one exists) and show that it is regular. See also [993].

▷ Numerical Data

13.62 Table Data concerning the known regular two-graphs with eigenvalues ρ_1 and $\rho_2 = -3, -5$ and the conference two-graphs on ≤ 50 vertices. N is the number of known nonisomorphic two-graphs on n vertices and N^* indicates that no further two-graphs on n vertices can exist. The main reference is [404]. For $n = 30, 36$, and 38, see also [1577, 1944]. In the cases $n = 46, 50$ additional work by Mathon [1538] improved $N(46)$ to 97 and $N(50)$ to 19. A further 24 regular two-graphs on 50 vertices were found as a result of the discovery of 12 new Steiner systems $S(2, 4, 25)$ [1339] (see Theorem 13.42), and seven more were found by the author, thus increasing $N(50)$ to 50. The case $n = 126$ corresponds to $U(5)$ and $n = 176, 276$ are the two sporadic two-graphs described in Constructions 13.48 and 13.49.

n	6	10	14	16	18	26	28	30
ρ_1, ρ_2	$\pm\sqrt{5}$	± 3	$\pm\sqrt{13}$	$5, -3$	$\pm\sqrt{17}$	± 5	$9, -3$	$\pm\sqrt{29}$
N	1^*	1^*	1^*	1^*	1^*	4^*	1^*	6^*
n	36	38	42	46	50	126	176	276
ρ_1, ρ_2	$7, -5$	$\pm\sqrt{37}$	$\pm\sqrt{41}$	$\pm\sqrt{45}$	± 7	$25, -5$	$35, -5$	$55, -5$
N	227^*	191	18	97	50	1	1	1^*

13.63 Remark It can happen that the switching class of a regular two-graph itself contains strongly regular graphs. There are five values of $n \leq 50$ for which this is possible, namely, $n = 10, 16, 26, 36$, and 50. The numbers of such graphs are listed, together with the numbers of nonisomorphic descendants. Here $|(n, \rho_0, \rho_1, \rho_2)|$ denotes the number of strongly regular graphs on n vertices with Seidel spectrum ρ_0, ρ_1, ρ_2.

n	10	16	26	36	50
ρ_1, ρ_2	$(3, -3)$	$(5, -3)$	$(5, -5)$	$(7, -5)$	$(7, -7)$
$\lvert(n-1, \rho_1+\rho_2, \rho_1, \rho_2)\rvert$	1	1	15	3854	312
$\lvert(n, \rho_1, \rho_1, \rho_2)\rvert$	1	1	10	180	1482
$\lvert(n, \rho_2, \rho_1, \rho_2)\rvert$	1	2	10	32548	1482

See Also

§II.4	t-designs are used in Constructions 13.48 and 13.49.
§III.3	MOLS are used in Theorem 13.42.
§V.1	Hadamard matrices are used to construct regular two-graphs (Remark 13.50).
§V.6	Conference matrices are used to construct conference two-graphs (Theorem 13.34).
§VII.11	Strongly regular graphs arise in the switching classes of some two-graphs (Remark 13.41).

References Cited: [284, 287, 404, 417, 418, 611, 675, 920, 921, 972, 993, 994, 1006, 1171, 1339, 1517, 1535, 1538, 1577, 1673, 1713, 1871, 1873, 1875, 1876, 1944, 2006, 2007, 2079, 2088, 2139]

Bibliography

The last entry of each item (in angle brackets) enumerates the page numbers on which the item is cited (unfortunately, it may in fact appear on the subsequent page instead).

[1] R. J. R. Abel, *Forty-three balanced incomplete block designs*, J. Combin. Theory A 65 (1994) 252–267. ⟨37, 38, 39, 40, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 53, 54, 55, 56, 409⟩

[2] ——, *On the Existence of Balanced Incomplete Block Designs and Transversal Designs*, PhD thesis, University of New South Wales, 1995. ⟨40, 41, 48, 56, 165, 170, 171, 175⟩

[3] ——, *Some new BIBDs with* $\lambda = 1$ *and* $6 \leq k \leq 10$, J. Combin. Des. 4 (1996) 27–50. ⟨72⟩

[4] ——, *Some new BIBDs with block size* 7, J. Combin. Des. 8 (2000) 146–150. ⟨50, 72, 405⟩

[5] ——, *Some new matrix-minus-diagonal* $V(11, t)$ *vectors*, J. Combin. Des. 11 (2003) 304–306. ⟨417⟩

[6] ——, *V(12,t) vectors and other designs from difference and quasi-difference matrices*, preprint (2006). ⟨165, 166, 167, 168, 169, 170, 220, 417⟩

[7] ——, *Some new near resolvable BIBDs with* $k = 7$ *and resolvable BIBDs with* $k = 5$, Australas. J. Combin. (to appear). ⟨127⟩

[8] R. J. R. Abel and A. M. Assaf, *Modified group divisible designs with block size* 5 *and* $\lambda = 1$, Discrete Math. 256 (2002) 1–22. ⟨260⟩

[9] R. J. R. Abel, A. M. Assaf, F. E. Bennett, I. Bluskov, and M. Greig, *Pair covering designs with block size* 5, preprint. ⟨372⟩

[10] R. J. R. Abel and F. E. Bennett, *The existence of* 2*-SOLSSOMs*, in Designs 2002, W. D. Wallis, ed., Kluwer, Boston, 2003, 1–21. ⟨169, 218⟩

[11] ——, *Quintessential PBDs and PBDs with prime power block sizes* $\geq$ 8, J. Combin. Des. 13 (2005) 239–267. ⟨251, 252, 253, 254⟩

[12] ——, *The existence of* $(v, 6, \lambda)$ *perfect Mendelsohn designs with* $\lambda > 1$, Des. Codes Crypt. 40 (2006) 211–224. ⟨531, 532⟩

[13] R. J. R. Abel, F. E. Bennett, and G. Ge, *Almost resolvable perfect Mendelsohn designs with block size* 5, Discrete Appl. Math. 116 (2002) 1–15. ⟨210, 531, 532⟩

[14] ——, *The existence of four HMOLS with equal sized holes*, Des. Codes Crypt. 26 (2002) 7–31. ⟨210⟩

[15] ——, *Resolvable perfect Mendelsohn designs with block size five*, Discrete Math. 247 (2002) 1–12. ⟨532⟩

[16] R. J. R. Abel, F. E. Bennett, and H. Zhang, *Perfect Mendelsohn designs with block size six*, J. Stat. Plann. Infer. 86 (2000) 287–319. ⟨531⟩

[17] R. J. R. Abel, F. E. Bennett, H. Zhang, and L. Zhu, *A few more incomplete self-orthogonal latin squares and related designs*, Australas. J. Combin. 21 (2000) 85–94. ⟨216⟩

[18] R. J. R. Abel, I. Bluskov, J. de Heer, and M. Greig, *Pair covering and other designs with block size* 6, preprint. ⟨54, 55, 253, 254⟩

[19] R. J. R. Abel, I. Bluskov, and M. Greig, *Balanced incomplete block designs with block size* 8, J. Combin. Des. 9 (2001) 233–268. ⟨43, 55, 72, 237, 245, 254⟩

[20] ——, *Balanced incomplete block designs with block size* 9 *and* $\lambda = 2, 4, 8$, Des. Codes Crypt. 26 (2002) 33–59. ⟨72⟩

[21] ——, *Balanced incomplete block designs with block size* 9. *II*, Discrete Math. 279 (2004) 5–32. ⟨40, 54, 72, 220⟩

[22] ——, *Balanced incomplete block designs with block size* 9. *III*, Australas. J. Combin. 30 (2004) 57–73. ⟨50, 72, 220⟩

[23] R. J. R. Abel and M. Buratti, *Some progress on* $(v, 4, 1)$ *difference families and optical orthogonal codes*, J. Combin. Theory A 106 (2004) 59–75. ⟨250, 251, 322, 397, 400, 556⟩

[24] R. J. R. Abel, M. Buratti, M. Greig, and Y. Miao, *Constructions for rotational near resolvable block designs*, J. Combin. Des. 9 (2001) 157–181. ⟨129, 263⟩

[25] R. J. R. Abel and N. J. Cavenagh, *Concerning eight mutually orthogonal latin squares*, J. Combin. Des. (to appear). ⟨169⟩

[26] R. J. R. Abel and Y. W. Cheng, *Some new MOLS of order* $2^n p$ *for* p *a prime power*, Australas. J. Combin. 10 (1994) 175–186. ⟨168, 171⟩

[27] R. J. R. Abel, C. J. Colbourn, and M. Wojtas, *Concerning seven and eight mutually orthogonal latin squares*, J. Combin. Des. 12 (2004) 123–131. ⟨166, 167, 170⟩

[28] R. J. R. Abel, C. J. Colbourn, J. X. Yin, and H. Zhang, *Existence of transversal designs with block size five and any index* λ, Des. Codes Crypt. 10 (1997) 275–307. ⟨209⟩

[29] R. J. R. Abel, D. Combe, and W. D. Palmer, *Generalized Bhaskar Rao designs and dihedral groups*, J. Combin. Theory A 106 (2004) 145–157. ⟨299⟩

[30] R. J. R. Abel, S. Costa, and N. J. Finizio, *Directed-ordered whist tournaments and* $(v, 5, 1)$ *difference families: Existence results and some new classes of* $\mathbb{Z}$*-cyclic solutions*, Discrete Appl. Math. 143 (2004) 43–53. ⟨216, 397, 400, 666, 667⟩

[31] R. J. R. Abel, S. Costa, N. J. Finizio, and M. Greig, $(2, 10)$ *GWhD*$(10n+1)$*—Existence results*, J. Combin. Math. Combin. Comput. (to appear). ⟨262⟩

[32] R. J. R. Abel, N. J. Finizio, G. Ge, and M. Greig, *New* $\mathbb{Z}$*-cyclic triplewhist frames and triplewhist tournament designs*, Discrete Appl. Math. 154 (2006) 1649–1673. ⟨346, 666⟩

[33] R. J. R. Abel, N. J. Finizio, and M. Greig, $(3, 6)$ GWhD(v)*—Existence results*, Discrete Math. 261 (2003) 3–26. ⟨45, 668⟩

[34] R. J. R. Abel, N. J. Finizio, M. Greig, and S. J. Lewis, *Pitch tournament designs and other BIBDs—Existence results for the case* $v = 8n + 1$, Congr. Numer. 138 (1999) 175–192. ⟨72, 127, 668⟩

[35] ——, $(2, 6)$ GWhD(v)*—Existence results and some* $\mathbb{Z}$*-cyclic solutions*, Congr. Numer. 144 (2000) 5–39. ⟨668⟩

[36] ——, *Pitch tournament designs and other BIBDs—Existence results for the case* $v = 8n$, J. Combin. Des. 9 (2001) 334–356. ⟨127, 668⟩

[37] ——, *Generalized whist tournament designs*, Discrete Math. 268 (2003) 1–19. ⟨537, 540, 668⟩

[38] R. J. R. Abel and G. Ge, *Some difference matrix constructions and an almost completion for the existence of triplewhist tournaments TWh*(v), Europ. J. Combin. 26 (2005) 1094–1104. ⟨167, 168, 169, 216, 407, 665, 666⟩

[39] R. J. R. Abel, G. Ge, M. Greig, and A. C. H. Ling, *Further results on* $(v, \{5, w^*\}, 1)$*-PBDs*, preprint. ⟨233, 258⟩

[40] R. J. R. Abel, G. Ge, M. Greig, and L. Zhu, *Resolvable BIBDs with a block size of* 5, J. Stat. Plann. Infer. 95 (2001) 49–65. ⟨127⟩

[41] R. J. R. Abel and M. Greig, *Some new* $(v, 5, 1)$ *RBIBDs and PBDs with block sizes* $\equiv 1$ *(mod* 5*)*, Australas. J. Combin. 15 (1997) 177–202. ⟨43, 51, 53, 72, 127, 253, 254⟩

[42] ——, *Balanced incomplete block designs with block size* 7, Des. Codes Crypt. 13 (1998) 5–30. ⟨72, 245, 246⟩

[43] R. J. R. Abel, M. Greig, Y. Miao, and L. Zhu, *Resolvable BIBDs with block size* 7 *and index* 6, Discrete Math. 261 (2003) 3–26. ⟨49, 127⟩

[44] R. J. R. Abel, M. Greig, and D. H. Rees, *Existence of OBIBDs with* $k = 4$ *with and without nesting*, Discrete Math. 266 (2003) 3–36. ⟨252, 254⟩

[45] R. J. R. Abel, E. R. Lamken, and J. Wang, *A few more Kirkman squares and doubly near resolvable BIBDs with block size* 3, preprint (2006). ⟨130, 131⟩
[46] R. J. R. Abel and W. H. Mills, *Some new BIBDs with $k = 6$ and $\lambda = 1$*, J. Combin. Des. 3 (1995) 381–391. ⟨49, 72⟩
[47] R. J. R. Abel and D. T. Todorov, *Four MOLS of order* 20, 30, 38 *and* 44, J. Combin. Theory A 64 (1994) 144–148. ⟨165, 166, 167⟩
[48] R. J. R. Abel and H. Zhang, *Direct constructions for certain types of HMOLS*, Discrete Math. 181 (1998) 1–17. ⟨210⟩
[49] R. J. R. Abel, H. Zhang, and X. Zhang, *Three mutually orthogonal idempotent latin squares of orders* 22 *and* 26, J. Stat. Plann. Infer. 51 (1996) 101–106. ⟨165⟩
[50] J. Abrham, *Exponential lower bounds for the number of Skolem and extremal Langford sequences*, Ars Combin. 22 (1986) 187–198. ⟨615⟩
[51] J. Abrham and A. Kotzig, *Skolem sequences and additive permutations*, Discrete Math. 37 (1981) 143–146. ⟨613, 615⟩
[52] O. A. AbuGhneim, *On nonabelian McFarland difference sets*, Congr. Numer. 168 (2004) 159–175. ⟨426⟩
[53] I. Adamczak, D. L. Kreher, A. C. H. Ling, and R. S. Rees, *Further results on the maximum size of a hole in an incomplete t-wise balanced design with specified minimum block size*, J. Combin. Des. 10 (2002) 256–281. ⟨659⟩
[54] C. M. Adams and S. E. Tavares, *Designing S-boxes resistant to differential cryptanalysis*, in Proc. 3rd Symposium on the State and Progress of Research in Cryptography, 1993, 181–193. ⟨338⟩
[55] P. Adams and J. Appleton, *Various labelings of some small graphs*, preprint. ⟨485⟩
[56] P. Adams, E. J. Billington, D. E. Bryant, and S. I. El-Zanati, *On the Hamilton–Waterloo problem*, Graphs Combin. 18 (2002) 31–51. ⟨377⟩
[57] P. Adams and D. E. Bryant, *i-perfect m-cycle systems, $m \leq 19$*, Aequat. Math. 53 (1997) 275–294. ⟨378, 379⟩
[58] ———, *On the spectrum problem for some small graphs*, preprint (2005). ⟨481⟩
[59] ———, *Resolvable directed cycle systems of all indices for cycle lengths* 3 *and* 4, preprint (2005). ⟨378⟩
[60] ———, *Two-factorisations of complete graphs of orders fifteen and seventeen*, Australas. J. Combin. 35 (2006) 113–118. ⟨376, 377⟩
[61] P. Adams, D. E. Bryant, and S. I. El-Zanati, *Lambda-fold cube decompositions*, Australas. J. Combin. 11 (1995) 197–210. ⟨481⟩
[62] P. Adams, D. E. Bryant, and A. Khodkar, *On Alspach's conjecture with two even cycle lengths*, Discrete Math. 223 (2000) 1–12. ⟨374⟩
[63] P. Adams, D. E. Bryant, and B. M. Maenhaut, *Cube factorizations of complete graphs*, J. Combin. Des. 12 (2004) 381–388. ⟨481⟩
[64] B. Adhikary and P. Das, *Construction and combinatorial properties of orthogonal arrays with variable number of symbols in rows*, Lect. Notes Math. 885 (1980) 165–170. ⟨549⟩
[65] S. S. Agaian, *Hadamard Matrices and Their Applications*, Springer, Berlin, 1985. ⟨275⟩
[66] A. Aguado and S. I. El-Zanati, *On labeling the union of three cycles I; σ-labelings*, preprint. ⟨485⟩
[67] A. Aguado, S. I. El-Zanati, H. Hake, J. Stob, and H. Yayla, *On labeling the union of three cycles II; ρ-labelings*, preprint. ⟨485⟩
[68] W. Ahrens, *Mathematische Unterhaltungen und Spiele*, B.G. Teubner, Leipzig, 1901. (2. Aufl., B.G. Teubner, Leipzig, 1918) 2. Band, Kap. XIV: Anordnungsprobleme. ⟨11⟩
[69] S. Ajoodani-Namini, *Extending large sets of t-designs*, J. Combin. Theory A 76 (1996) 139–144. ⟨99⟩
[70] ———, *All block designs with $b = \binom{v}{k}/2$ exist*, Discrete Math. 179 (1998) 27–35. ⟨99⟩
[71] S. Ajoodani-Namini and G. B. Khosrovshahi, *More on halving the complete designs*, Discrete Math. 135 (1994) 29–37. ⟨98, 99⟩

[72] S. Akbari, H. R. Maimani, and C. Maysoori, *Minimal defining sets for full 2-$(v, 3, v-2)$ designs*, Australas. J. Combin. 23 (2001) 5–8. ⟨385⟩
[73] A. A. Albert, *Quasigroups. I*, Trans. Amer. Math. Soc. 54 (1943) 507–519. ⟨18⟩
[74] ———, *Quasigroups. II*, Trans. Amer. Math. Soc. 55 (1944) 401–419. ⟨18⟩
[75] W. O. Alltop, *An infinite class of 5-designs*, J. Combin. Theory A 12 (1972) 390–395. ⟨82⟩
[76] ———, *Extending t-designs*, J. Combin. Theory A 18 (1975) 177–186. ⟨81⟩
[77] N. Alon, L. Babai, and A. Itai, *A fast and simple randomized parallel algorithm for the maximal independent set problem*, J. Algorithms 7 (1986) 567–583. ⟨390⟩
[78] N. Alon, J.-H. Kim, and J. H. Spencer, *Nearly perfect matchings in regular simple hypergraphs*, Israel J. Math. 100 (1997) 171–187. ⟨67⟩
[79] N. Alon and J. H. Spencer, *The Probabilistic Method*, Wiley, New York, 1992. ⟨390⟩
[80] N. Alon and M. Tarsi, *Colorings and orientations of graphs*, Combinatorica 12 (1992) 125–134. ⟨151⟩
[81] B. Alspach, J.-C. Bermond, and D. Sotteau, *Decomposition into cycles I. Hamilton decompositions*, in Cycles and Rays, G. Hahn, G. Sabidussi, and R. E. Woodrow, eds., Kluwer, Dordrecht, 1990, 9–18. ⟨755⟩
[82] B. Alspach, D. Dyer, and D. L. Kreher, *On isomorphic factorizations of circulant graphs*, J. Combin. Des. 14 (2006) 406–414. ⟨485⟩
[83] B. Alspach, H. Gavlas, M. Šajna, and H. Verrall, *Cycle decompositions IV: Complete directed graphs and fixed length directed cycles*, J. Combin. Theory A 103 (2003) 165–208. ⟨374⟩
[84] B. Alspach, K. Heinrich, and G. Liu, *Orthogonal factorizations of graphs*, in [724], 1992, 13–40. ⟨590, 740, 755⟩
[85] L. D. Andersen and A. J. W. Hilton, *Symmetric latin square and complete graph analogues of the Evans conjecture*, J. Combin. Des. 2 (1994) 197–252. ⟨146⟩
[86] L. D. Andersen, A. J. W. Hilton, and C. A. Rodger, *A solution to the problem of embedding partial idempotent latin squares*, J. London Math. Soc. 26 (1982) 21–27. ⟨159⟩
[87] L. D. Andersen and C. A. Rodger, *Decompositions of complete graphs: Embedding partial edge-colourings and the method of amalgamations*, in Surveys in Combinatorics, 2003, C. D. Wensley, ed., Cambridge Univ. Press, Cambridge, 2003, 7–41. ⟨382⟩
[88] B. A. Anderson, *A fast method for sequencing low order non-Abelian groups*, Ann. Discrete Math. 34 (1987) 27–41. ⟨770⟩
[89] ———, *A family of $n \times n$ tuscan-2 squares with $n+1$ composite*, Ars Combin. 32 (1991) 33–55. ⟨656⟩
[90] B. A. Anderson, P. J. Schellenberg, and D. R. Stinson, *The existence of Howell designs of even side*, J. Combin. Theory A 36 (1984) 23–55. ⟨499, 504⟩
[91] D. A. Anderson and A. M. Thomas, *Resolution IV fractional factorial designs for the general asymmetric factorial*, Commun. Stat. Theory Methods 8 (1979) 931–943. ⟨451⟩
[92] I. Anderson, *Combinatorial Designs: Construction Methods*, Ellis Horwood, England, 1990. ⟨164, 219⟩
[93] ———, *A hundred years of whist tournaments*, J. Combin. Math. Combin. Comput. 19 (1995) 129–150. ⟨665, 668⟩
[94] ———, *Combinatorial Designs and Tournaments*, Clarendon Press, Oxford, 1997. ⟨664, 668⟩
[95] ———, *Balancing carry-over effects in tournaments*, in Combinatorial Designs and Their Applications, F. C. Holroyd, K. A. S. Quinn, C. Rowley, and B. S. Webb, eds., Chapman and Hall/CRC, Boca Raton FL, 1999, 1–16. ⟨592⟩
[96] ———, *Some cyclic and 1-rotational designs*, in Surveys in Combinatorics, 2001, J. W. P. Hirschfeld, ed., Cambridge Univ. Press, London, 2001, 47–73. ⟨410, 665, 666⟩

[97] I. Anderson and L. Ellison, *$\mathbb{Z}$-cyclic ordered triplewhist and directed triplewhist tournaments on p elements*, J. Combin. Math. Combin. Comput. 53 (2005) 39–48. ⟨667⟩

[98] I. Anderson and N. J. Finizio, *On the construction of directed triplewhist tournaments*, J. Combin. Math. Combin. Comput. 35 (2000) 107–115. ⟨666⟩

[99] ———, *Some new $\mathbb{Z}$-cyclic whist tournament designs*, Discrete Math. 293 (2005) 19–28. ⟨216, 665, 666⟩

[100] I. Anderson, N. J. Finizio, and P. A. Leonard, *New product theorems for $\mathbb{Z}$-cyclic whist tournaments*, J. Combin. Theory A 88 (1999) 162–166. ⟨665, 666⟩

[101] O. Anglada and J.-F. Maurras, *Another complete invariant for Steiner triple systems of order* 15, J. Combin. Des. 13 (2005) 388–391. ⟨779⟩

[102] R. Anstee, M. Hall Jr., and J. Thompson, *Planes of order* 10 *do not have a collineation of order* 5, J. Combin. Theory A 29 (1980) 39–58. ⟨690⟩

[103] R. R. Anstice, *On a problem in combinations*, Cambridge and Dublin Math. J. 7 (1852) 279–292. ⟨13⟩

[104] ———, *On a problem in combinations*, Cambridge and Dublin Math. J. 8 (1853) 149–154. ⟨13⟩

[105] K. Appel and W. Haken, *Every Planar Map is Four Colorable*, Amer. Math. Soc., Providence RI, 1989. ⟨741⟩

[106] D. Applegate, E. M. Rains, and N. J. A. Sloane, *On asymmetric coverings and covering numbers*, J. Combin. Des. 11 (2003) 218–228. ⟨762⟩

[107] K. T. Arasu, *Number theoretic consequences on the parameters of a symmetric design*, Discrete Math. 65 (1987) 1–4. ⟨111⟩

[108] K. T. Arasu and Y. Q. Chen, *A difference set in $(\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/5\mathbb{Z}$*, Des. Codes Crypt. 23 (2001) 317–323. ⟨435⟩

[109] K. T. Arasu, Y. Q. Chen, and A. Pott, *On abelian $2^{2m+1}(2^{m-1}+1), 2^m(2^m+1), 2^m)$-difference sets*, J. Combin. Theory A 113 (2006) 1120–1137. ⟨424⟩

[110] K. T. Arasu and S. L. Ma, *Abelian difference sets without self-conjugacy*, Des. Codes Crypt. 15 (1998) 223–230. ⟨435⟩

[111] K. T. Arasu and K. J. Player, *A new family of cyclic difference sets with Singer parameters in characteristic three*, Des. Codes Crypt. 28 (2003) 75–91. ⟨423⟩

[112] K. T. Arasu and S. K. Sehgal, *Some new difference sets*, J. Combin. Theory A 69 (1995) 170–172. ⟨427⟩

[113] J. Arkin, P. Smith, and E. G. Straus, *Euler's* 36 *officers problem in three dimensions—Solved*, J. Recreational Math. 15 (1982/83) 81–84. ⟨468⟩

[114] M. Aschbacher, *On collineation groups of symmetric block designs*, J. Combin. Theory A 11 (1971) 272–281. ⟨37, 112, 118⟩

[115] A. Ash, *Generalized Youden designs: Constructions and tables*, J. Stat. Plann. Infer. 5 (1981) 1–25. ⟨673, 674⟩

[116] A. M. Assaf, H. Alhalees, and L. P. S. Singh, *Directed covering with block size* 5 *and v even*, Australas. J. Combin. 28 (2003) 3–24. ⟨366, 444⟩

[117] A. M. Assaf, I. Bluskov, M. Greig, and N. Shalaby, *Block designs with block size* 5 *with higher index*, preprint. ⟨259, 551⟩

[118] A. M. Assaf, N. Shalaby, and J. X. Yin, *Directed packings with block size* 5, Australas. J. Combin. 17 (1998) 235–256. ⟨444⟩

[119] ———, *Directed packing and covering designs with block size four*, Discrete Math. 238 (2001) 3–17. ⟨444⟩

[120] E. F. Assmus Jr., *New* 5*-designs*, J. Combin. Theory 6 (1969) 122–151. ⟨87, 88⟩

[121] ———, *On* 2*-ranks of Steiner triple systems*, Electron. J. Comb. 2 (1995) Research Paper 9, approx. 35 pp.˙ ⟨691, 701⟩

[122] E. F. Assmus Jr. and J. D. Key, *Designs and Their Codes*, Cambridge Univ. Press, Cambridge, 1992. ⟨701⟩

[123] E. F. Assmus Jr. and H. F. Mattson Jr., *Coding and combinatorics*, SIAM Rev. 16 (1974) 349–388. ⟨680⟩

[124] E. F. Assmus Jr., J. A. Mezzaroba, and C. J. Salwach, *Planes and biplanes*, in Higher Combinatorics, M. Aigner, ed., Reidel, Dordrecht, 1977, 205–212. ⟨36⟩

[125] M. Atici, S. S. Magliveras, D. R. Stinson, and W. D. Wei, *Some recursive constructions for perfect hash families*, J. Combin. Des. 4 (1996) 353–363. ⟨567, 568⟩
[126] A. C. Atkinson and A. N. Donev, *Experimental designs optimally balanced for trend*, Technometrics 38 (1996) 333–341. ⟨449⟩
[127] A. H. Baartmans, I. F. Blake, and V. D. Tonchev, *On the extendability of Steiner t-designs*, J. Combin. Des. 1 (1993) 239–247. ⟨44⟩
[128] A. H. Baartmans, I. Bluskov, and V. D. Tonchev, *The Preparata codes and a class of* 4*-designs*, J. Combin. Des. 2 (1994) 167–170. ⟨84, 685⟩
[129] A. H. Baartmans, I. Landjev, and V. D. Tonchev, *On the binary codes of Steiner triple systems*, Des. Codes Crypt. 8 (1996) 29–43. ⟨691, 701⟩
[130] L. Babai, *Almost all Steiner triple systems are asymmetric*, Ann. Discrete Math. 7 (1980) 37–39. ⟨61⟩
[131] W. C. Babcock, *Intermodulation interference in radio systems*, Bell Syst. Tech. J. 31 (1953) 63–73. ⟨436⟩
[132] R. Bacher, *Cyclic difference sets with parameters* (511, 255, 127), Enseign. Math. (2) 40 (1994) 187–192. ⟨433⟩
[133] R. Baer, *Nets and groups*, Trans. Amer. Math. Soc. 46 (1939) 110–141. ⟨18⟩
[134] ———, *Nets and groups. II*, Trans. Amer. Math. Soc. 47 (1940) 435–439. ⟨18⟩
[135] S. Bagchi, A. C. Mukhopadhyay, and B. K. Sinha, *A search for optimal nested row-column designs*, Sankhyā B 52 (1990) 93–104. ⟨539⟩
[136] R. A. Bailey, *Factorial design and abelian groups*, Lin. Alg. Appl. 70 (1985) 349–368. ⟨465, 564⟩
[137] ———, *Association Schemes: Designed Experiments, Algebra and Combinatorics*, Cambridge Univ. Press, Cambridge, 2004. ⟨327, 330, 565⟩
[138] C. Baker, *Extended Skolem sequences*, J. Combin. Des. 3 (1995) 363–379. ⟨613⟩
[139] C. Baker and N. Shalaby, *Disjoint Skolem sequences and related disjoint structures*, J. Combin. Des. 1 (1993) 329–345. ⟨616⟩
[140] R. D. Baker, *Factorizations of Graphs*, PhD thesis, Ohio State University, 1975. ⟨216, 668⟩
[141] ———, *Whist tournaments*, Congr. Numer. 35 (1975) 89–100. ⟨664⟩
[142] ———, *An elliptic semiplane*, J. Combin. Theory A 25 (1978) 193–195. ⟨730⟩
[143] ———, *Quasigroups and tactical systems*, Aequat. Math. 18 (1978) 296–303. ⟨158⟩
[144] ———, *Resolvable BIBDs and SOLS*, Discrete Math. 44 (1983) 13–29. ⟨41, 47, 50, 125, 246, 263, 265⟩
[145] R. D. Baker and G. L. Ebert, *Elliptic semiplanes. II. Structure theory*, Ars Combin. 12 (1981) 147–164. ⟨730⟩
[146] K. Balasubramanian, *On transversals in latin squares*, Lin. Alg. Appl. 131 (1990) 125–129. ⟨143⟩
[147] D. J. Balding and D. C. Torney, *Optimal pooling designs with error detection*, J. Combin. Theory A 74 (1996) 131–140. ⟨631⟩
[148] ———, *The design of pooling experiments for screening a clone map*, Fungal Genetics and Biology 21 (1997) 302–307. ⟨575⟩
[149] P. Balister, *On the Alspach conjecture*, Combin. Probab. Comput. 10 (2001) 95–125. ⟨374⟩
[150] ———, *Packing circuits into* K_N, Combin. Probab. Comput. 10 (2001) 463–499. ⟨374⟩
[151] S. Ball, A. Blokhuis, and F. Mazzocca, *Maximal arcs in Desarguesian planes of odd order do not exist*, Combinatorica 17 (1997) 31–41. ⟨559⟩
[152] S. Ball and J. W. P. Hirschfeld, *Bounds on* (n, r)*-arcs and their application to linear codes*, Finite Fields Appl. 11 (2005) 326–336. ⟨713⟩
[153] W. W. R. Ball, *Mathematical Recreations and Essays*, Macmillan, London, 1892. ⟨22⟩
[154] W. W. R. Ball and H. S. M. Coxeter, *Mathematical Recreations and Essays*, University of Toronto Press, Toronto, 11th ed., 1938. 12th Edition: 1974. ⟨22, 525, 526, 527⟩
[155] E. Bannai, *On tight designs*, Quart. J. Math. Oxford 28 (1977) 433–448. ⟨329⟩

[156] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin Cummings, London, 1984. ⟨330⟩
[157] E. Bannai, A. Munemasa, and B. Venkov, *The nonexistence of certain tight spherical designs*, Algebra i Analiz 16 (2004) 1–23. ⟨620⟩
[158] Z. Baranyai, *On the factorizations of the complete uniform hypergraph*, in Finite and Infinite Sets, A. Hajnal, R. Rado, and V. T. Sós, eds., North-Holland, Amsterdam, 1975, 91–108. ⟨98, 99⟩
[159] E. Barbut and A. Bialostocki, *On regular r-tournaments*, Ars Combin. 34 (1992) 97–106. ⟨603, 604, 606⟩
[160] E. Barillot, B. Lacroix, and D. Cohen, *Theoretical analysis of library screening using a n-dimensional pooling strategy*, Nucl. Acids Res. 19 (1991) 6241–6247. ⟨575⟩
[161] J. A. Barrau, *Over drietalstelsels, in het bijzonder die van dertien elementen*, Kon. Akad. Wetensch. Amst. Verslag Wis-en Natuurk. Afd. 17 (1908) 274–279. ⟨17⟩
[162] L. A. Bassalygo, G. V. Zaĭcev, and V. A. Zinov′ev, *Uniformly close-packed codes*, Problemy Peredači Informacii 10 (1974) 9–14. ⟨684⟩
[163] J. A. Bate and G. H. J. Van Rees, *Lotto designs*, J. Combin. Math. Combin. Comput. 28 (1998) 15–39. ⟨514⟩
[164] L. M. Batten and A. Beutelspacher, *The Theory of Finite Linear Spaces*, Cambridge Univ. Press, Cambridge, 1993. ⟨270, 508, 509, 510, 511, 512⟩
[165] B. J. Battersby, D. E. Bryant, and C. A. Rodger, *Factorizations of complete multigraphs*, Australas. J. Combin. 16 (1997) 35–43. ⟨376⟩
[166] B. Baudelet and M. Sebille, *A generalization of a result of Tran Van Trung on t-designs*, J. Combin. Des. 7 (1999) 107–112. ⟨81⟩
[167] L. D. Baumert, *Cyclic Difference Sets*, Springer, Berlin, 1971. ⟨422, 423, 433, 435⟩
[168] L. D. Baumert and D. M. Gordon, *On the existence of cyclic difference sets with small parameters*, in High Primes and Misdemeanours, A. van der Poorten and A. Stein, eds., Amer. Math. Soc., Providence RI, 2004, 61–68. ⟨421, 425, 435⟩
[169] S. Bays, *Une question de Cayley relative au problème des triades de Steiner*, Enseignement Math. 19 (1917) 57–67. ⟨13⟩
[170] ———, *Sur les systèmes cycliques de triples de Steiner*, Ann. Sci. École Norm. Sup. (3) 40 (1923) 55–96. ⟨16⟩
[171] S. Bays and G. Belhôte, *Sur les systèmes cycliques de triples de Steiner différents pour N premier de la forme 6 n+1*, Comment. Math. Helv. 6 (1934) 28–46. ⟨16⟩
[172] S. Bays and E. de Weck, *Sur les systèmes de quadruples*, Comment. Math. Helv. 7 (1935) 222–241. ⟨16, 84⟩
[173] R. Beals, J. A. Gallian, P. Headley, and D. Jungreis, *Harmonious groups*, J. Combin. Theory A 56 (1991) 223–238. ⟨351⟩
[174] R. Bean, *The size of the smallest uniquely completable set in order 8 latin squares*, J. Combin. Math. Combin. Comput. 52 (2005) 159–168. ⟨147⟩
[175] J. K. Beard, K. Erickson, M. Monteleone, M. Wright, and J. C. Russo, *Combinatoric collaboration on Costas arrays and radar applications*, in Proceedings of the IEEE Radar Conference, IEEE, 2004, 260–265. ⟨360⟩
[176] M. Beck, M. Cohen, J. Cuomo, and P. Gribelyuk, *The number of "magic" squares, cubes, and hypercubes*, Amer. Math. Monthly 110 (2003) 707–717. ⟨528⟩
[177] J. H. Beder, *The problem of confounding in two-factor experiments*, Commun. Stat. Theory Methods 18 (1989) 2165–2188. ⟨465⟩
[178] D. Bedford, *Orthomorphisms and near orthomorphisms of groups and orthogonal latin squares: A survey*, Bull. Inst. Combin. Appl. 15 (1995) 13–33. ⟨352⟩
[179] H. Beker and W. H. Haemers, *2-designs having an intersection number $k-n$*, J. Combin. Theory A 28 (1980) 64–81. ⟨118⟩
[180] H. Beker and F. Piper, *Some designs which admit strong tactical decompositions*, J. Combin. Theory A 22 (1977) 38–42. ⟨38⟩
[181] V. Belevitch, *Theory of 2n-terminal networks with applications to conference telephony*, Elect. Commun. 27 (1950) 231–244. ⟨19⟩

[182] V. D. Belousov, *Parastrofno-Ortogonalnye Kvazigruppy*, Akad. Nauk Moldav. SSR Inst. Mat. s Vychisl. Tsentrom, Kishinev, 1983. English: *Parastrophic-orthogonal quasigroups*. Quasigroups Related Systems 13 (2005), 25–72. ⟨156⟩

[183] G. B. Belyavskaya and G. L. Mullen, *Orthogonal hypercubes and many-placed operations*, Quasigroups and Related Systems 13 (2005) 75–86. ⟨471⟩

[184] L. Bénéteau, *Free commutative Moufang loops and anticommutative graded rings*, J. Algebra 67 (1980) 1–35. ⟨849⟩

[185] ———, *Extended triple systems: geometric motivations and algebraic constructions*, Discrete Math. 208/209 (1999) 31–47. ⟨850⟩

[186] L. Bénéteau and J. Lacaze, *Symplectic trilinear forms and related designs and quasigroups*, Comm. Algebra 16 (1988) 1035–1051. ⟨499⟩

[187] B. T. Bennett and R. B. Potts, *Arrays and brooks*, J. Austral. Math. Soc. 7 (1967) 23–31. ⟨360⟩

[188] C. H. Bennett, G. Brassard, and J. M. Robert, *How to reduce your enemy's information*, Lect. Notes Comp. Sci. 218 (1986) 468–476. ⟨356, 357⟩

[189] F. E. Bennett, *On r-fold perfect Mendelsohn designs*, Ars Combin. 23 (1987) 57–68. ⟨253⟩

[190] ———, *Quasigroup identities and Mendelsohn designs*, Canad. J. Math. 77 (1989) 29–50. ⟨157, 158⟩

[191] ———, *The spectra of a variety of quasigroups and related combinatorial designs*, Discrete Math. 41 (1989) 341–368. ⟨153, 156, 157, 158⟩

[192] ———, *Concerning pairwise balanced designs with prime power block sizes*, in Finite Geometries and Combinatorial Designs, E. S. Kramer and S. S. Magliveras, eds., Amer. Math. Soc., Providence RI, 1990, 23–37. ⟨233, 250, 251, 253⟩

[193] ———, *A brief survey of perfect Mendelsohn packing and covering designs*, Discrete Appl. Math. 95 (1999) 73–81. ⟨534⟩

[194] ———, *Recent progress on the existence of perfect Mendelsohn designs*, J. Stat. Plann. Infer. 94 (2001) 121–138. ⟨531, 532, 534⟩

[195] F. E. Bennett, Y. X. Chang, G. Ge, and M. Greig, *Existence of* $(v, \{5, w^*\}, 1)$*-PBDs*, Discrete Math. 279 (2004) 61–105. ⟨233⟩

[196] F. E. Bennett, C. J. Colbourn, and R. C. Mullin, *Quintessential pairwise balanced designs*, J. Stat. Plann. Infer. 72 (1998) 15–66. ⟨251, 252⟩

[197] F. E. Bennett, C. J. Colbourn, and L. Zhu, *Existence of certain types of three HMOLS*, Discrete Math. 160 (1996) 49–65. ⟨210⟩

[198] F. E. Bennett, E. Mendelsohn, and N. S. Mendelsohn, *Resolvable perfect cyclic designs*, J. Combin. Theory A 29 (1980) 142–150. ⟨532⟩

[199] F. E. Bennett, N. Shalaby, and J. X. Yin, *Existence of directed GDDs with block size five*, J. Combin. Des. 6 (1998) 389–402. ⟨442⟩

[200] F. E. Bennett, R. Wei, J. X. Yin, and A. Mahmoodi, *Existence of DBIBDs with block size six*, Utilitas Math. 43 (1993) 205–217. ⟨442⟩

[201] F. E. Bennett, R. Wei, and L. Zhu, *Incomplete idempotent Schröder quasigroups and related packing designs*, Aequat. Math. 51 (1996) 100–114. ⟨157, 158, 214, 215⟩

[202] F. E. Bennett and J. X. Yin, *Packings and coverings of the complete directed multigraph with* 3- *and* 4*-circuits*, Discrete Math. 162 (1996) 23–29. ⟨533⟩

[203] ———, *Existence of HPMDs with block size five and index* $\lambda \geq 2$, J. Combin. Math. Combin. Comput. 37 (2001) 129–137. ⟨534⟩

[204] F. E. Bennett, J. X. Yin, H. Zhang, and R. J. R. Abel, *Perfect Mendelsohn packing designs with block size five*, Des. Codes Crypt. 14 (1998) 5–22. ⟨533⟩

[205] F. E. Bennett, J. X. Yin, and L. Zhu, *On the existence of perfect Mendelsohn designs with* $k = 7$ *and* λ *even*, Discrete Math. 113 (1993) 7–25. ⟨254⟩

[206] F. E. Bennett, H. Zhang, and L. Zhu, *Self-orthogonal Mendelsohn triple systems*, J. Combin. Theory A 73 (1996) 207–218. ⟨155, 215⟩

[207] F. E. Bennett and X. Zhang, *Resolvable Mendelsohn designs with block size* 4, Aequat. Math. 40 (1990) 248–260. ⟨531⟩

[208] F. E. Bennett and L. Zhu, *Conjugate orthogonal latin squares and related structures*, in [724], 1992, 41–96. ⟨153, 157, 158, 159, 253⟩
[209] ——, *Further results on the existence of HSOLSSOM(h^n)*, Australas. J. Combin. 14 (1996) 207–220. ⟨216, 218⟩
[210] ——, *The spectrum of HSOLSSOM(h^n) where h is even*, Discrete Math. 158 (1996) 11–25. ⟨216, 218⟩
[211] G. K. Bennett, M. J. Grannell, and T. S. Griggs, *Cyclic bi-embeddings of Steiner triple systems on $12s+7$ points*, J. Combin. Des. 10 (2002) 92–110. ⟨489⟩
[212] ——, *On the bi-embeddability of certain Steiner triple systems of order* 15, Europ. J. Combin. 23 (2002) 499–505. ⟨488⟩
[213] ——, *Exponential lower bounds for the numbers of Skolem-type sequences*, Ars Combin. 73 (2004) 101–106. ⟨615⟩
[214] ——, *Non-orientable biembeddings of Steiner triple systems of order* 15, Acta Math. Univ. Comenian. (N.S.) 73 (2004) 101–106. ⟨488⟩
[215] J. L. Bentley, *Writing Efficient Programs*, Prentice-Hall, Englewood Cliffs, 1982. ⟨781⟩
[216] E. R. Berlekamp, J. H. van Lint, and J. J. Seidel, *A strongly regular graph derived from the perfect ternary Golay code*, in A Survey of Combinatorial Theory, J. N. Srivastava, ed., North-Holland, Amsterdam, 1973, 25–30. ⟨864⟩
[217] J.-C. Bermond, L. Braud, and D. Coudert, *Traffic grooming on the path*, Lect. Notes Comp. Sci. 3499 (2005) 34–48. ⟨494⟩
[218] J.-C. Bermond and S. Ceroi, *Minimizing SONET ADMs in unidirectional WDM ring with grooming ratio 3*, Networks 41 (2003) 83–86. ⟨495⟩
[219] J.-C. Bermond, C. J. Colbourn, D. Coudert, G. Ge, A. C. H. Ling, and X. Muñoz, *Traffic grooming in unidirectional WDM rings with grooming ratio $C = 6$*, SIAM J. Disc. Math. 19 (2005) 523–542. ⟨495⟩
[220] J.-C. Bermond, C. J. Colbourn, A. C. H. Ling, and M.-L. Yu, *Grooming in unidirectional rings: $K_4 - e$ designs*, Discrete Math. 284 (2004) 57–62. ⟨495⟩
[221] J.-C. Bermond, D. Coudert, and X. Muñoz, *Traffic grooming in unidirectional WDM ring networks: The all-to-all unitary case*, in IFIP ONDM, 2003, 1135–1153. ⟨494, 495⟩
[222] J.-C. Bermond, O. DeRivoyre, S. Pérennes, and M. Syska, *Groupage par tubes*, in Conference ALGOTEL, 2003, 169–174. ⟨495⟩
[223] R. Bertolo, I. Bluskov, and H. Hämäläinen, *Upper bounds on the general covering number $C_\lambda(v, k, t, m)$*, J. Combin. Des. 12 (2004) 362–380. ⟨514, 519⟩
[224] T. Beth, *Eine Bemerkung zur Abschätzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren*, Abh. Math. Sem. Hamburg 53 (1983) 284–288. ⟨163⟩
[225] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge Univ. Press, 2nd ed., 1999. ⟨79, 103, 110, 123, 250, 251, 254, 302, 400, 404, 410, 414, 417, 419, 420, 421, 422, 424, 425, 435, 730, 847⟩
[226] A. Betten, *Genealogy of t-designs*, Australas. J. Combin. 29 (2004) 3–34. ⟨80⟩
[227] A. Betten and D. Betten, *Regular linear spaces*, Beiträge Algebra Geom. 38 (1997) 111–124. ⟨268, 762⟩
[228] ——, *Linear spaces with at most* 12 *points*, J. Combin. Des. 7 (1999) 119–145. ⟨269⟩
[229] ——, *The proper linear spaces on* 17 *points*, Discrete Appl. Math. 95 (1999) 83–108. ⟨269, 354⟩
[230] ——, *Tactical decompositions and some configurations v_4*, J. Geom. 66 (1999) 27–41. ⟨269⟩
[231] ——, *Note on the proper linear spaces on* 18 *points*, in Algebraic Combinatorics and Applications, A. Betten, A. Kohnert, R. Laue, and A. Wassermann, eds., Springer, Berlin, 2001, 40–54. ⟨269⟩
[232] ——, *More on regular linear spaces*, J. Combin. Des. 13 (2005) 441–461. ⟨268⟩
[233] A. Betten, G. Brinkmann, and T. Pisanski, *Counting symmetric configurations v_3*, Discrete Appl. Math. 99 (2000) 331–338. ⟨269, 354⟩

[234] A. Betten, A. Delandtsheer, M. Law, A. C. Niemeyer, C. E. Praeger, and S. Zhou, *Linear spaces with a line-transitive point-imprimitive automorphism group and Fang Li parameter (k,r) at most eight*, preprint. ⟨344⟩

[235] A. Betten, A. Kerber, A. Kohnert, R. Laue, and A. Wassermann, *The discovery of simple 7-designs with automorphism group* $P\Gamma L(2, 32)$, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, G. Cohen, M. Giusti, and T. Mora, eds., Springer, Berlin, 1995, 131–145. ⟨95, 97, 766⟩

[236] A. Betten, A. Kerber, R. Laue, and A. Wassermann, *Simple 8-designs with small parameters*, Des. Codes Crypt. 15 (1998) 5–27. ⟨766⟩

[237] A. Betten, M. Klin, R. Laue, and A. Wassermann, *Graphical t-designs via polynomial Kramer–Mesner matrices*, Discrete Math. 197/198 (1999) 83–109. ⟨491, 492⟩

[238] A. Betten, R. Laue, S. Molodtsov, and A. Wassermann, *Steiner systems with automorphism groups* $PSL(2, 71)$, $PSL(2, 83)$, *and* $P\Sigma L(2, 3^5)$, J. Geom. 67 (2000) 35–41. ⟨107, 110⟩

[239] A. Betten, R. Laue, and A. Wassermann, *Simple 6 and 7-designs on 19 to 33 points*, Congr. Numer. 123 (1997) 149–160. ⟨87, 92, 93, 94, 95⟩

[240] ———, *A Steiner 5-design on 36 points*, Des. Codes Crypt. 17 (1999) 181–186. ⟨106, 107, 766⟩

[241] ———, *DISCRETA: A tool for constructing t-designs*, in Computer Algebra Handbook: Foundations, Applications, Systems, J. Grabmeier, E. Kaltofen, and V. Weispfenning, eds., Springer, Berlin, 2003, 372–375. ⟨85, 101, 766, 776⟩

[242] D. Betten, *Die 12 lateinischen Quadrate der Ordnung 6*, Mitt. Math. Sem. Giessen 163 (1984) 181–188. ⟨269⟩

[243] D. Betten and M. Braun, *A tactical decomposition for incidence structures*, Ann. Discrete Math. 52 (1992) 37–43. ⟨269⟩

[244] D. Betten and U. Schumacher, *The ten configurations* 10_3, Rostock. Math. Kolloq. 46 (1993) 3–10. ⟨269⟩

[245] V. K. Bhargava and J. M. Stein, *(v, k, λ) configurations and self-dual codes*, Inf. Control 28 (1975) 352–355. ⟨683⟩

[246] V. N. Bhat-Nayak, V. D. Kane, W. L. Kocay, and R. G. Stanton, *Settling some BIBD conjectures*, Ars Combin. 16 (1983) 229–234. ⟨37⟩

[247] V. N. Bhat-Nayak and S. S. Shrikhande, *Non-isomorphic solutions of some balanced incomplete block designs*, J. Combin. Theory A 9 (1970) 174–191. ⟨467⟩

[248] V. N. Bhat-Nayak and A. Wirmani-Prasad, *Three new dicyclic solutions of* $(21, 42, 20, 10, 9)$*-designs*, J. Combin. Theory A 40 (1985) 427–428. ⟨40⟩

[249] K. N. Bhattacharya, *A note on two-fold triple systems*, Sankhyā 6 (1943) 313–314. ⟨19⟩

[250] ———, *A new balanced incomplete block design*, Science and Culture 9 (1944) 508. ⟨113⟩

[251] J. Bierbrauer, *Monotypical uniformly homogeneous sets of permutations*, Arch. Math. (Basel) 58 (1992) 338–344. ⟨544⟩

[252] ———, *A new family of 4-designs*, Graphs Combin. 11 (1995) 209–211. ⟨82⟩

[253] ———, *A new family of 4-designs with block size 9*, Discrete Math. 138 (1995) 113–117. ⟨82⟩

[254] ———, *The uniformly 3-homogeneous subsets of* $\mathrm{PGL}(2, q)$, J. Algeb. Combin. 4 (1995) 99–102. ⟨544⟩

[255] ———, *Construction of orthogonal arrays*, J. Stat. Plann. Infer. 56 (1996) 39–47. ⟨227, 567⟩

[256] ———, *An infinite family of 7-designs*. unpublished manuscript, 1999. ⟨83⟩

[257] ———, *Some friends of Alltop's designs* $4\text{-}(2^f + 1, 5, 5)$, J. Combin. Math. Combin. Comput. 36 (2001) 43–53. ⟨82⟩

[258] ———, *Introduction to Coding Theory*, Chapman and Hall/CRC, Boca Raton FL, 2005. ⟨228, 357, 391⟩

[259] J. Bierbrauer, S. Black, and Y. Edel, *Some t-homogeneous sets of permutations*, Des. Codes Crypt. 9 (1996) 29–38. ⟨545⟩

[260] J. Bierbrauer and Y. Edel, *Theory of perpendicular arrays*, J. Combin. Des. 2 (1994) 375–406. ⟨543, 545, 546, 547⟩
[261] ——, *Halving* PSL$(2, q)$, J. Geom. 64 (1999) 51–54. ⟨545⟩
[262] J. Bierbrauer, Y. Edel, and W. C. Schmid, *Coding-theoretic constructions for* (t, m, s)*-nets and ordered orthogonal arrays*, J. Combin. Des. 10 (2002) 403–418. ⟨641, 642⟩
[263] J. Bierbrauer, K. Gopalakrishnan, and D. R. Stinson, *Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds*, SIAM J. Disc. Math. 9 (1996) 424–452. ⟨357⟩
[264] J. Bierbrauer and H. Schellwat, *Almost independent and weakly biased arrays: Efficient constructions and cryptologic applications*, Lect. Notes Comp. Sci. 1880 (2000) 533–543. ⟨362, 365⟩
[265] J. Bierbrauer and Tran van Trung, *Halving* PGL$(2, 2^f)$, f *odd: A series of cryptocodes*, Des. Codes Crypt. 1 (1991) 141–148. ⟨545⟩
[266] ——, *Some highly symmetric authentication perpendicular arrays*, Des. Codes Crypt. 1 (1991) 307–319. ⟨545⟩
[267] D. C. Bigelow and C. J. Colbourn, *Faithful enclosing of triple systems: Doubling the index*, Acta Math. Univ. Comenian. (N.S.) 60 (1991) 133–151. ⟨63, 770⟩
[268] ——, *Faithful enclosing of triple systems: A generalization of Stern's theorem*, in Graphs, Matrices and Designs, R. S. Rees, ed., Dekker, New York, 1993, 31–42. ⟨63, 69⟩
[269] N. L. Biggs, *T.P. Kirkman, mathematician*, Bull. London Math. Soc. 13 (1981) 97–120. ⟨14⟩
[270] E. J. Billington, *Balanced* n*-ary designs: A combinatorial survey and some new results*, Ars Combin. 17A (1984) 37–72. ⟨331, 332⟩
[271] ——, *Designs with repeated elements in blocks: A survey and some recent results*, Congr. Numer. 68 (1989) 123–146. ⟨331⟩
[272] ——, *New cyclic* $(61, 244, 40, 10, 6)$ *BIBDs*, Discrete Math. 77 (1989) 51–53. ⟨55⟩
[273] ——, *Combinatorial trades: A survey of recent results*, in Designs 2002, Kluwer, Boston MA, 2003, 47–67. ⟨648⟩
[274] E. J. Billington, A. Khodkar, and E. S. Mahmoodian, *Balanced ternary designs with block size four*, J. Stat. Plann. Infer. 37 (1993) 95–126. ⟨332⟩
[275] E. J. Billington and P. J. Robinson, *A list of balanced ternary designs with* $r \leq 15$*, and some necessary existence conditions*, Ars Combin. 16 (1983) 235–258. ⟨332, 333⟩
[276] S. Bisgaard, *Blocking generators for small* 2^{k-p} *designs*, J. Qual. Technol. 26 (1994) 288–296. ⟨446⟩
[277] I. F. Blake and R. C. Mullin, *An Introduction to Algebraic and Combinatorial Coding Theory*, Academic Press, New York, 1976. ⟨698⟩
[278] G. R. Blakley, *Safeguarding cryptographic keys*, AFIPS Conf. Proc. 48 (1979) 313–317. ⟨639⟩
[279] G. R. Blakley and C. Meadows, *Security of ramp schemes*, Lect. Notes Comp. Sci. 196 (1985) 242–268. ⟨636, 639⟩
[280] J. L. Blanchard, *A construction for orthogonal arrays with strength* $t \geq 3$, Discrete Math. 137 (1995) 35–44. ⟨227⟩
[281] ——, *A construction for Steiner* 3*-designs*, J. Combin. Theory A 71 (1995) 60–67. ⟨103⟩
[282] A. Blinco and S. I. El-Zanati, *A note on the cyclic decomposition of complete graphs into bipartite graphs*, Bull. Inst. Combin. Appl. 40 (2004) 77–82. ⟨484⟩
[283] R. E. Block, *On the orbits of collineation groups*, Math. Zeitschr. 96 (1967) 33–49. ⟨20, 339⟩
[284] A. Blokhuis and A. E. Brouwer, *Uniqueness of the Zara graph on* 126 *points and nonexistence of a completely regular graph on* 288 *points*, in Papers Dedicated to J.J. Seidel, P. J. de Doelder, J. de Graaf, and J. H. van Lint, eds., Report 84-WSK-03, Techn. Univ. Eindhoven, 1984, 6–19. ⟨881⟩

[285] A. Blokhuis, A. E. Brouwer, A. Delandtsheer, and J. Doyen, *Orbits on points and lines in finite linear and quasi-linear spaces*, J. Combin. Theory A 44 (1987) 159–163. ⟨339⟩

[286] A. Blokhuis and W. H. Haemers, *An infinite family of quasi-symmetric designs*, J. Stat. Plann. Infer. 95 (2001) 117–119. ⟨580⟩

[287] A. Blokhuis and H. A. Wilbrink, *Characterisation theorems for Zara graphs*, Europ. J. Combin. 10 (1989) 57–68. ⟨881⟩

[288] C. Blundo, A. De Santis, and D. R. Stinson, *On the contrast in visual cryptography schemes*, J. Cryptology 12 (1999) 261–289. ⟨638, 639⟩

[289] I. Bluskov, *private communication*. ⟨85, 86, 87, 88, 89⟩

[290] I. Bluskov and K. Heinrich, *Super-simple designs with $v \leq 32$*, J. Stat. Plann. Infer. 95 (2001) 121–131. ⟨635⟩

[291] J. Bolick, *t-Designs und Schnittzahlen*, Master's thesis, University of Hamburg (1990) 1–83. ⟨84⟩

[292] D. W. Bolton, *Problem*, in Combinatorics, D. J. A. Welsh and D. R. Woodall, eds., Instit. Math. Applic., Southend-on-Sea, Essex, England, 1972, 351–352. ⟨570⟩

[293] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, Macmillan, London, 1976. ⟨740, 741⟩

[294] D. Boneh and J. Shaw, *Collusion-secure fingerprinting for digital data*, Lect. Notes Comp. Sci. 963 (1995) 452–465. ⟨632⟩

[295] C. P. Bonnington, M. J. Grannell, T. S. Griggs, and J. Širáň, *Exponential families of non-isomorphic triangulations of complete graphs*, J. Combin. Theory B 78 (2000) 169–184. ⟨488⟩

[296] E. Boros, T. Szőnyi, and K. Tichler, *On defining sets for projective planes*, Discrete Math. 303 (2005) 17–31. ⟨384⟩

[297] P. B. Borwein, K.-K. S. Choi, and J. Jedwab, *Binary sequences with merit factor greater than* 6.34, IEEE Trans. Inform. Theory 50 (2004) 3234–3249. ⟨317⟩

[298] P. B. Borwein and R. A. Ferguson, *A complete description of Golay pairs for lengths up to* 100, Math. Comp. 73 (2004) 967–985. ⟨318, 321⟩

[299] J. Bosák, *Decompositions of Graphs*, Kluwer, Dordrecht, 1990. ⟨755⟩

[300] R. C. Bose, *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-latin squares*, Sankhyā 3 (1938) 323–338. ⟨16, 18⟩

[301] ———, *On the construction of balanced incomplete block designs*, Ann. Eugenics 9 (1939) 353–399. ⟨18⟩

[302] ———, *An affine analogue of Singer's theorem*, J. Indian Math. Soc. 6 (1942) 1–15. ⟨17, 246, 437⟩

[303] ———, *On some new series of balanced incomplete block designs*, Bull. Calcutta Math. Soc. 34 (1942) 17–31. ⟨18⟩

[304] ———, *Strongly regular graphs, partial geometries and partially balanced designs*, Pacific J. Math. 13 (1963) 389–419. ⟨20⟩

[305] R. C. Bose and W. S. Connor, *Combinatorial properties of group divisible incomplete block designs*, Ann. Math. Stat. 23 (1952) 367–383. ⟨19, 730⟩

[306] R. C. Bose and K. R. Nair, *Partially balanced incomplete block designs*, Sankhyā 4 (1938) 337–372. ⟨18⟩

[307] R. C. Bose and T. Shimamoto, *Classification and analysis of partially balanced incomplete block designs with two associate classes*, J. Amer. Statist. Assoc. 47 (1952) 151–184. ⟨18⟩

[308] R. C. Bose and S. S. Shrikhande, *On the falsity of Euler's conjecture about the non-existence of two orthogonal latin squares of order $4t + 2$*, Proc. Nat. Acad. Sci. U.S.A. 45 (1959) 734–737. ⟨12⟩

[309] R. C. Bose, S. S. Shrikhande, and E. T. Parker, *Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture*, Canad. J. Math. 12 (1960) 189–203. ⟨12⟩

[310] R. C. Bose, S. S. Shrikhande, and N. M. Singhi, *Edge regular multigraphs and partial geometric designs with an application to the embedding of quasi-residual designs*, in Colloquio Internazionale sulle Teorie Combinatorie, Tomo I, Accad. Naz. Lincei, Rome, 1976, 49–81. ⟨113⟩

[311] P. A. H. Bours, *On the construction of perfect deletion-correcting codes using design theory*, Des. Codes Crypt. 6 (1995) 5–20. ⟨387⟩
[312] S. Bouyuklieva and M. Harada, *Extremal self-dual* $[50, 25, 10]$ *codes with automorphisms of order* 3 *and quasi-symmetric* 2-$(49, 9, 6)$ *designs*, Des. Codes Crypt. 28 (2003) 163–169. ⟨580, 689⟩
[313] A. Bowler, M. Grannell, T. S. Griggs, and K. A. S. Quinn, *On directed designs with block size five*, J. Geom. 67 (2000) 50–60. ⟨442⟩
[314] G. E. P. Box, S. Bisgaard, and C. A. Fung, *An explanation and critique of Taguchi's contribution to quality engineering*, Qual. Reliab. Eng. Int. 4 (1988) 123–131. ⟨451⟩
[315] C. Bracken, *Codes, Designs, Spin Models and the Walsh Transform*, PhD thesis, National University of Ireland, Maynooth, 2004. ⟨576, 577⟩
[316] C. Bracken and G. McGuire, *Characterization of SDP designs that yield certain spin models*, Des. Codes Crypt. 36 (2005) 45–52. ⟨577, 578⟩
[317] C. Bracken, G. McGuire, and H. N. Ward, *New quasi-symmetric designs constructed using mutually orthogonal latin squares and Hadamard matrices*, preprint. ⟨580⟩
[318] L. Brankovic and A. Rosa, *private communication.* ⟨485⟩
[319] L. J. Brant and G. L. Mullen, *Some results on enumeration and isotopic classification of frequency squares*, Utilitas Math. 29 (1986) 231–244. ⟨471⟩
[320] ———, *A study of frequency cubes*, Discrete Math. 69 (1988) 115–121. ⟨471⟩
[321] M. Braun, A. Kerber, and R. Laue, *Systematic construction of q-analogs of* t-(v, k, λ)*-designs*, Des. Codes Crypt. 34 (2005) 55–70. ⟨850⟩
[322] R. K. Brayton, D. Coppersmith, and A. J. Hoffman, *Self-orthogonal latin squares*, in Colloquio Internazionale sulle Teorie Combinatorie, Tomo II, Accad. Naz. Lincei, Rome, 1976, 509–517. ⟨20, 212⟩
[323] D. Breach, *private communication.* ⟨36⟩
[324] D. Breach and A. R. Thompson, *Reducible* 2-$(11, 5, 4)$ *and* 3-$(12, 6, 4)$ *designs*, J. Austral. Math. Soc. A 39 (1985) 194–215. ⟨37, 41⟩
[325] E. F. Brickell, *A few results in message authentication*, Congr. Numer. 43 (1984) 141–154. ⟨502⟩
[326] W. G. Bridges, M. Hall Jr., and J. L. Hayden, *Codes and designs*, J. Combin. Theory A 31 (1981) 155–174. ⟨118, 690⟩
[327] G. Brinkmann, *Fast generation of cubic graphs*, J. Graph Theory 23 (1996) 139–149. ⟨734⟩
[328] B. W. Brock, *Hermitian congruence and the existence and completion of generalized Hadamard matrices*, J. Combin. Theory A 49 (1988) 233–261. ⟨303, 305⟩
[329] W. Broughton and G. McGuire, *Some observations on quasi-3 designs and Hadamard matrices*, Des. Codes Crypt. 18 (1999) 55–61. ⟨576, 577, 582⟩
[330] ———, *On the non-existence of quasi-*3 *designs*, Discrete Math. 262 (2003) 79–87. ⟨576, 578⟩
[331] A. E. Brouwer, *private communication.* ⟨37, 47⟩
[332] ———, *Some nonisomorphic BIBDs* $(4, 1; v)$. Math. Centrum Amsterdam, ZW 102, 1977. ⟨41, 44, 45, 47, 48, 55, 56⟩
[333] ———, *Table of* t*-designs without repeated blocks,* $2 \le t \le k \le v/2$, $\lambda \le \lambda^+/2$, Report ZN76, Math. Centrum. Amsterdam, 1977. Unpublished update 1986. ⟨84, 85, 86, 87⟩
[334] ———, *The number of mutually orthogonal latin squares—A table up to order* 10000, Tech. Report ZW 123/79, Mathematisch Centrum, Amsterdam, 1979. ⟨175⟩
[335] ———, *Optimal packings of* K_4*'s into a* K_n, J. Combin. Theory A 26 (1979) 278–297. ⟨250, 253⟩
[336] ———, *A series of separable designs with application to pairwise orthogonal latin squares*, Europ. J. Combin. 1 (1980) 39–41. ⟨240, 241⟩
[337] ———, *The linear spaces on* 15 *points*, Ars Combin. 12 (1981) 3–35. ⟨269⟩
[338] ———, *Polarities of G. Higman's symmetric design and a strongly regular graph on* 176 *vertices*, Aequat. Math. 25 (1982) 77–82. ⟨861⟩

[339] ———, *An infinite series of symmetric designs*, vol. 202 of Afdeling Zuivere Wiskunde [Department of Pure Mathematics], Mathematisch Centrum, Amsterdam, 1983. ⟨117⟩
[340] ———, *The uniqueness of the strongly regular graph on* 77 *points*, J. Graph Theory 7 (1983) 455–461. ⟨857⟩
[341] ———, *Four MOLS of order* 10 *with a hole of order* 2, J. Stat. Plann. Infer. 10 (1984) 203–205. ⟨194⟩
[342] ———, *Some new two-weight codes and strongly regular graphs*, Discrete Appl. Math. 10 (1985) 111–114. ⟨855, 856, 857, 865, 866⟩
[343] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Springer, Heidelberg, 1989. ⟨327, 330, 868⟩
[344] A. E. Brouwer, A. M. Cohen, and M. V. M. Nguyen, *Orthogonal arrays of strength* 3 *and small run sizes*, J. Stat. Plann. Infer. 136 (2006) 3268–3280. ⟨227⟩
[345] A. E. Brouwer and W. H. Haemers, *Structure and uniqueness of the* $(81, 20, 1, 6)$ *strongly regular graph*, Discrete Math. 106/107 (1992) 77–82. ⟨857⟩
[346] ———, *The Gewirtz graph—An exercise in the theory of graph spectra*, Europ. J. Combin. 14 (1993) 397–407. ⟨856⟩
[347] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, *A new table of constant weight codes*, IEEE Trans. Inform. Theory 36 (1990) 1334–1380. ⟨701⟩
[348] A. E. Brouwer and J. H. van Lint, *Strongly regular graphs and partial geometries*, in Enumeration and Design, D. M. Jackson and S. A. Vanstone, eds., Academic Press, Toronto, 1984, 85–122. ⟨561, 854, 855, 868⟩
[349] A. E. Brouwer and T. Verhoeff, *An updated table of minimum-distance bounds for binary linear codes*, IEEE Trans. Inform. Theory 39 (1993) 662–676. ⟨701⟩
[350] A. E. Brouwer and M. Voorhoeve, *Turán theory and the lotto problem*, Mathematical Centrum Tracts 106 (1979) 99–105. ⟨514⟩
[351] A. E. Brouwer and H. A. Wilbrink, *Blocking sets in translation planes*, J. Geom. 19 (1982) 200. ⟨728⟩
[352] ———, *A symmetric design with parameters* 2-$(49, 16, 5)$, J. Combin. Theory A 37 (1984) 193–194. ⟨37, 38, 118⟩
[353] J. W. Brown, F. Cherry, L. Most, M. Most, E. T. Parker, and W. D. Wallis, *The spectrum of orthogonal diagonal latin squares*, in Graphs, Matrices and Designs, R. S. Rees, ed., Dekker, New York, 1993, 43–49. ⟨190⟩
[354] R. H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. 55 (1944) 19–52. ⟨18⟩
[355] ———, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. 60 (1946) 245–354. ⟨18⟩
[356] R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canad. J. Math. 1 (1949) 88–93. ⟨19, 111⟩
[357] W. Bruno, E. Knill, D. Balding, D. Bruce, N. Doggett, W. Sawhill, R. Stallings, C. Whittaker, and D. Torney, *Efficient pooling designs for library screening*, Genomics 26 (1995) 21–30. ⟨574⟩
[358] D. E. Bryant, *Hamilton cycle rich* 2*-factorizations of complete graphs*, J. Combin. Des. 12 (2004) 147–155. ⟨376, 377⟩
[359] D. E. Bryant and M. Buchanan, *Embedding partial totally symmetric quasigroups*, preprint. ⟨159⟩
[360] D. E. Bryant, S. I. El-Zanati, B. M. Maenhaut, and C. Vanden Eynden, *Decomposition of complete graphs into* 5*-cubes*, J. Combin. Des. 14 (2006) 159–166. ⟨480⟩
[361] D. E. Bryant and D. Horsley, *A proof of Lindner's conjecture on embeddings of partial Steiner triple systems*, preprint (2005). ⟨63, 159, 380⟩
[362] D. E. Bryant, D. Horsley, and B. M. Maenhaut, *Decompositions into* 2*-regular subgraphs and equitable partial cycle decompositions*, J. Combin. Theory B 93 (2005) 67–72. ⟨374⟩

[363] D. E. Bryant, C. D. Leach, and C. A. Rodger, *Hamilton decompositions of complete bipartite graphs with a 3-factor leave*, Australas. J. Combin. 31 (2005) 331–336. ⟨378⟩
[364] D. E. Bryant and B. M. Maenhaut, *Decompositions of complete graphs into triangles and Hamilton cycles*, J. Combin. Des. 12 (2004) 221–232. ⟨374⟩
[365] D. E. Bryant, B. M. Maenhaut, and I. M. Wanless, *New families of atomic latin squares and perfect 1-factorisations*, J. Combin. Theory A 113 (2006) 608–624. ⟨752⟩
[366] D. E. Bryant, C. A. Rodger, and E. R. Spicer, *Embeddings of m-cycle systems and incomplete m-cycle systems: $m \leq 14$*, Discrete Math. 171 (1997) 55–75. ⟨380⟩
[367] R. C. Bryce, C. J. Colbourn, and M. B. Cohen, *A framework of greedy methods for constructing interaction test suites*, in Proc. 27th International Conference on Software Engineering (ICSE2005), St. Louis MO, 2005, 146–155. ⟨363⟩
[368] T. Brylawski, *Intersection theory for embeddings of matroids into uniform geometries*, Stud. Appl. Math. 61 (1979) 211–244. ⟨852⟩
[369] F. Budden, *Speedway tournaments in the classroom*, Math. Gaz. 61 (1977) 266–272. ⟨604⟩
[370] F. Buekenhout, *Existence of unitals in finite translation planes of order q^2 with a kernel of order q*, Geom. Ded. 5 (1976) 189–194. ⟨728⟩
[371] F. Buekenhout, P.-O. Dehaye, and D. Leemans, *RWPRI and $(2T)_1$ flag-transitive linear spaces*, Beiträge Algebra Geom. 44 (2003) 25–46. ⟨510⟩
[372] F. Buekenhout, A. Delandtsheer, and J. Doyen, *Finite linear spaces with flag-transitive groups*, J. Combin. Theory A 49 (1988) 268–293. ⟨341⟩
[373] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, and J. Saxl, *Linear spaces with flag-transitive automorphism groups*, Geom. Ded. 36 (1990) 89–94. ⟨341⟩
[374] B. R. Bugelski, *A note on Grant's discussion of the latin square principle in the design of experiments*, Psychological Bull. 46 (1949) 49–50. ⟨656, 657⟩
[375] M. Buratti, *private communication*. ⟨55, 481⟩
[376] ———, *A powerful method for constructing difference families and optimal optical orthogonal codes*, Des. Codes Crypt. 5 (1995) 13–25. ⟨402⟩
[377] ———, *Improving two theorems of Bose on difference families*, J. Combin. Des. 3 (1995) 15–24. ⟨401⟩
[378] ———, *On simple radical difference families*, J. Combin. Des. 3 (1995) 161–168. ⟨401⟩
[379] ———, *Recursive constructions for difference matrices and relative difference families*, J. Combin. Des. 6 (1998) 165–182. ⟨399, 410, 412⟩
[380] ———, *Some constructions for 1-rotational BIBD's with block size 5*, Australas. J. Combin. 17 (1998) 199–227. ⟨50⟩
[381] ———, *Old and new designs via difference multisets and strong difference families*, J. Combin. Des. 7 (1999) 406–425. ⟨405, 407⟩
[382] ———, *Pairwise balanced designs from finite fields*, Discrete Math. 208/209 (1999) 103–117. ⟨49⟩
[383] ———, *Existence of $\mathbb{Z}$-cyclic triplewhist tournaments for a prime number of players*, J. Combin. Theory A 90 (2000) 315–325. ⟨666⟩
[384] ———, *1-rotational Steiner triple systems over arbitrary groups*, J. Combin. Des. 9 (2001) 215–226. ⟨406⟩
[385] ———, *Abelian 1-factorizations of the complete graph*, Europ. J. Combin. 22 (2001) 291–295. ⟨751, 752⟩
[386] ———, *Cyclic designs with block size 4 and related optimal optical orthogonal codes*, Des. Codes Crypt. 26 (2002) 111–125. ⟨404⟩
[387] ———, *Existence of 1-rotational k-cycle systems of the complete graph*, Graphs Combin. 20 (2004) 41–46. ⟨382⟩
[388] M. Buratti and A. Del Fra, *Existence of cyclic k-cycle systems of the complete graph*, Discrete Math. 261 (2003) 113–125. ⟨616⟩
[389] M. Buratti and N. J. Finizio, *Existence results for 1-rotational resolvable Steiner 2-designs with block-size 6 or 8*, preprint. ⟨406⟩

[390] M. Buratti and A. Pasotti, *Graph decompositions with the use of difference matrices*, Bull. Inst. Combin. Appl. 47 (2006) 23–32. ⟨419⟩
[391] M. Buratti and F. Zuanni, *G-invariantly resolvable Steiner 2-designs which are 1-rotational over G*, Bull. Belg. Math. Soc. Simon Stevin 5 (1998) 221–235. ⟨406⟩
[392] ———, *The 1-rotational* $(52, 4, 1)$*-RBIBD's*, J. Combin. Math. Combin. Comput. 30 (1999) 99–102. ⟨38⟩
[393] ———, *On singular 1-rotational Steiner 2-designs*, J. Combin. Theory A 86 (1999) 232–244. ⟨42⟩
[394] ———, *Explicit constructions for 1-rotational Kirkman triple systems*, Utilitas Math. 59 (2001) 27–30. ⟨406⟩
[395] ———, *Perfect Cayley designs as generalizations of perfect Mendelsohn designs*, Des. Codes Crypt. 23 (2001) 233–247. ⟨534, 666⟩
[396] ———, *Some observations on three classical BIBD constructions*, Discrete Math. 238 (2001) 19–26. ⟨38, 42, 47, 48, 51, 53, 56⟩
[397] A. P. Burger, W. R. Grundlingh, and J. H. van Vuuren, *Towards a characterization of lottery set overlapping structures*, Ars Combin. (to appear). ⟨513⟩
[398] L. Burgess and D. J. Street, *Algorithms for constructing orthogonal main effect plans*, Utilitas Math. 46 (1994) 33–48. ⟨548, 549⟩
[399] D. Burshtein and G. Miller, *Expander graph arguments for message-passing algorithms*, IEEE Trans. Inform. Theory 47 (2001) 782–790. ⟨521, 522⟩
[400] K. A. Bush, *A generalization of the theorem due to MacNeish*, Ann. Math. Stat. 23 (1952) 293–295. ⟨226⟩
[401] ———, *Orthogonal arrays of index unity*, Ann. Math. Stat. 23 (1952) 426–434. ⟨226⟩
[402] K. A. Bush, W. T. Federer, H. Pesotan, and D. Raghavarao, *New combinatorial designs and their applications to group testing*, J. Stat. Plann. Infer. 10 (1984) 335–343. ⟨633⟩
[403] F. C. Bussemaker, W. H. Haemers, R. A. Mathon, and H. A. Wilbrink, *A* $(49, 16, 3, 6)$ *strongly regular graph does not exist*, Europ. J. Combin. 10 (1989) 413–418. ⟨856⟩
[404] F. C. Bussemaker, R. A. Mathon, and J. J. Seidel, *Tables of two-graphs*, in Combinatorics and Graph Theory, S. B. Rao, ed., Springer, Berlin, 1981, 70–112. ⟨37, 38, 50, 876, 880, 882⟩
[405] F. C. Bussemaker and V. D. Tonchev, *New extremal doubly-even codes of length* 56 *derived from Hadamard matrices of order* 28, Discrete Math. 76 (1989) 45–49. ⟨683⟩
[406] ———, *Extremal doubly-even codes of length* 40 *derived from Hadamard matrices of order* 20, Discrete Math. 82 (1990) 317–321. ⟨682⟩
[407] W. H. Bussey, *The tactical problem of Steiner*, Amer. Math. Monthly 21 (1914) 3–12. ⟨12⟩
[408] A. T. Butson, *Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences*, Canad. J. Math. 15 (1963) 42–48. ⟨305⟩
[409] L. Calabi, *On the computation of Levenshtein's distances*, Tech. Report TN-9-0030, Parke Math. Labs., Carlisle MA, 1967. ⟨386⟩
[410] A. R. Calderbank, *The application of invariant theory to the existence of quasi-symmetric designs*, J. Combin. Theory A 44 (1987) 94–109. ⟨580, 690⟩
[411] ———, *Geometric invariants for quasi-symmetric designs*, J. Combin. Theory A 47 (1988) 101–110. ⟨690⟩
[412] A. R. Calderbank and W. M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. 18 (1986) 97–122. ⟨701, 855⟩
[413] P. J. Cameron, *Extending symmetric designs*, J. Combin. Theory A 14 (1973) 215–220. ⟨114⟩
[414] ———, *Near regularity conditions for designs*, Geom. Ded. 2 (1973) 213–223. ⟨329, 577, 789⟩
[415] ———, *Parallelisms of Complete Designs*, Cambridge Univ. Press, London, 1976. ⟨743⟩

[416] ——, *Several* 2-$(46, 6, 3)$ *designs*, Discrete Math. 87 (1991) 89–90. ⟨44⟩
[417] ——, *Two-graphs and trees*, Discrete Math. 127 (1994) 63–74. ⟨876, 877⟩
[418] ——, *Counting two-graphs related to trees*, Electron. J. Comb. 2 (1995) #R4. ⟨877⟩
[419] ——, *Multi-letter Youden rectangles from quadratic forms*, Discrete Math. 266 (2003) 143–151. ⟨674⟩
[420] P. J. Cameron, J.-M. Goethals, and J. J. Seidel, *Strongly regular graphs having strongly regular subconstituents*, J. Algebra 55 (1978) 257–280. ⟨558, 858, 860⟩
[421] P. J. Cameron, H. R. Maimani, G. R. Omidi, and B. Tayfeh-Rezaie, 3-*Designs from PSL*$(2, q)$, Discrete Math. (to appear). ⟨82⟩
[422] P. J. Cameron and C. E. Praeger, *Block-transitive t-designs I: Point-imprimitive designs*, Discrete Math. 118 (1993) 33–43. ⟨342, 343, 344, 492⟩
[423] ——, *Block-transitive t-designs II: Large t*, in Proc. Finite Geometries and Combinatorics, London Math. Soc., 1993, 103–119. ⟨340⟩
[424] P. J. Cameron and J. H. van Lint, *Graphs, Codes and Designs*, Cambridge Univ. Press, Cambridge, 1980. ⟨684, 701⟩
[425] ——, *Designs, Graphs, Codes and Their Links*, Cambridge Univ. Press, Cambridge, 1991. ⟨578⟩
[426] P. J. Cameron and B. S. Webb, *What is an infinite design?* J. Combin. Des. 10 (2002) 79–91. ⟨504, 506⟩
[427] A. R. Camina, *A survey of the automorphism groups of block designs*, J. Combin. Des. 2 (1994) 79–100. ⟨340⟩
[428] ——, *Projective planes with a transitive automorphism group*, Innov. Incidence Geom. 1 (2005) 191–196. ⟨342⟩
[429] A. R. Camina, P. Neumann, and C. E. Praeger, *Alternating groups acting on linear spaces*, Proc. London Math. Soc. 87 (2003) 29–53. ⟨342⟩
[430] A. R. Camina and C. E. Praeger, *Line-transitive, point-quasi-primitive automorphism groups of finite linear spaces are affine or almost simple*, Aequat. Math. 61 (2001) 221–232. ⟨342⟩
[431] A. R. Camina and F. Spiezia, *Sporadic groups and automorphisms of linear spaces*, J. Combin. Des. 8 (2000) 353–362. ⟨342⟩
[432] P. Camion and A. Canteaut, *Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography*, Des. Codes Crypt. 16 (1999) 121–149. ⟨357⟩
[433] S. v. R. Cammann, *Magic squares*, in Encyclopædia Britannica, Vol. 14, 14th Edition, Encyclopædia Britannica, Chicago, 1973, 573–575. ⟨524, 525, 528⟩
[434] J. Cannon and C. Playoust, *MAGMA: A new computer algebra system*, Euromath Bull. 2 (1996) 113–144. ⟨820⟩
[435] I. Cardinali and S. E. Payne, *The q-clan geometries with* $q = 2^e$, `http://www-math.cudenver.edu/~spayne/publications/card.ps` (2003) 210 pp. ⟨477⟩
[436] C. Carlet, *Recent results on binary bent functions*, J. Combin. Inf. Syst. Sci. 25 (2000) 133–149. ⟨339⟩
[437] R. D. Carmichael, *Tactical configurations of rank two*, Amer. J. Math. 53 (1931) 217–240. ⟨17⟩
[438] ——, *Introduction to the Theory of Groups of Finite Order*, Ginn, Boston, 1937. ⟨17⟩
[439] Y. Caro and R. Yuster, *Covering graphs: The covering problem solved*, J. Combin. Theory A 83 (1998) 273–282. ⟨367⟩
[440] N. J. Cavenagh, *The size of the smallest latin trade in a back circulant latin square*, Bull. Inst. Combin. Appl. 38 (2003) 11–18. ⟨148⟩
[441] ——, *A superlinear lower bound for the size of a critical set in a latin square*, preprint (2005). ⟨147⟩
[442] A. Cayley, *On the triadic arrangements of seven and fifteen things*, London Edinburgh and Dublin Philos. Mag. and J. Sci. 37 (1850) 50–53. (Collected Mathematical Papers I, 481–484). ⟨13, 66⟩

[443] ——, *On a tactical theorem relating to the triads of fifteen things*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. 25 (1863) 59–61. (Collected Mathematical Papers V, 95–97). ⟨13⟩
[444] ——, *On the theory of groups*, Proc. London Math. Soc. 9 (1877) 126–133. ⟨18⟩
[445] ——, *Desiderata and suggestions I. The theory of groups*, Amer. J. Math. 1 (1878) 50–52. ⟨18⟩
[446] ——, *On latin squares*, Oxford Cambridge Dublin Messenger Math. 19 (1890) 135–137. ⟨15⟩
[447] H. C. Chan, C. A. Rodger, and J. Seberry, *On inequivalent weighing matrices*, Ars Combin. 21 (1986) 299–333. ⟨288⟩
[448] D. B. Chandler and Q. Xiang, *The invariant factors of some cyclic difference sets*, J. Combin. Theory A 101 (2003) 131–146. ⟨787, 790⟩
[449] C.-T. Chang and K. Hinkelmann, *A new series of EGD-PBIB designs*, J. Stat. Plann. Infer. 16 (1987) 1–13. ⟨564⟩
[450] L. C. Chang, *Association schemes of partially balanced block designs with parameters* $v = 28$, $n_1 = 12$, $n_2 = 15$ *and* $p_{11}^2 = 4$, Sci. Record 4 (1960) 12–18. ⟨855⟩
[451] Y. X. Chang, *The existence of resolvable BIBD with* $\lambda = 1$, Acta Math. Appl. Sinica (English Ser.) 16 (2000) 373–385. ⟨127⟩
[452] ——, *The spectrum for large sets of idempotent quasigroups*, J. Combin. Des. 8 (2000) 79–82. ⟨546⟩
[453] ——, *The spectra for two classes of graph designs*, Ars Combin. 65 (2002) 237–243. ⟨482⟩
[454] ——, *Some cyclic BIBDs with block size four*, J. Combin. Des. 12 (2004) 177–183. ⟨404⟩
[455] ——, *The existence spectrum of golf designs*, J. Combin. Des. (to appear). ⟨597⟩
[456] Y. X. Chang, R. Fuji-Hara, and Y. Miao, *Combinatorial constructions for optimal optical orthogonal codes with weight* 4, IEEE Trans. Inform. Theory 49 (2003) 1283–1292. ⟨556⟩
[457] Y. X. Chang and L. Ji, *Optimal* $(4up, 5, 1)$*-optical orthogonal codes*, J. Combin. Des. 12 (2004) 346–361. ⟨404⟩
[458] Y. X. Chang and Y. Miao, *General constructions for double group divisible designs and double frames*, Des. Codes Crypt. 26 (2002) 155–168. ⟨263, 265⟩
[459] Y. X. Chang and J. X. Yin, *Further results on optimal optical orthogonal codes with weight* 4, Discrete Math. 279 (2004) 135–151. ⟨322, 556⟩
[460] M. A. Chateauneuf and D. L. Kreher, *On the state of strength-three covering arrays*, J. Combin. Des. 10 (2002) 217–238. ⟨362, 363, 365⟩
[461] K. Chatterjee, *Search designs for searching three-factor interaction effects in the general symmetric and asymmetric factorials*, Sankhyā B 53 (1991) 304–326. ⟨454⟩
[462] G. R. Chaudhry, M. Greig, and J. R. Seberry, *On the* $(v, 5, \lambda)$*-family of Bhaskar Rao designs*, J. Stat. Plann. Infer. 106 (2002) 303–327. ⟨300⟩
[463] Y. M. Chee, *Graphical t-designs with block sizes three and four*, Discrete Math. 91 (1991) 201–206. ⟨491⟩
[464] ——, *On graphical quintuple systems*, J. Symbolic Comput. 13 (1992) 677–681. ⟨491⟩
[465] ——, *The existence of a simple* 3-$(28, 5, 30)$ *design*, Discrete Math. 118 (1993) 251–252. ⟨491⟩
[466] ——, *An improved finiteness theorem for graphical t-designs*, Discrete Math. 237 (2001) 185–186. ⟨492⟩
[467] Y. M. Chee, C. J. Colbourn, S. C. Furino, and D. L. Kreher, *Large sets of disjoint t-designs*, Australas. J. Combin. 2 (1990) 111–119. ⟨84, 85⟩
[468] Y. M. Chee, C. J. Colbourn, R. P. Gallant, and A. C. H. Ling, *On a problem of Hartman and Heinrich concerning pairwise balanced designs with holes*, J. Combin. Math. Combin. Comput. 23 (1997) 121–127. ⟨233⟩

[469] Y. M. Chee, C. J. Colbourn, and A. C. H. Ling, *Asymptotically optimal erasure-resilient codes for large disk arrays*, Discrete Appl. Math. 102 (2000) 3–36. ⟨520⟩
[470] O. Chein, H. O. Pflugfelder, and J. D. H. Smith, *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, Berlin, 1990. ⟨499⟩
[471] H. B. Chen and F. K. Hwang, *Exploring the missing link among d-separable, $\overline{d}$-separable and d-disjunct matrices*, Discrete Appl. Math. (to appear). ⟨630⟩
[472] J. Chen, D. X. Sun, and C. F. J. Wu, *A catalogue of two-level and three-level fractional factorial designs with small runs*, Int. Stat. Rev. 61 (1993) 131–145. ⟨446⟩
[473] J. Chen and C. F. J. Wu, *Some results on s^{n-k} fractional factorial designs with minimum aberration or optimal moments*, Ann. Statist. 19 (1991) 1028–1041. ⟨451, 452, 453⟩
[474] K. Chen, Z. Cao, and R. Wei, *Elementary abelian difference families with block size ≤ 6*, Bull. Inst. Combin. Appl. 43 (2005) 80–84. ⟨404⟩
[475] ———, *Super-simple balanced incomplete block designs with block size 4 and index 6*, J. Stat. Plann. Infer. 133 (2005) 535–554. ⟨634⟩
[476] K. Chen, G. Ge, and L. Zhu, *Starters and related codes*, J. Stat. Plann. Infer. 86 (2000) 379–395. ⟨404, 623, 625, 628⟩
[477] K. Chen and R. Wei, *Super-simple cyclic designs with small values*, preprint. ⟨634, 635⟩
[478] ———, *Super-simple $(v, 5, 5)$ designs*, Des. Codes Crypt. 39 (2006) 173–187. ⟨634⟩
[479] K. Chen, R. Wei, and L. Zhu, *Existence of $(q, 7, 1)$ difference families with q a prime power*, J. Combin. Des. 10 (2002) 126–138. ⟨404⟩
[480] K. Chen and L. Zhu, *On the existence of skew Room frames of type t^u*, Ars Combin. 43 (1996) 65–79. ⟨588⟩
[481] ———, *Existence of $(q, 6, 1)$ difference families with q a prime power*, Des. Codes Crypt. 15 (1998) 167–173. ⟨404⟩
[482] ———, *Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$*, J. Combin. Des. 7 (1999) 21–30. ⟨404⟩
[483] ———, *Existence of $\mathrm{APAV}(q, k)$ with q a prime power $\equiv 3 \pmod 4$ and k odd > 1*, J. Combin. Des. 7 (1999) 57–68. ⟨545⟩
[484] ———, *Existence of $V(m, t)$ vectors*, J. Stat. Plann. Infer. 106 (2002) 461–471. ⟨417, 418⟩
[485] M. H. Chen and P. C. Wang, *Multi-level factorial designs with minimum numbers of level changes*, Commun. Stat. Theory Methods 30 (2001) 875–885. ⟨449⟩
[486] Y. Q. Chen, *A construction of difference sets*, Des. Codes Crypt. 13 (1998) 247–250. ⟨117⟩
[487] Z. Chen, *Further results on difference triangle sets*, IEEE Trans. Inform. Theory 40 (1994) 1268–1270. ⟨440⟩
[488] Z. Chen, P. Fan, and F. Jin, *Disjoint difference sets, difference triangle sets, and related codes*, IEEE Trans. Inform. Theory 38 (1992) 518–522. ⟨439, 440⟩
[489] C.-S. Cheng and R. A. Bailey, *Optimality of some two-associate-class partially balanced incomplete-block designs*, Ann. Statist. 19 (1991) 1667–1671. ⟨542, 562⟩
[490] C.-S. Cheng, L. Y. Deng, and B. Tang, *Generalized minimum aberration and design efficiency for nonregular fractional factorial designs*, Statist. Sinica 12 (2002) 991–1000. ⟨453⟩
[491] C.-S. Cheng, R. J. Martin, and B. Tang, *Two-level factorial designs with extreme numbers of level changes*, Ann. Statist. 26 (1998) 1522–1539. ⟨449⟩
[492] W. E. Cherowitzo, *Ovals in Figueroa planes*, J. Geom. 37 (1990) 84–86. ⟨728⟩
[493] W. E. Cherowitzo, T. Penttila, I. Pinneri, and G. F. Royle, *Flocks and ovals*, Geom. Ded. 60 (1996) 17–37. ⟨476⟩
[494] A. G. Chetwynd and A. J. W. Hilton, *1-factorizing regular graphs of high degree—An improved bound*, Discrete Math. 75 (1989) 103–112. ⟨741⟩

[495] I. Chlamtac and A. Faragó, *Making transmission schedules immune to topology changes in multi-hop packet radio networks*, IEEE/ACM Trans. Networking 2 (1994) 23–29. ⟨632⟩

[496] B. Chor and O. Goldreich, *On the power of two-point based sampling*, J. Complexity 5 (1989) 96–106. ⟨389⟩

[497] B. Chor, O. Goldreich, J. Haastad, J. Friedman, S. Rudich, and R. Smolensky, *The bit extraction problem of t-resilient functions*, IEEE Symp. Foundations Comp. Sci. 26 (1985) 396–407. ⟨357⟩

[498] L. G. Chouinard, *Partitions of the 4-subsets of a 13-set into disjoint projective planes*, Discrete Math. 45 (1983) 297–300. ⟨98⟩

[499] ——, *Bounding graphical t-wise balanced designs*, Discrete Math. 159 (1996) 261–263. ⟨492⟩

[500] L. G. Chouinard, E. S. Kramer, and D. L. Kreher, *Graphical t-wise balanced designs*, Discrete Math. 46 (1983) 227–240. ⟨490, 491, 658⟩

[501] S. A. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India. Sect. A 14 (1944) 45–46. ⟨17, 116⟩

[502] S. A. Chowla, P. Erdős, and E. G. Straus, *On the maximal number of pairwise orthogonal latin squares of a given order*, Canad. J. Math. 13 (1960) 204–208. ⟨163⟩

[503] S. A. Chowla and H. J. Ryser, *Combinatorial problems*, Canad. J. Math. 2 (1950) 93–99. ⟨19, 111⟩

[504] W. Chu and C. J. Colbourn, *Optimal $(n, 4, 2)$-OOC of small orders*, Discrete Math. 279 (2004) 163–172. ⟨322⟩

[505] ——, *Recursive constructions for optimal $(n, 4, 2)$-OOCs*, J. Combin. Des. 12 (2004) 333–345. ⟨322, 556⟩

[506] W. Chu, C. J. Colbourn, and P. J. Dukes, *Constructions for permutation codes in powerline communications*, Des. Codes Crypt. 32 (2004) 51–64. ⟨569, 571⟩

[507] ——, *Tables for constant composition codes*, J. Combin. Math. Combin. Comput. 54 (2005) 57–65. ⟨571⟩

[508] W. Chu, C. J. Colbourn, and V. R. Syrotiuk, *Slot synchronized topology-transparent scheduling for sensor networks*, Computer Communications 29 (2006) 421–428. ⟨632⟩

[509] W. Chu and S. W. Golomb, *Circular tuscan-k arrays from permutation binomials*, J. Combin. Theory A 97 (2002) 195–202. ⟨652, 655, 656⟩

[510] ——, *A note on the equivalence between strict optical orthogonal codes and difference triangle sets*, IEEE Trans. Inform. Theory 49 (2003) 759–761. ⟨322⟩

[511] J. B. Clark and A. M. Dean, *Equivalence of fractional factorial designs*, Statist. Sinica 11 (2001) 537–547. ⟨449⟩

[512] W. H. Clatworthy, *Partially balanced incomplete block designs with two associate classes and two treatments per block*, J. Res. Nat. Bur. Standards 54 (1955) 177–190. ⟨855⟩

[513] ——, *Tables of Two-Associate-Class Partially Balanced Designs*, National Bureau of Standards (U.S.) Applied Mathematics Series No. 63, Washington DC, 1973. ⟨541, 542, 563, 564, 565⟩

[514] W. H. Clatworthy and R. J. Lewyckyj, *Comments on Takeuchi's table of difference sets generating balanced incomplete block designs*, Rev. Inst. Internat. Statist. 36 (1968) 12–18. ⟨38, 39, 40, 44⟩

[515] A. Clebsch, *Über die Flächen vierter Ordnung, welche eine Doppelcurve zweiten Grades besitzen*, J. für Math. 69 (1868) 142–184. ⟨855⟩

[516] D. M. Cohen, S. R. Dalal, M. L. Fredman, and G. C. Patton, *The AETG system: An approach to testing based on combinatorial design*, IEEE Trans. Software Engineering 23 (1997) 437–444. ⟨363⟩

[517] M. B. Cohen, *Designing Test Suites for Software Interaction Testing*, PhD thesis, University of Auckland, 2004. ⟨363, 365⟩

[518] M. B. Cohen, C. J. Colbourn, L. A. Ives, and A. C. H. Ling, *Kirkman triple*

systems of order 21 *with nontrivial automorphism group*, Math. Comp. 71 (2002) 873–881. ⟨36⟩

[519] M. B. Cohen, C. J. Colbourn, and A. C. H. Ling, *Constructing strength* 3 *covering arrays with augmented annealing*, Discrete Math. (to appear). ⟨362, 363, 365⟩

[520] C. J. Colbourn, *Hamiltonian decompositions of complete graphs*, Ars Combin. 14 (1982) 261–269. ⟨750⟩

[521] ——, *Embedding partial Steiner triple systems is NP-complete*, J. Combin. Theory A 35 (1983) 100–105. ⟨756⟩

[522] ——, *The complexity of completing partial latin squares*, Discrete Appl. Math. 8 (1984) 25–30. ⟨146, 754, 756⟩

[523] ——, *Orienting triple systems is NP-complete*, Ars Combin. 22 (1986) 155–163. ⟨70, 756⟩

[524] ——, *Simple neighbourhoods in triple systems*, J. Combin. Theory A 52 (1989) 10–19. ⟨64⟩

[525] ——, *Small group divisible designs with block size three*, J. Combin. Math. Combin. Comput. 14 (1993) 153–171. ⟨256⟩

[526] ——, *Four MOLS of order 26*, J. Combin. Math. Combin. Comput. 17 (1995) 147–148. ⟨166⟩

[527] ——, *Some direct constructions for incomplete transversal designs*, J. Stat. Plann. Infer. 56 (1996) 93–104. ⟨417⟩

[528] ——, *Transversal designs of block size eight and nine*, Europ. J. Combin. 17 (1996) 1–14. ⟨41, 43, 49, 53, 54, 220⟩

[529] ——, *Group testing for consecutive positives*, Ann. Comb. 3 (1999) 37–41. ⟨575⟩

[530] ——, *Combinatorial aspects of covering arrays*, Le Matematiche (Catania) 58 (2004) 121–167. ⟨362, 365⟩

[531] ——, *Strength two covering arrays: Existence tables and projection*, Discrete Math. (to appear). ⟨363, 365⟩

[532] C. J. Colbourn and M. J. Colbourn, *Combinatorial isomorphism problems involving 1-factorizations*, Ars Combin. 9 (1980) 191–200. ⟨503⟩

[533] ——, *Cyclic Steiner systems having multiplier automorphisms*, Utilitas Math. 17 (1980) 127–149. ⟨344⟩

[534] ——, *On cyclic Steiner systems* $S(2, 6, 91)$, Abstracts Amer. Math. Soc. 2 (1981) 463. ⟨39⟩

[535] ——, *Nested triple systems*, Ars Combin. 16 (1983) 27–34. ⟨70⟩

[536] ——, *The computational complexity of decomposing block designs*, Ann. Discrete Math. 27 (1985) 345–350. ⟨756⟩

[537] C. J. Colbourn, M. J. Colbourn, J. J. Harms, and A. Rosa, *A complete census of* (10, 3, 2) *block designs and of Mendelsohn triple systems of order ten. III.* (10, 3, 2) *block designs without repeated blocks*, Congr. Numer. 37 (1983) 211–234. ⟨36⟩

[538] C. J. Colbourn, M. J. Colbourn, and K. T. Phelps, *Combinatorial algorithms for generating cyclic Steiner quadruple systems*, in Proc. Conf. on Discrete Mathematical Analysis and Combinatorial Computation, Fredericton NB, 1980, 25–39. ⟨758⟩

[539] C. J. Colbourn, M. J. Colbourn, K. T. Phelps, and V. Rödl, *Coloring block designs is NP-complete*, SIAM J. Alg. Disc. Meth. 3 (1982) 305–307. ⟨756⟩

[540] ——, *Colouring Steiner quadruple systems*, Discrete Appl. Math. 4 (1982) 103–111. ⟨756⟩

[541] C. J. Colbourn, M. J. Colbourn, and A. Rosa, *Completing small partial triple systems*, Discrete Math. 45 (1983) 165–179. ⟨64⟩

[542] C. J. Colbourn, C. A. Cusack, and D. L. Kreher, *Partial Steiner triple systems with equal-sized holes*, J. Combin. Theory A 70 (1995) 56–65. ⟨256⟩

[543] C. J. Colbourn and J. H. Dinitz, *Making the MOLS table*, in Computational and Constructive Design Theory, W. D. Wallis, ed., Kluwer, Dordrecht, 1996, 67–134. ⟨175, 193, 194, 211, 768⟩

[544] ——, *Mutually orthogonal latin squares: A brief survey of constructions*, J. Stat. Plann. Infer. 95 (2001) 9–48. ⟨193⟩

[545] C. J. Colbourn, J. H. Dinitz, and D. R. Stinson, *More thwarts in transversal designs*, Finite Fields Appl. 2 (1996) 293–303. ⟨242, 243, 244⟩

[546] ——, *Applications of combinatorial designs to communications, cryptography, and networking*, in Surveys in Combinatorics, 1999, J. D. Lamb and D. A. Preece, eds., Cambridge Univ. Press, Cambridge, 1999, 37–100. ⟨555, 755⟩

[547] ——, *Quorum systems constructed from combinatorial designs*, Inform. Comput. 169 (2001) 160–173. ⟨366⟩

[548] C. J. Colbourn, J. H. Dinitz, and M. Wojtas, *Thwarts in transversal designs*, Des. Codes Crypt. 5 (1995) 189–197. ⟨244⟩

[549] C. J. Colbourn, P. B. Gibbons, R. Mathon, R. C. Mullin, and A. Rosa, *The spectrum of orthogonal Steiner triple systems*, Canad. J. Math. 46 (1994) 239–252. ⟨66⟩

[550] C. J. Colbourn, L. Haddad, and V. Linek, *Equitable embeddings of Steiner triple systems*, J. Combin. Theory A 73 (1996) 229–247. ⟨233⟩

[551] C. J. Colbourn, R. C. Hamm, and A. Rosa, *Embedding, immersing, and enclosing*, Congr. Numer. 47 (1985) 229–236. ⟨63⟩

[552] C. J. Colbourn and J. J. Harms, *Directing triple systems*, Ars Combin. 15 (1983) 261–266. ⟨70⟩

[553] C. J. Colbourn and K. E. Heinrich, *Conflict-free access to parallel memories*, J. Parallel Distributed Computing 14 (1992) 193–200. ⟨151⟩

[554] C. J. Colbourn, D. G. Hoffman, K. T. Phelps, V. Rödl, and P. M. Winkler, *The number of t-wise balanced designs*, Combinatorica 11 (1991) 207–218. ⟨659⟩

[555] C. J. Colbourn, D. G. Hoffman, and R. S. Rees, *A new class of group divisible designs with block size three*, J. Combin. Theory A 59 (1992) 73–89. ⟨255⟩

[556] C. J. Colbourn and Z. Jiang, *The spectrum for rotational Steiner triple systems*, J. Combin. Des. 4 (1996) 205–217. ⟨61⟩

[557] C. J. Colbourn, T. Kløve, and A. C. H. Ling, *Permutation arrays for powerline communication and mutually orthogonal latin squares*, IEEE Trans. Inform. Theory 50 (2004) 1289–1291. ⟨569, 571⟩

[558] C. J. Colbourn and D. L. Kreher, *Concerning difference matrices*, Des. Codes Crypt. 9 (1996) 61–70. ⟨414⟩

[559] C. J. Colbourn, D. L. Kreher, J. P. McSorley, and D. R. Stinson, *Orthogonal arrays of strength three from regular 3-wise balanced designs*, J. Stat. Plann. Infer. 100 (2002) 191–195. ⟨228⟩

[560] C. J. Colbourn, E. R. Lamken, A. C. H. Ling, and W. H. Mills, *The existence of Kirkman squares—Doubly resolvable $(v, 3, 1)$ BIBDs*, Des. Codes Crypt. 26 (2002) 169–196. ⟨130, 252⟩

[561] C. J. Colbourn and C. C. Lindner, *Support sizes of triple systems*, J. Combin. Theory A 61 (1992) 193–210. ⟨65⟩

[562] C. J. Colbourn and A. C. H. Ling, *Kirkman triple systems of orders 27, 33 and 39*, J. Combin. Math. Combin. Comput. 43 (2002) 3–8. ⟨38, 39, 47⟩

[563] ——, *Graph decompositions with application to wavelength add-drop multiplexing for minimizing SONET ADMs*, Discrete Math. 261 (2003) 141–156. ⟨496⟩

[564] C. J. Colbourn, A. C. H. Ling, and V. R. Syrotiuk, *Cover-free families and topology-transparent scheduling for MANETs*, Des. Codes Crypt. 32 (2004) 35–65. ⟨632⟩

[565] C. J. Colbourn and E. S. Mahmoodian, *Support sizes of sixfold triple systems*, Discrete Math. 115 (1993) 103–131. ⟨65⟩

[566] C. J. Colbourn, S. S. Martirosyan, G. L. Mullen, D. E. Shasha, G. B. Sherwood, and J. L. Yucas, *Products of mixed covering arrays of strength two*, J. Combin. Des. 14 (2006) 124–138. ⟨362, 363, 365⟩

[567] C. J. Colbourn, S. S. Martirosyan, Tran van Trung, and R. A. Walker II, *Roux-type constructions for covering arrays of strengths three and four*, Des. Codes Crypt. (to appear). ⟨362, 365⟩

[568] C. J. Colbourn and R. A. Mathon, *Leave graphs of small maximal partial triple systems*, J. Combin. Math. Combin. Comput. 2 (1987) 13–28. ⟨770⟩
[569] C. J. Colbourn, R. A. Mathon, A. Rosa, and N. Shalaby, *The fine structure of threefold triple systems: $v \equiv 1$ or 3 (mod 6)*, Discrete Math. 92 (1991) 49–64. ⟨65⟩
[570] C. J. Colbourn, R. A. Mathon, and N. Shalaby, *The fine structure of threefold triple systems: $v \equiv 5$ (mod 6)*, Australas. J. Combin. 3 (1991) 75–92. ⟨65⟩
[571] C. J. Colbourn and B. D. McKay, *Cubic neighbourhoods in triple systems*, Ann. Discrete Math. 34 (1987) 119–136. ⟨64⟩
[572] C. J. Colbourn and G. Nonay, *A golf design of order* 11, J. Stat. Plann. Infer. 58 (1997) 29–31. ⟨597⟩
[573] C. J. Colbourn and A. Rosa, *Quadratic leaves of maximal partial triple systems*, Graphs Combin. 2 (1986) 317–337. ⟨64⟩
[574] ——, *Quadratic excesses of coverings by triples*, Ars Combin. 24 (1987) 23–30. ⟨64⟩
[575] ——, *Repeated edges in 2-factorizations*, J. Graph Theory 14 (1990) 1–24. ⟨616⟩
[576] ——, *Directed and Mendelsohn triple systems*, in [724], 1992, 97–136. ⟨442, 443, 444⟩
[577] ——, *Orthogonal resolutions of triple systems*, Australas. J. Combin. 12 (1995) 259–269. ⟨132⟩
[578] ——, *Triple Systems*, Oxford University Press, Oxford, 1999. ⟨18, 22, 60, 61, 65, 67, 69, 70, 71, 110, 233, 382, 442, 444, 531, 534⟩
[579] C. J. Colbourn, A. Rosa, and D. R. Stinson, *Pairwise balanced designs with block sizes three and four*, Canad. J. Math. 43 (1991) 673–704. ⟨770⟩
[580] C. J. Colbourn and D. R. Stinson, *Edge-coloured designs with block size four*, Aequat. Math. 36 (1988) 230–245. ⟨157, 158, 214, 215⟩
[581] C. J. Colbourn, D. R. Stinson, and L. Teirlinck, *A parallelization of Miller's $n^{\log n}$ isomorphism technique*, Inform. Process. Lett. 42 (1992) 223–228. ⟨60⟩
[582] C. J. Colbourn, D. R. Stinson, and L. Zhu, *More frames with block size four*, J. Combin. Math. Combin. Comput. 23 (1997) 3–19. ⟨265⟩
[583] C. J. Colbourn and V. R. Syrotiuk, *Cover-free families and topology-transparency*, Bayreuth. Math. Schr. 74 (2005) 79–99. ⟨631, 633⟩
[584] C. J. Colbourn and P. C. van Oorschot, *Applications of combinatorial designs in computer science*, ACM Comput. Surveys 21 (1989) 223–250. ⟨755⟩
[585] C. J. Colbourn and S. A. Vanstone, *Doubly resolvable twofold triple systems*, Congr. Numer. 34 (1982) 219–223. ⟨130⟩
[586] C. J. Colbourn and L. Zhu, *The spectrum of r-orthogonal latin squares*, in Combinatorics Advances, Kluwer, New York, 1995, 49–75. ⟨190⟩
[587] M. J. Colbourn, *Cyclic Block Designs: Computational Aspects of their Construction and Analysis*, PhD thesis, University of Toronto, 1980. ⟨36, 37, 38, 39, 40, 42⟩
[588] ——, *Algorithmic aspects of combinatorial designs: A survey*, Ann. Discrete Math. 26 (1985) 67–136. ⟨779, 782⟩
[589] M. J. Colbourn and C. J. Colbourn, *Concerning the complexity of deciding isomorphism of block designs*, Discrete Appl. Math. 3 (1981) 155–162. ⟨60⟩
[590] ——, *Cyclic block designs with block size* 3, Europ. J. Combin. 2 (1981) 21–26. ⟨396, 556⟩
[591] M. J. Colbourn, C. J. Colbourn, and W. L. Rosenbaum, *Trains: An invariant for Steiner triple systems*, Ars Combin. 13 (1982) 149–162. ⟨779⟩
[592] M. J. Colbourn and R. A. Mathon, *On cyclic Steiner 2-designs*, Ann. Discrete Math. 7 (1980) 215–253. ⟨410⟩
[593] F. N. Cole, *Kirkman parades*, Bull. Amer. Math. Soc. 28 (1922) 435–437. ⟨13⟩
[594] B. J. Collings, *Generating the intrablock and interblock subgroups for confounding in general factorial experiments*, Ann. Statist. 12 (1984) 1500–1509. ⟨465⟩
[595] R. Compton, W. de Launey, and J. R. Seberry, *Generalized Hadamard matrices over sixth roots of unity*, in preparation (2006). ⟨305⟩
[596] W. S. Connor, *On the structure of balanced incomplete block designs*, Ann. Math. Stat. 23 (1952) 57–71. ⟨786⟩

[597] J. H. Conway, *Graphs and groups and M_{13}*, in Notes from New York Graph Theory Day XIV, 1987, 18–29. ⟨544⟩
[598] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, Eynsham, 1985, 2003. ⟨820⟩
[599] J. H. Conway, A. Hulpke, and J. McKay, *On transitive permutation groups*, LMS J. Comput. Math. 1 (1998) 1–8. ⟨764⟩
[600] J. H. Conway and V. S. Pless, *On the enumeration of self-dual codes*, J. Combin. Theory A 28 (1980) 26–53. ⟨688⟩
[601] ——, *On primes dividing the group order of a doubly-even* (72, 36, 16) *code and the group order of a quaternary* (24, 12, 10) *code*, Discrete Math. 38 (1982) 143–156. ⟨690⟩
[602] J. H. Conway and N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory 36 (1990) 1319–1333. ⟨689⟩
[603] ——, *Sphere Packings, Lattices and Groups*, Springer, New York, 3rd ed., 1999. ⟨622⟩
[604] K. Coolsaet and J. Degraer, *Classification of some strongly regular subgraphs of the McLaughlin graph*, Discrete Math. (to appear). ⟨858, 859, 861⟩
[605] K. Coolsaet, J. Degraer, and E. Spence, *The strongly regular* $(45, 12, 3, 3)$ *graphs*, Electron. J. Comb. 13 (2006) R32. ⟨855⟩
[606] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, M.I.T. Press, Cambridge, 2nd ed., 2001. ⟨780⟩
[607] D. G. Corneil and R. A. Mathon, *Algorithmic techniques for the generation and analysis of strongly regular graphs and other combinatorial configurations*, Ann. Discrete Math. 2 (1978) 1–32. ⟨42⟩
[608] J. P. Costas, *A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties*, Proc. IEEE 72 (1984) 996–1009. ⟨360⟩
[609] E. Cousins and W. D. Wallis, *Maximal sets of one-factors*, Lect. Notes Math. 452 (1975) 90–94. ⟨754⟩
[610] H. S. M. Coxeter, *Self-dual configurations and regular graphs*, Bull. Amer. Math. Soc. 56 (1950) 413–455. ⟨855⟩
[611] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, Springer, Berlin, 1965. ⟨877⟩
[612] R. Craigen, *A new class of weighing matrices with square weights*, Bull. Inst. Combin. Appl. 3 (1991) 33–42. ⟨289, 295⟩
[613] ——, *The craft of weaving matrices*, Congr. Numer. 92 (1993) 9–28. ⟨289, 295⟩
[614] ——, *The structure of weighing matrices having large weights*, Des. Codes Crypt. 5 (1995) 199–216. ⟨288⟩
[615] R. Craigen, J. R. Seberry, and X.-M. Zhang, *Product of four Hadamard matrices*, J. Combin. Theory A 59 (1992) 318–320. ⟨275⟩
[616] R. Craigen and W. D. Wallis, *Hadamard matrices: 1893–1993*, Congr. Numer. 97 (1993) 99–129. ⟨280⟩
[617] R. Craigen and R. Woodford, *Power Hadamard matrices*, preprint (2004). ⟨306⟩
[618] F. Cretté de Palluel, *Sur les avantages et l'économie que procurent les racines employées à l'engrais les moutons à l'étable*, Mémoires d'Agriculture 14 (1788) 17–23. ⟨17⟩
[619] D. Crnković and D. Held, *Some Hadamard designs with parameters* $(71, 35, 17)$, J. Combin. Des. 10 (2002) 144–149. ⟨51⟩
[620] D. Crnković and S. Rukavina, *Some symmetric* $(47, 23, 11)$ *designs*, Glas. Mat. III 38(58) (2003) 1–9. ⟨41, 42⟩
[621] A. B. Cruse, *On embedding incomplete symmetric latin squares*, J. Combin. Theory A 16 (1974) 18–27. ⟨158, 159⟩
[622] A. B. Cruse and C. C. Lindner, *Small embeddings for partial semisymmetric and totally symmetric quasigroups*, J. London Math. Soc. 12 (1976) 479–484. ⟨159⟩
[623] D. J. Curran and S. A. Vanstone, *Doubly resolvable designs from generalized Bhaskar Rao designs*, Discrete Math. 73 (1989) 49–63. ⟨39, 45⟩

[624] S. J. Curran and J. A. Gallian, *Hamiltonian cycles and paths in Cayley graphs and digraphs—A survey*, Discrete Math. 156 (1996) 1–18. ⟨375⟩
[625] C. A. Cusack, D. L. Kreher, and S. W. Graham, *Large sets of 3-designs from $PSL(2,q)$, with block sizes 4 and 5*, J. Combin. Des. 3 (1995) 147–160. ⟨98⟩
[626] T. Czerwinski and D. Oakden, *The translation planes of order twenty-five*, J. Combin. Theory A 59 (1992) 193–217. ⟨727⟩
[627] P. Danziger, *Uniform restricted resolvable designs with $r = 3$*, Ars Combin. 46 (1997) 161–176. ⟨131, 132⟩
[628] P. Danziger and E. Mendelsohn, *Uniformly resolvable designs*, J. Combin. Math. Combin. Comput. 21 (1996) 65–83. ⟨131⟩
[629] P. Danziger and B. Stevens, *Class-uniformly resolvable group divisible structures I: Resolvable group divisible designs*, Electron. J. Comb. 11 (2004) 13 pp. ⟨265⟩
[630] ———, *Class-uniformly resolvable group divisible structures II: Frames*, Electron. J. Comb. 11 (2004) 17 pp. ⟨265⟩
[631] A. Das, A. M. Dean, and S. Gupta, *On optimality of some partial diallel cross designs*, Sankhyā B 60 (1998) 511–524. ⟨562, 564⟩
[632] D. H. Davies, *Flag-transitivity and primitivity*, Discrete Math. 63 (1987) 91–93. ⟨342⟩
[633] C. Davis, B. Grünbaum, and F. A. Sherk, eds., *The Geometric Vein*, Springer, New York, 1981. ⟨622⟩
[634] E. W. Davis, *A geometric picture of the fifteen school-girl problem*, Ann. Math. 11 (1897) 156–157. ⟨13⟩
[635] J. A. Davis and J. Jedwab, *A unifying construction for difference sets*, J. Combin. Theory A 80 (1997) 13–78. ⟨117⟩
[636] J. A. Davis, J. Jedwab, and K. W. Smith, *Proof of the Barker array conjecture*, Proc. Amer. Math. Soc. (to appear). ⟨317⟩
[637] J. A. Davis and K. Smith, *A construction of difference sets in high exponent 2-groups using representation theory*, J. Algeb. Combin. 3 (1994) 137–151. ⟨425⟩
[638] M. de Brandes, K. T. Phelps, and V. Rödl, *Coloring Steiner triple systems*, SIAM J. Alg. Disc. Meth. 3 (1982) 241–249. ⟨69⟩
[639] N. G. de Bruijn and P. Erdős, *On a combinatorial problem*, Nederl. Akad. Wetensch., Proc. 51 (1948) 1277–1279 = Indagationes Math. 10, 421–423 (1948). ⟨266⟩
[640] D. de Caen and D. G. Hoffman, *Impossibility of decomposing the complete graph on n points into $n-1$ isomorphic complete bipartite graphs*, SIAM J. Disc. Math. 2 (1989) 48–50. ⟨482⟩
[641] D. de Caen and D. L. Kreher, *The 3-hypergraphical Steiner quadruple systems of order twenty*, in Graphs, Matrices and Designs, R. S. Rees, ed., Dekker, New York, 1993, 85–92. ⟨493⟩
[642] F. De Clerck, *New partial geometries constructed from old ones*, Bull. Belg. Math. Soc. Simon Stevin 5 (1998) 255–263. ⟨560⟩
[643] F. De Clerck, M. Delanote, N. Hamilton, and R. A. Mathon, *Perp-systems and partial geometries*, Adv. Geom. 2 (2002) 1–12. ⟨560⟩
[644] F. De Clerck and H. Van Maldeghem, *Some classes of rank 2 geometries*, in Handbook of Incidence Geometry, North-Holland, Amsterdam, 1995, 433–475. ⟨559, 560, 561⟩
[645] W. de Launey, *Generalised Hadamard matrices whose rows and columns form a group*, Lect. Notes Math. 1036 (1983) 154–176. ⟨306⟩
[646] ———, *On the nonexistence of generalised weighing matrices*, Ars Combin. A17 (1984) 117–132. ⟨302⟩
[647] ———, *A survey of generalized Hadamard matrices and difference matrices $D(k,\lambda;G)$ with large k*, Utilitas Math. 30 (1986) 5–29. ⟨302, 413⟩
[648] ———, *$(0,G)$-Designs and Applications*, PhD thesis, University of Sydney, 1987. ⟨299, 300, 413⟩

[649] ——, *On difference matrices, transversal designs, resolvable transversal designs, and large sets of mutually orthogonal F-squares*, J. Stat. Plann. Infer. 16 (1987) 107–125. ⟨413⟩
[650] ——, *Square GBRDs over nonabelian groups*, Ars Combin. 27 (1989) 40–49. ⟨302⟩
[651] ——, *On the construction of n-dimensional designs from 2-dimensional designs*, Australas. J. Combin. 1 (1990) 67–81. ⟨304⟩
[652] ——, *Generalised Hadamard matrices which are developed modulo a group*, Discrete Math. 104 (1992) 49–65. ⟨305⟩
[653] ——, *A technique for constructing cocyclic generalized Hadamard matrices*, in preparation (2006). ⟨304⟩
[654] W. de Launey and J. E. Dawson, *A note on the construction of* $\mathrm{GH}(4tq; \mathrm{EA}(q))$ *for* $t = 1, 2$, Australas. J. Combin. 6 (1992) 177–186. ⟨302⟩
[655] ——, *An asymptotic result on the existence of generalised Hadamard matrices*, J. Combin. Theory A 65 (1994) 158–163. ⟨302⟩
[656] W. de Launey, D. L. Flannery, and K. J. Horadam, *Cocyclic Hadamard matrices and difference sets*, Discrete Appl. Math. 102 (2000) 47–61. ⟨280⟩
[657] W. de Launey and D. G. Sarvate, *Nonexistence of certain GBRDs*, Ars Combin. 18 (1984) 5–20. ⟨300, 313⟩
[658] W. de Launey and M. J. Smith, *Cocyclic orthogonal designs and the asymptotic existence of cocyclic Hadamard matrices and maximal size relative difference sets with forbidden subgroup of size* 2, J. Combin. Theory A 93 (2001) 37–92. ⟨280⟩
[659] V. de Pasquale, *Sui sistemi ternari di* 13 *elementi*, Rend. R. Ist. Lombardo Sci. Lett. 32 (1899) 213–221. ⟨15⟩
[660] M. J. de Resmini, *On the Mathon plane*, J. Geom. 60 (1997) 47–64. ⟨38⟩
[661] M. J. de Resmini and N. Hamilton, *Hyperovals and unitals in Figueroa planes*, Europ. J. Combin. 19 (1998) 215–220. ⟨728⟩
[662] M. J. de Resmini and A. O. Leone, *Subplanes of the derived Hughes plane of order* 25, Simon Stevin 67 (1993) 289–322. ⟨729⟩
[663] D. de Werra, *Scheduling in sports*, Ann. Discrete Math. 11 (1981) 381–395. ⟨593⟩
[664] J. Degraer and K. Coolsaet, *Classification of three-class association schemes using backtracking with dynamic variable ordering*, Discrete Math. 300 (2005) 71–81. ⟨762⟩
[665] I. J. Dejter, F. Franek, E. Mendelsohn, and A. Rosa, *Triangles in* 2*-factorizations*, J. Graph Theory 26 (1997) 83–94. ⟨375, 376⟩
[666] I. J. Dejter, P. I. Rivera-Vega, and A. Rosa, *Invariants for* 2*-factorizations and cycle systems*, J. Combin. Math. Combin. Comput. 16 (1994) 129–152. ⟨375⟩
[667] A. Delandtsheer, *Classifications of finite highly transitive dimensional linear spaces*, Discrete Math. 129 (1994) 75–111. ⟨341⟩
[668] ——, *Dimensional linear spaces*, in Handbook of Incidence Geometry, North-Holland, Amsterdam, 1995, 193–294. ⟨512⟩
[669] A. Delandtsheer and J. Doyen, *Most block-transitive t-designs are point-primitive*, Geom. Ded. 29 (1989) 307–310. ⟨343⟩
[670] A. Delandtsheer, J. Doyen, J. Siemons, and C. Tamburini, *Doubly homogeneous* 2*-*$(v, k, 1)$ *designs*, J. Combin. Theory A 43 (1986) 140–145. ⟨342⟩
[671] A. Delandtsheer, A. C. Niemeyer, and C. E. Praeger, *Finite line-transitive linear spaces: Parameters and normal point-partitions*, Adv. Geom. 3 (2003) 469–485. ⟨344, 510⟩
[672] P. Delsarte, *Weights of linear codes and strongly regular normed spaces*, Discrete Math. 3 (1972) 47–64. ⟨695, 855⟩
[673] ——, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. No. 10 (1973). ⟨325, 329, 330, 789, 855⟩
[674] ——, *Four fundamental parameters of a code and their combinatorial significance*, Inf. Control 23 (1973) 407–438. ⟨225, 684⟩
[675] P. Delsarte, J.-M. Goethals, and J. J. Seidel, *Orthogonal matrices with zero diagonal II*, Canad. J. Math. 23 (1971) 816–832. ⟨878⟩

[676] ———, *Bounds for systems of lines and Jacobi polynomials*, Philips Res. Rep. 30 (1975) 91–105. ⟨855⟩
[677] ———, *Spherical codes and designs*, Geom. Ded. 6 (1977) 363–388. ⟨622⟩
[678] P. Dembowski, *Möbiusebenen gerader Ordnung*, Math. Ann. 157 (1964) 179–205. ⟨103⟩
[679] ———, *Finite Geometries*, Springer, Berlin, 1968. ⟨36, 43, 45, 49, 720, 729, 730⟩
[680] U. Dempwolff, *Translation planes of order* 27, Des. Codes Crypt. 4 (1994) 105–121. ⟨727⟩
[681] ———, *Primitive rank* 3 *groups on symmetric designs*, Des. Codes Crypt. 22 (2001) 191–207. ⟨112, 118⟩
[682] ———, *Affine rank* 3 *groups on symmetric designs*, Des. Codes Crypt. 31 (2004) 159–168. ⟨112⟩
[683] U. Dempwolff and A. Reifart, *The classification of the translation planes of order* 16 *I*, Geom. Ded. 15 (1983) 137–153. ⟨727⟩
[684] J. Dénes and A. D. Keedwell, *Latin Squares and Their Applications*, English Universities Press, London, 1974. ⟨136, 152, 159, 352, 748⟩
[685] ———, *Latin Squares: New Developments in the Theory and Applications*, North-Holland, Amsterdam, 1991. ⟨143, 152, 352, 465, 466, 468, 469, 471⟩
[686] J. Dénes and G. L. Mullen, *Enumeration formulas for latin and frequency squares*, Discrete Math. 111 (1993) 157–163. ⟨748⟩
[687] D. Deng, M. Greig, and P. R. J. Östergård, *More c-Bhaskar Rao designs with small block size*, Discrete Math. 261 (2003) 189–208. ⟨301⟩
[688] R. H. F. Denniston, *Some maximal arcs in finite projective planes*, J. Combin. Theory 6 (1969) 317–319. ⟨48⟩
[689] ———, *On arcs in projective planes of order* 9, Manuscripta Math. 4 (1971) 61–89. ⟨727⟩
[690] ———, *Sylvester's problem of the* 15 *school-girls*, Discrete Math. 9 (1974) 229–233. ⟨13, 66⟩
[691] ———, *Some new* 5*-designs*, Bull. London Math. Soc. 8 (1976) 263–267. ⟨87, 89, 107⟩
[692] ———, *On biplanes with* 56 *points*, Ars Combin. 9 (1980) 167–179. ⟨36⟩
[693] ———, *A Steiner system with a maximal arc*, Ars Combin. 9 (1980) 247–248. ⟨37⟩
[694] ———, *Enumeration of symmetric designs* (25, 9, 3), Ann. Discrete Math. 15 (1982) 111–127. ⟨36⟩
[695] ———, *A small* 4*-design*, Ann. Discrete Math. 18 (1983) 291–294. ⟨85⟩
[696] P. C. Denny, *Search and enumeration techniques for incidence structures*, Tech. Report CDMTCS-085, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, 1998. ⟨36, 40, 54, 758, 782⟩
[697] P. C. Denny and P. B. Gibbons, *Case studies and new results in combinatorial enumeration*, J. Combin. Des. 8 (2000) 239–260. ⟨50, 533, 534, 762, 775, 776⟩
[698] M. Deza, *Pavage généralisé parfait comme généralisation de matroïde-configurations et de simples t-configurations*, in Problèmes Combinatoires et Théorie des Graphes, CNRS, Paris, 1978, 99–102. ⟨852⟩
[699] M. Deza, R. C. Mullin, and S. A. Vanstone, *Recent results on* (r, λ)*-designs and related configurations*, Rev. Técn. Fac. Ingr. Univ. Zulia 4 (1981) 139–158. ⟨583⟩
[700] M. Deza and S. A. Vanstone, *Bounds for permutation arrays*, J. Stat. Plann. Infer. 2 (1978) 197–209. ⟨569⟩
[701] C. S. Dibley and W. D. Wallis, *The effect of starting position in jai-alai*, Congr. Numer. 32 (1981) 253–259. ⟨605, 606⟩
[702] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*, Dover, New York, 1958. ⟨820, 842⟩
[703] L. E. Dickson and F. H. Safford, *Solution to problem 8 (group theory)*, Amer. Math. Monthly 13 (1906) 150–151. ⟨15⟩
[704] J. F. Dillon, *Elementary Hadamard Difference Sets*, PhD thesis, University of Maryland, 1974. ⟨338, 339⟩

[705] ——, *Variations on a scheme of McFarland for noncyclic difference sets*, J. Combin. Theory A 40 (1985) 9–21. ⟨426⟩
[706] ——, *Multiplicative difference sets via additive characters*, Des. Codes Crypt. 17 (1999) 225–235. ⟨423⟩
[707] J. F. Dillon and H. Dobbertin, *New cyclic difference sets with Singer parameters*, Finite Fields Appl. 10 (2004) 342–389. ⟨314, 423⟩
[708] J. F. Dillon and J. R. Schatz, *Block designs with the symmetric difference property*, in Proceedings NSA Mathematical Sciences Meetings, U.S. Government Printing Office, Washington DC, 1987, 159–164. ⟨695⟩
[709] C. Ding, T. Helleseth, and H. Martinsen, *New families of binary sequences with optimal three-level autocorrelation*, IEEE Trans. Inform. Theory 47 (2001) 428–433. ⟨315⟩
[710] Y. Ding, S. K. Houghten, C. W. H. Lam, S. Smith, L. H. Thiel, and V. D. Tonchev, *Quasi-symmetric* 2-$(28, 12, 11)$ *designs with an automorphism of order* 7, J. Combin. Des. 6 (1998) 213–223. ⟨44, 45, 580⟩
[711] J. H. Dinitz and M. H. Dinitz, *Enumeration of balanced tournament designs on* 10 *points*, J. Combin. Math. Combin. Comput. 52 (2005) 51–63. ⟨334, 762⟩
[712] J. H. Dinitz, P. J. Dukes, and A. C. H. Ling, *Sets of three pairwise orthogonal Steiner triple systems*, J. Combin. Theory A 101 (2003) 90–116. ⟨66, 770⟩
[713] J. H. Dinitz and D. K. Garnick, *Holey factorizations*, Ars Combin. 44 (1996) 65–92. ⟨588⟩
[714] ——, *There are* 23 *nonisomorphic perfect one-factorizations of* K_{14}, J. Combin. Des. 4 (1996) 1–4. ⟨753, 762⟩
[715] J. H. Dinitz, D. K. Garnick, and B. D. McKay, *There are* $526,915,620$ *nonisomorphic* 1*-factorizations of* K_{12}, J. Combin. Des. 2 (1994) 273–285. ⟨15, 743, 751, 762, 768, 775, 781⟩
[716] J. H. Dinitz and E. R. Lamken, *Uniform Room frames with five holes*, J. Combin. Des. 1 (1993) 323–328. ⟨588⟩
[717] ——, *Howell designs with sub-designs*, J. Combin. Theory A 65 (1994) 268–301. ⟨503, 770⟩
[718] J. H. Dinitz and P. Rodney, *Disjoint difference families with block size* 3, Utilitas Math. 52 (1997) 153–160. ⟨485⟩
[719] J. H. Dinitz and N. Shalaby, *Block disjoint difference families for Steiner triple systems:* $v \equiv 3 \pmod 6$, J. Stat. Plann. Infer. 106 (2002) 77–86. ⟨396⟩
[720] J. H. Dinitz and D. R. Stinson, *A fast algorithm for finding strong starters*, SIAM J. Alg. Disc. Meth. 2 (1981) 50–56. ⟨770⟩
[721] ——, *MOLS with holes*, Discrete Math. 44 (1983) 145–154. ⟨211⟩
[722] ——, *A hill-climbing algorithm for the construction of one-factorizations and Room squares*, SIAM J. Alg. Disc. Meth. 8 (1987) 430–438. ⟨770⟩
[723] ——, *Some new perfect one-factorizations from starters in finite fields*, J. Graph Theory 13 (1989) 405–415. ⟨759⟩
[724] ——, eds., *Contemporary Design Theory*, Wiley, 1992. ⟨886, 890, 905⟩
[725] ——, *Room squares and related designs*, in [724], 1992, 137–204. ⟨190, 191, 193, 503, 504, 586, 590, 600, 622, 624, 628, 742, 755⟩
[726] ——, *A few more Room frames*, in Graphs, Matrices and Designs, R. S. Rees, ed., Dekker, New York, 1993, 133–146. ⟨588, 770⟩
[727] ——, *On assigning referees to tournament schedules*, Bull. Inst. Combin. Appl. 44 (2005) 22–28. ⟨589, 596⟩
[728] ——, *On the maximum number of different ordered pairs of symbols in sets of latin squares*, J. Combin. Des. 13 (2005) 1–15. ⟨192⟩
[729] J. H. Dinitz, D. R. Stinson, and L. Zhu, *On the spectra of certain classes of Room frames*, Electron. J. Comb. 1 (1994). #R7. ⟨587, 588⟩
[730] J. H. Dinitz and W. D. Wallis, *Four orthogonal one-factorizations on ten points*, Ann. Discrete Math. 26 (1985) 143–150. ⟨590⟩
[731] ——, *Trains: An invariant for one-factorizations*, Ars Combin. 32 (1991) 161–180. ⟨780⟩

[732] J. D. Dixon and B. Mortimer, *The primitive permutation groups of degree less than* 1000, Math. Proc. Cambridge Philos. Soc. 103 (1988) 213–238. ⟨825⟩
[733] H. Dobbertin, *Kasami power functions, permutation polynomials and cyclic difference sets*, in Difference Sets, Sequences and Their Correlation Properties, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, eds., Kluwer, 1999, 133–158. ⟨423⟩
[734] P. Dobcsányi and L. H. Soicher, *An online collection of $t-$designs.* `http://designtheory.org/database/t-designs/` (2005). ⟨37, 38, 39⟩
[735] E. Dobson, *Packing almost stars into the complete graph*, J. Graph Theory 25 (1997) 169–172. ⟨479⟩
[736] S. M. Dodunekov, S. B. Encheva, and S. N. Kapralov, *On the* $[28, 7, 12]$ *binary self-complementary codes and their residuals*, Des. Codes Crypt. 4 (1994) 57–67. ⟨701⟩
[737] D. Ž. Đoković, *Some new D-optimal designs*, Australas. J. Combin. 15 (1997) 221–231. ⟨298⟩
[738] ———, *Aperiodic complementary quadruples of binary sequences*, J. Combin. Math. Combin. Comput. 27 (1998) 3–31. ⟨319, 321⟩
[739] ———, *Equivalence classes and representatives of Golay sequences*, Discrete Math. 189 (1998) 79–93. ⟨318⟩
[740] ———, *Note on periodic complementary sets of binary sequences*, Des. Codes Crypt. 13 (1998) 251–256. ⟨318, 319, 321⟩
[741] D. Donovan, A. Khodkar, and A. P. Street, *Doubling and tripling constructions for defining sets in Steiner triple systems*, Graphs Combin. 19 (2003) 65–89. ⟨384⟩
[742] D. Donovan, E. S. Mahmoodian, C. Ramsay, and A. P. Street, *Defining sets in combinatorics: A survey*, in Surveys in Combinatorics, 2003, C. D. Wensley, ed., Cambridge Univ. Press, Cambridge, 2003, 115–174. ⟨383, 384, 385⟩
[743] D. Dor and M. Tarsi, *Graph decomposition is NP-complete: A complete proof of Holyer's conjecture*, SIAM J. Comput. 26 (1997) 1166–1187. ⟨478⟩
[744] J. Doyen, *Sur le nombre d'espaces linéaires non isomorphes de n points*, Bull. Soc. Math. Belg. 19 (1967) 421–437. ⟨269⟩
[745] ———, *Systèmes triples de Steiner non engendrés par tous leurs triangles*, Math. Zeitschr. 118 (1970) 197–206. ⟨63⟩
[746] J. Doyen, X. Hubaut, and M. Vandensavel, *Ranks of incidence matrices of Steiner triple systems*, Math. Zeitschr. 163 (1978) 251–259. ⟨687, 691, 788⟩
[747] J. Doyen and R. M. Wilson, *Embeddings of Steiner triple systems*, Discrete Math. 5 (1973) 229–239. ⟨63⟩
[748] D. A. Drake, *Partial λ-geometries and generalized Hadamard matrices over groups*, Canad. J. Math. 31 (1979) 617–627. ⟨302, 411⟩
[749] D. A. Drake and J. A. Larson, *Pairwise balanced designs whose line sizes do not divide* 6, J. Combin. Theory A 34 (1983) 266–300. ⟨247⟩
[750] D. A. Drake and W. J. Myrvold, *The non-existence of maximal sets of four mutually orthogonal latin squares of order* 8, Des. Codes Crypt. 33 (2004) 63–69. ⟨189⟩
[751] D. A. Drake, G. H. J. Van Rees, and W. D. Wallis, *Maximal sets of mutually orthogonal latin squares*, Discrete Math. 194 (1999) 87–94. ⟨189⟩
[752] A. Drápal, *On a planar construction of quasigroups*, Czechoslovak Math. J. 41 (1991) 538–548. ⟨148⟩
[753] L. M. H. E. Driessen, *t-Designs, $t \geq 3$*, Tech. Report, Department of Mathematics, Eindhoven University of Technology, 1978. ⟨82, 85, 86, 87⟩
[754] A. A. Drisko, *On the number of even and odd latin squares of order $p + 1$*, Adv. Math. 128 (1997) 20–35. ⟨151⟩
[755] B. Du, *Some constructions of pairwise orthogonal diagonal latin squares*, J. Combin. Math. Combin. Comput. 9 (1991) 97–106. ⟨191⟩
[756] ———, *A few more resolvable spouse-avoiding mixed-doubles round robin tournaments*, Ars Combin. 36 (1993) 309–314. ⟨216⟩

[757] B. Du and L. Zhu, *The existence of incomplete Room squares*, J. Combin. Math. Combin. Comput. 14 (1993) 183–192. ⟨587⟩
[758] D.-Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, World Scientific, Singapore, 2nd ed., 2000. ⟨575, 630, 633⟩
[759] P. J. Dukes and A. C. H. Ling, *A combinatorial error bound for t-point based sampling*, Theor. Comput. Sci. 310 (2004) 479–488. ⟨390⟩
[760] P. J. Dukes and R. M. Wilson, *The cone condition and t-designs*, preprint. ⟨788⟩
[761] C. F. Dunkl, *Discrete quadrature and bounds on t-designs*, Michigan Math. J. 26 (1979) 81–102. ⟨102⟩
[762] R. Dutta and N. Rouskas, *Traffic grooming in WDM networks: Past and future*, IEEE Network 16 (2002) 46–56. ⟨494⟩
[763] A. Duval, *A directed graph version of strongly regular graphs*, J. Combin. Theory A 47 (1988) 71–100. ⟨869, 870, 872⟩
[764] A. G. D'yachkov, A. J. Macula, and P. A. Vilenkin, *Nonadaptive and trivial two-stage group testing with error-correcting d^e-disjunct inclusion matrices*, preprint. ⟨631⟩
[765] A. G. D'yachkov and V. V. Rykov, *Bounds on the length of disjunct codes*, Problems Control Inform. Theory 11 (1982) 7–13. ⟨630⟩
[766] A. G. D'yachkov, V. V. Rykov, and A. M. Rashad, *Superimposed distance codes*, Problems Control Inform. Theory 18 (1989) 237–250. ⟨630⟩
[767] A. G. D'yachkov, P. Vilenkin, A. Macula, and D. Torney, *Families of finite sets in which no intersection of l sets is covered by the union of s others*, J. Combin. Theory A 99 (2002) 195–218. ⟨632⟩
[768] P. Eades, *Integral quadratic forms and orthogonal designs*, J. Austral. Math. Soc. A 30 (1980/81) 297–306. ⟨293⟩
[769] O. Eckenstein, *Bibliography of Kirkman's school-girl problem*, Messenger Math. 41 (1912) 33–36. ⟨13⟩
[770] A. R. Eckler, *Construction of missile guidance codes resistant to random interference*, Bell Syst. Tech. J. (1960) 973–994. ⟨616⟩
[771] H. Ehlich, *Determinantenabschätzung für binäre Matrizen mit $n \equiv 3 \bmod 4$*, Math. Zeitschr. 84 (1964) 438–447. ⟨297⟩
[772] B. Eick and B. Höfling, *The solvable primitive permutation groups of degree at most* 6560, LMS J. Comput. Math. 6 (2003) 29–39. ⟨825⟩
[773] P. A. Eisen and D. R. Stinson, *Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels*, Des. Codes Crypt. 25 (2002) 15–61. ⟨639⟩
[774] S. I. El-Zanati, C. V. Eynden, and N. Punnim, *On the cyclic decomposition of complete graphs into bipartite graphs*, Australas. J. Combin. 24 (2001) 209–219. ⟨483⟩
[775] S. I. El-Zanati, S. K. Tipnis, and C. Vanden Eynden, *A generalization of the Oberwolfach problem*, J. Graph Theory 41 (2002) 151–161. ⟨377⟩
[776] S. I. El-Zanati and C. Vanden Eynden, *Factorizations of complete multipartite graphs into generalized cubes*, J. Graph Theory 33 (2000) 144–150. ⟨481⟩
[777] ———, *Decomposing complete graphs into cubes*, Discuss. Math. (to appear). ⟨480⟩
[778] A. S. Eldin, N. Shalaby, and F. Al-Thukair, *Construction of Skolem sequences*, Int. J. Comput. Math. 70 (1998) 333–345. ⟨770⟩
[779] B. Elenbogen and B. Maxim, *Scheduling a bridge club (a case study in discrete optimization)*, Math. Mag. 65 (1992) 18–26. ⟨602⟩
[780] S. Eliahou and M. Kervaire, *A survey on modular Hadamard matrices*, Discrete Math. 302 (2005) 85–106. ⟨280⟩
[781] M. N. Ellingham, *Isomorphic factorization of r-regular graphs into r parts*, Discrete Math. 69 (1988) 19–34. ⟨486⟩
[782] M. N. Ellingham and N. C. Wormald, *Isomorphic factorization of regular graphs and 3-regular multigraphs*, J. London Math. Soc. 37 (1988) 14–24. ⟨485⟩
[783] J. R. Elliott and P. B. Gibbons, *The construction of subsquare free latin squares by simulated annealing*, Australas. J. Combin. 5 (1992) 209–228. ⟨772⟩

[784] K. Engel, *Über die Anzahl elementarer, teilweise balancierter, unvollständiger Blockpläne*, Rostock. Math. Kolloq. 13 (1980) 19–41. ⟨70⟩
[785] ——, *Optimalitätsaussagen über Tripelsysteme*, Rostock. Math. Kolloq. 17 (1981) 17–26. ⟨64⟩
[786] P. Erdős, *Problems and results in combinatorial analysis*, Creation in Mathematics 9 (1976) 25. ⟨69⟩
[787] ——, *On the combinatorial problems which I would most like to see solved*, Combinatorica 1 (1981) 25–42. ⟨67⟩
[788] D. L. Erickson and C. J. Colbourn, *Conflict-free access to rectangular subarrays of constant perimeter*, in Interconnection Networks and Mapping and Scheduling Parallel Computations, ACM/DIMACS, 1995, 105–124. ⟨151⟩
[789] T. Ericson and V. Zinoviev, *Codes on Euclidean Spheres*, North-Holland, Amsterdam, 2001. ⟨622⟩
[790] Z. Eslami, *Classification of designs with nontrivial automorphism groups*, J. Combin. Des. (to appear). ⟨36⟩
[791] Z. Eslami and G. B. Khosrovshahi, *Algorithmic aspects of trades*, preprint. ⟨769⟩
[792] T. Etzion, *Combinatorial designs derived from Costas arrays*, in Sequences, R. M. Capocelli, ed., Springer, New York, 1990, 208–227. ⟨359, 360⟩
[793] ——, *Optimal constant weight codes over $\mathbb{Z}_k$ and generalized designs*, Discrete Math. 169 (1997) 55–82. ⟨259, 555⟩
[794] T. Etzion, S. W. Golomb, and H. Taylor, *Tuscan-k squares*, Adv. Appl. Math. 10 (1989) 164–174. ⟨655, 656⟩
[795] T. Etzion and A. Hartman, *Towards a large set of Steiner quadruple systems*, SIAM J. Disc. Math. 4 (1991) 182–195. ⟨98⟩
[796] T. Etzion and A. Vardy, *Perfect binary codes: constructions, properties, and enumeration*, IEEE Trans. Inform. Theory 40 (1994) 754–763. ⟨680⟩
[797] T. Etzion, V. Wei, and Z. Zhang, *Bounds on the size of constant weight covering codes*, Des. Codes Crypt. 5 (1995) 217–239. ⟨519⟩
[798] L. Euler, *Recherches sur une nouvelle espèce de quarrés magiques*, Verh. Zeeuw. Gen. Weten. Vlissengen 9 (1782) 85–239. ⟨11, 15, 193⟩
[799] A. B. Evans, *On orthogonal orthomorphisms of cyclic and non-abelian groups II*, preprint. ⟨346, 412⟩
[800] ——, *Orthomorphism Graphs of Groups*, Springer, New York, 1992. ⟨193, 352⟩
[801] ——, *Latin squares without orthogonal mates*, Des. Codes Crypt. 40 (2006) 121–130. ⟨189⟩
[802] D. M. Evans, *Block transitive Steiner systems with more than one point orbit*, J. Combin. Des. 12 (2004) 459–465. ⟨505⟩
[803] T. Evans, *Embedding incomplete latin squares*, Amer. Math. Monthly 67 (1960) 958–961. ⟨146, 147, 159⟩
[804] ——, *Algebraic structures associated with latin squares and orthogonal arrays*, Congr. Numer. 13 (1975) 31–52. ⟨153, 155, 156⟩
[805] K. T. Fang, G. Ge, M. Q. Liu, and H. Qin, *Combinatorial constructions for optimal supersaturated designs*, Discrete Math. 279 (2004) 191–202. ⟨453⟩
[806] W. Fang and H. Li, *A generalization of the Camina–Gagen theorem*, Chinese J. Math. (Wuhan 13) 4 (1993) 437–442. ⟨342, 344⟩
[807] G. Fano, *Sui postulari fondamenti della geometria proiettiva*, Giornale di Matematiche 30 (1892) 106–132. ⟨16⟩
[808] I. A. Faradžev, *Constructive enumeration of combinatorial objects*, in Problèmes Combinatoires et Théorie des Graphes, Paris, 1978, CNRS, 131–135. ⟨761⟩
[809] W. T. Federer and J. P. Mandeli, *Orthogonal F-rectangles, orthogonal arrays and codes*, J. Combin. Theory A 43 (1986) 149–164. ⟨471⟩
[810] K. Feng, P. J.-S. Shiue, and Q. Xiang, *On aperiodic and periodic complementary binary sequences*, IEEE Trans. Inform. Theory 45 (1999) 296–303. ⟨321⟩

[811] H. C. Ferreira and A. J. H. Vinck, *Interference cancellation with permutation trellis codes*, Proc. IEEE Vehicular Technology Conference 5 (2000) 2401–2407. ⟨571⟩
[812] N. C. Fiala, *λ-designs on $8p+1$ points*, Ars Combin. 68 (2003) 17–32. ⟨115⟩
[813] F. Fiedler, M. Klin, and M. Muzychuk, *Small vertex-transitive directed strongly regular graphs*, Discrete Math. 255 (2002) 87–115. ⟨870, 872⟩
[814] F. Fiedler, M. Klin, and C. Pech, *Directed strongly regular graphs as elements of coherent algebras*, in Proc. Conf. General Algebra and Discrete Mathematics, K. Denecke and H.-J. Vogel, eds., Shaker Verlag, Aachen, 1999, 69–87. ⟨870⟩
[815] N. J. Finizio, *Tournament designs balanced with respect to several bias categories*, Bull. Inst. Combin. Appl. 9 (1993) 69–95. ⟨336, 594, 595⟩
[816] ———, *Some quick and easy SOLSSOMs*, Congr. Numer. 99 (1994) 307–313. ⟨219⟩
[817] D. J. Finney, *The fractional replication of factorial arrangements*, Ann. Eugenics 12 (1945) 291–301. ⟨19⟩
[818] R. A. Fisher, *The arrangement of field experiments*, J. Ministry Agriculture 33 (1926) 503–513. ⟨17⟩
[819] ———, *An examination of the different possible solutions of a problem in incomplete blocks*, Ann. Eugenics 10 (1940) 52–75. ⟨15, 19⟩
[820] R. A. Fisher and F. Yates, *The 6×6 latin squares*, J. Cambridge Phil. Soc. 30 (1934) 492–507. ⟨12, 15, 17⟩
[821] ———, *Statistical Tables for Biological, Agricultural and Medical Research*, Oliver and Boyd, Edinburgh, 1938. ⟨17⟩
[822] F. Fitting, *Zyklische Lösungen des Steinerschen Problems*, Nieuw Archief (2) 11 (1914) 140–148. ⟨17⟩
[823] M. Flammini, L. Moscardelli, M. Shalom, and S. Zaks, *Approximating the traffic grooming problem*, Lect. Notes Comp. Sci. 3827 (2005) 915–924. ⟨494⟩
[824] T. J. Fletcher, *Speedway tournaments*, Math. Gaz. 60 (1976) 256–264. ⟨604⟩
[825] W. Foody and A. S. Hedayat, *On theory and applications of BIB designs with repeated blocks*, Ann. Statist. 5 (1977) 932–945. ⟨647⟩
[826] A. D. Forbes, M. J. Grannell, and T. S. Griggs, *On 6-sparse Steiner triple systems*, preprint. ⟨69⟩
[827] F. Franek, R. A. Mathon, R. C. Mullin, and A. Rosa, *A census of dicyclic $(v, 4, 2)$-designs for $v \leq 22$*, J. Combin. Math. Combin. Comput. 8 (1990) 89–96. ⟨37⟩
[828] F. Franek, R. A. Mathon, and A. Rosa, *On a class of linear spaces with 16 points*, Ars Combin. 31 (1991) 97–104. ⟨269⟩
[829] M. F. Franklin, *Constructing tables of minimum aberration p^{n-m} designs*, Technometrics 26 (1984) 225–232. ⟨453⟩
[830] ———, *Selecting defining contrasts and confounding effects in p^{n-m} factorial experiments*, Technometrics 27 (1985) 165–172. ⟨451⟩
[831] V. Frezza and V. Napolitano, *On finite $\{2, 5\}$-semiaffine linear spaces*, J. Combin. Math. Combin. Comput. 51 (2004) 95–111. ⟨509⟩
[832] M. D. Fried, R. M. Guralnick, and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. 82 (1993) 157–225. ⟨573⟩
[833] A. Fries and W. G. Hunter, *Minimum aberration 2^{k-p} designs*, Technometrics 22 (1980) 601–608. ⟨452⟩
[834] M. Frolov, *Sur les permutations carrés*, J. de Math. spéc. 4 (1890) 8–11,25–30. ⟨15, 18⟩
[835] D. Froncek, T. Kovarova, and P. Kovar, *Fair incomplete tournaments*, Bull. Inst. Combin. Appl. (to appear). ⟨592⟩
[836] D. Froncek and M. Meszka, *Round robin tournaments with one bye and no breaks in home-away patterns are unique*, in Multidisciplinary Scheduling: Theory and Applications, G. Kendall, E. K. Burke, S. Petrovic, and M. Gendreau, eds., Springer, 2005, 331–340. ⟨593⟩
[837] C. M. Fu, H. L. Fu, S. Milici, G. Quattrocchi, and C. A. Rodger, *Almost resolvable directed $2r$-cycle systems*, J. Combin. Des. 3 (1995) 443–447. ⟨378⟩

[838] H. L. Fu, S.-C. Lin, and C. M. Fu, *The length of a partial transversal in a latin square*, J. Combin. Math. Combin. Comput. 43 (2002) 57–64. ⟨143⟩
[839] H. L. Fu, S. L. Logan, and C. A. Rodger, *Maximal sets of Hamilton cycles in* $K_{2p} - F$, Discrete Math. (to appear). ⟨379⟩
[840] H. L. Fu and C. A. Rodger, *Almost resolvable directed m-cycle systems:* $m \equiv 3 \pmod 6$, Ars Combin. 53 (1999) 315–318. ⟨378⟩
[841] R. Fuji-Hara and Y. Miao, *Optical orthogonal codes: Their bounds and new optimal constructions*, IEEE Trans. Inform. Theory 46 (2000) 396–2406. ⟨556⟩
[842] R. Fuji-Hara, Y. Miao, and J. X. Yin, *Optimal* $(9v, 4, 1)$ *optical orthogonal codes*, SIAM J. Disc. Math. 14 (2001) 256–266. ⟨404⟩
[843] R. Fuji-Hara and S. A. Vanstone, *The existence of orthogonal resolutions of lines in* $AG(n, q)$, J. Combin. Theory A 45 (1987) 139–147. ⟨130⟩
[844] M. Fujita, J. Slaney, and F. E. Bennett, *Automatic generation of some results in finite algebra*, in Proc. 13th International Joint Conference on Artificial Intelligence, R. Bajcsy, ed., Morgan Kaufmann, 1993, 52–57. ⟨157⟩
[845] Z. Füredi, *Turán type problems*, in Surveys in Combinatorics, 1991, A. D. Keedwell, ed., Cambridge Univ. Press, Cambridge, 1991, 253–300. ⟨649, 651⟩
[846] Z. Füredi, G. Székely, and Z. Zuber, *On the lottery problem*, J. Combin. Des. 4 (1996) 5–10. ⟨514⟩
[847] S. C. Furino, M. Greig, Y. Miao, and J. X. Yin, *Resolvable BIBDs with block size* 8 *and index* 7, J. Combin. Des. 2 (1994) 101–116. ⟨127⟩
[848] S. C. Furino, Y. Miao, and J. X. Yin, *Frames and Resolvable Designs*, CRC Press, Boca Raton FL, 1996. ⟨41, 44, 125, 126, 127, 129, 132, 263, 265⟩
[849] P. Gaal and S. W. Golomb, *Exhaustive determination of* $(1023, 511, 255)$*-cyclic difference sets*, Math. Comput. 70 (2001) 357–366. ⟨434⟩
[850] R. Gagliardi, J. Robbins, and H. Taylor, *Acquisition sequences in PPM communication*, IEEE Trans. Inform. Theory 33 (1987) 738–744. ⟨440⟩
[851] Z. Galil and J. Kiefer, *D-optimum weighing designs*, Ann. Statist. 8 (1980) 1293–1306. ⟨298⟩
[852] R. G. Gallager, *Low-Density Parity-Check Codes*, M.I.T. Press, Cambridge, Mass., 1963. ⟨520, 521⟩
[853] R. Gallant and C. J. Colbourn, *Asymptotic existence of tight orthogonal main effect plans*, Canad. Math. Bull. 41 (1998) 33–40. ⟨548, 549⟩
[854] J. A. Gallian, *A dynamic survey of graph labeling, Dynamic Survey 6*, Electron. J. Comb. (2005) 148pp. ⟨479, 484⟩
[855] F. Galvin, *The list chromatic index of a bipartite multigraph*, J. Combin. Theory B 63 (1995) 153–158. ⟨151⟩
[856] B. Ganter, A. Gülzow, R. A. Mathon, and A. Rosa, *A complete census of* $(10, 3, 2)$*-block designs and of Mendelsohn triple systems of order ten, IV.* $(10, 3, 2)$ *designs with repeated blocks.* Math. Schriften Kassel 5/78 (1978). ⟨36⟩
[857] B. Ganter, R. A. Mathon, and A. Rosa, *A complete census of* (10, 3, 2)*-block designs and of Mendelsohn triple systems of order ten. I. Mendelsohn triple systems without repeated blocks*, Congr. Numer. 20 (1978) 383–398. ⟨530, 533⟩
[858] B. Ganter, J. Pelikan, and L. Teirlinck, *Small sprawling systems of equicardinal sets*, Ars Combin. 4 (1977) 133–142. ⟨81⟩
[859] M. Gardner, *Time Travel and Other Mathematical Bewilderments*, Freeman, New York, 1988. ⟨525⟩
[860] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, 1979. ⟨741, 756⟩
[861] M. L. Gargano and W. Edelson, *Optimal sequenced matroid bases solved by genetic algorithms with feasibility including applications*, Congr. Numer. 150 (2001) 5–14. ⟨774⟩
[862] C. F. Gauss, *Eulersche (magische) Quadrate*, Gauss Werke 12 (1929) 13–18. Correspondence of 1842 from *Briefwechsel zwischen Gauss und Schumacher IV*, Altona, 1862, with commentary by W. Ahrens. ⟨12⟩

[863] G. Ge, *All $V(3,t)$'s exist for $3t+1$ a prime power*, J. Combin. Math. Combin. Comput. 34 (2000) 197–202. ⟨417⟩
[864] ——, *Uniform frames with block size four and index one or three*, J. Combin. Des. 9 (2001) 28–39. ⟨263⟩
[865] ——, *Mandatory representation designs* $\mathrm{MRD}(\{4,k\};v)$ *with* $k \equiv 1 \bmod 3$, Discrete Math. 275 (2004) 319–329. ⟨234⟩
[866] ——, *Group divisible designs with block size four and group type $g^u m^1$ for more small g*, preprint (2005). ⟨250⟩
[867] ——, *On $(g,4;1)$-difference matrices*, Discrete Math. 301 (2005) 164–174. ⟨412⟩
[868] ——, *Resolvable group divisible designs with block size four and index three*, Discrete Math. 306 (2006) 52–65. ⟨265⟩
[869] G. Ge and R. J. R. Abel, *Some new HSOLSSOMs of type h^n and $1^n u^1$*, J. Combin. Des. 9 (2001) 435–444. ⟨210, 218⟩
[870] G. Ge, M. Greig, and J. R. Seberry, *Generalized Bhaskar Rao designs with block size 4 signed over elementary abelian groups*, J. Combin. Math. Combin. Comput. 46 (2003) 3–45. ⟨300⟩
[871] G. Ge, M. Greig, J. R. Seberry, and R. Seberry, *Generalized Bhaskar Rao designs with block size 3 over finite abelian groups*, preprint. ⟨250, 299⟩
[872] G. Ge and C. W. H. Lam, *Bhaskar Rao designs with block size four*, Discrete Math. 268 (2003) 293–298. ⟨300⟩
[873] ——, *Some new triplewhist tournaments $TWh(v)$*, J. Combin. Theory A 101 (2003) 153–159. ⟨407⟩
[874] ——, *Whist tournaments with the three person property*, Discrete Appl. Math. 138 (2004) 265–276. ⟨667⟩
[875] G. Ge, C. W. H. Lam, and A. C. H. Ling, *Some new uniform frames with block size four and index one or three*, J. Combin. Des. 12 (2004) 112–122. ⟨264⟩
[876] G. Ge, C. W. H. Lam, A. C. H. Ling, and H. Shen, *Resolvable maximum packing with quadruples*, Des. Codes Crypt. 35 (2005) 287–302. ⟨554⟩
[877] G. Ge, E. R. Lamken, and A. C. H. Ling, *Scheduling CCRR tournaments*, J. Combin. Theory A 113 (2006) 352–379. ⟨601⟩
[878] G. Ge and A. C. H. Ling, *Group divisible designs with block size four and group type $g^u m^1$ for small g*, Discrete Math. 285 (2004) 97–120. ⟨258⟩
[879] ——, *Some more 5-GDDs and optimal $(v,5,1)$-packings*, J. Combin. Des. 12 (2004) 132–141. ⟨551⟩
[880] ——, *A systematic approach to some block design constructions*, J. Combin. Theory A 108 (2004) 89–97. ⟨551⟩
[881] ——, *Asymptotic results on the existence of 4-RGDDs and uniform 5-GDDs*, J. Combin. Des. 13 (2005) 222–237. ⟨258, 263, 265⟩
[882] G. Ge and R. S. Rees, *On group divisible designs with block size four and group type $6^u m^1$*, Discrete Math. 279 (2004) 247–265. ⟨250, 251⟩
[883] G. Ge, R. S. Rees, and N. Shalaby, *Kirkman frames having hole type $h^u m^1$ for small h*, preprint. ⟨264⟩
[884] G. Ge and R. Wei, *HGDDs with block size four*, Discrete Math. 279 (2004) 267–276. ⟨260⟩
[885] G. Ge and L. Zhu, *On the existence of Room frames of type t^u*, J. Combin. Des. 1 (1993) 183–191. ⟨588⟩
[886] ——, *Authentication perpendicular arrays* $\mathrm{APA}_1(2,5,v)$, J. Combin. Des. 4 (1996) 365–375. ⟨545⟩
[887] E. N. Gelling, *On One-Factorizations of a Complete Graph and the Relationship to Round-Robin Schedules*, PhD thesis, Univ. Victoria, Canada, 1973. ⟨15⟩
[888] M. Genma, M. Mishima, and M. Jimbo, *Cyclic resolvability of cyclic Steiner 2-designs*, J. Combin. Des. 5 ((1997) 177–187. ⟨401⟩
[889] S. Georgiou, W. H. Holzmann, H. Kharaghani, and B. Tayfeh-Rezaie, *Three variables full orthogonal designs of order 56*, J. Stat. Plann. Infer. (to appear). ⟨294⟩

[890] A. V. Geramita and N. J. Pullman, *Radon's function and Hadamard arrays*, Linear Multilinear Algebra 2 (1974) 147–150. ⟨295⟩

[891] A. V. Geramita and J. R. Seberry, *Orthogonal Designs. Quadratic Forms and Hadamard Matrices*, Dekker, New York, 1979. ⟨280, 282, 283, 285, 288, 289, 294, 295⟩

[892] E. Gergely, *A simple method for constructing doubly diagonalized latin squares*, J. Combin. Theory A 16 (1974) 266–272. ⟨149⟩

[893] A. Gewirtz, *Graphs with maximal even girth*, Canad. J. Math. 21 (1969) 915–934. ⟨856, 858⟩

[894] ———, *The uniqueness of* $g(2, 2, 10, 56)$, Trans. New York Acad. Sci. 31 (1969) 656–675. ⟨856⟩

[895] M. Ghandehari, H. Hatami, and E. S. Mahmoodian, *On the size of the minimum critical set of a latin square*, Discrete Math. 293 (2005) 121–127. ⟨148⟩

[896] D. K. Ghosh and J. Divecha, *Two associate class partially balanced incomplete block designs and partial diallel crosses*, Biometrika 84 (1997) 245–248. ⟨562, 564⟩

[897] S. Ghosh and C. Burns, *Two general classes of search designs for factor screening experiments with factors at three levels*, Metrika 54 (2001) 1–17. ⟨454⟩

[898] P. B. Gibbons, *Computing Techniques for the Construction and Analysis of Block Designs*, PhD thesis, University of Toronto, 1976. ⟨36⟩

[899] P. B. Gibbons and R. A. Mathon, *Construction methods for Bhaskar Rao and related designs*, J. Austral. Math. Soc. A 42 (1987) 5–30. Correction: 43 (1987), 420. ⟨299, 762⟩

[900] ———, *Group signings of symmetric balanced incomplete block designs*, Ars Combin. 23 (1987) 123–134. ⟨313⟩

[901] ———, *The use of hill-climbing to construct orthogonal Steiner triple systems*, J. Combin. Des. 1 (1993) 27–50. ⟨770⟩

[902] ———, *Signings of group divisible designs and projective planes*, Australas. J. Combin. 11 (1995) 79–104. ⟨759, 762, 776⟩

[903] P. B. Gibbons, R. A. Mathon, and D. G. Corneil, *Computing techniques for the construction and analysis of block designs*, Utilitas Math. 11 (1977) 161–192. ⟨765⟩

[904] P. B. Gibbons and E. Mendelsohn, *The construction of antipodal triple systems by simulated annealing*, Discrete Math. 155 (1996) 59–76. ⟨531⟩

[905] P. B. Gibbons, E. Mendelsohn, and H. Shen, *Antipodal triple systems*, Australas. J. Combin. 9 (1994) 137–151. ⟨531, 773⟩

[906] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, *Codes which detect deception*, Bell Syst. Tech. J. 53 (1974) 405–424. ⟨611⟩

[907] N. Gill, *Linear spaces with significant characteristic prime*, Innov. Incidence Geom. (to appear). ⟨342⟩

[908] J. Gimbert, *On digraphs with unique walks of closed lengths between vertices*, Australas. J. Combin. 20 (1999) 77–90. ⟨872⟩

[909] B. D. Ginzburg, *A certain number-theoretic function which has an application in coding theory*, Problemy Kibernet. 19 (1967) 249–252. ⟨387⟩

[910] F. Glover, E. Taillard, and D. de Werra, *A user's guide to tabu search*, Ann. Oper. Res. 41 (1993) 3–28. ⟨773⟩

[911] D. G. Glynn, *A geometrical isomorphism algorithm*, Bull. Inst. Combin. Appl. 7 (1993) 36–38. ⟨269⟩

[912] C. D. Godsil, *Algebraic Combinatorics*, Chapman and Hall, New York, 1993. ⟨326, 330, 622⟩

[913] ———, *Tools from linear algebra*, in Handbook of Combinatorics, vol. 2, Elsevier, Amsterdam, 1995. ⟨790⟩

[914] C. D. Godsil, S. A. Hobart, and W. J. Martin, *Representations of directed strongly regular graphs*, Europ. J. Combin. (to appear). ⟨870, 871⟩

[915] C. D. Godsil and B. D. McKay, *Asymptotic enumeration of latin rectangles*, J. Combin. Theory B 48 (1990) 19–44. ⟨143⟩

[916] J.-M. Goethals, *Two dual families of nonlinear binary codes*, Electron. Lett. 10 (1974) 471–472. ⟨685⟩
[917] J.-M. Goethals and P. Delsarte, *On a class of majority-logic decodable cyclic codes*, IEEE Trans. Inform. Theory 14 (1968) 182–188. ⟨686⟩
[918] J.-M. Goethals and J. J. Seidel, *Orthogonal matrices with zero diagonal*, Canad. J. Math. 19 (1967) 1001–1010. ⟨854⟩
[919] ———, *A skew Hadamard matrix of order* 36, J. Austral. Math. Soc. A 11 (1970) 343–344. ⟨276⟩
[920] ———, *Strongly regular graphs derived from combinatorial designs*, Canad. J. Math. 22 (1970) 597–614. ⟨853, 854, 880⟩
[921] ———, *The regular two-graph on* 276 *vertices*, Discrete Math. 12 (1975) 143–158. ⟨866, 880⟩
[922] J.-M. Goethals and H. C. A. van Tilborg, *Uniformly packed codes*, Philips Res. Rep. 30 (1975) 9–36. ⟨684⟩
[923] M. J. E. Golay, *Notes on digital coding*, Proc. IRE 37 (1949) 657. ⟨19⟩
[924] ———, *Complementary series*, IRE Trans. 7 (1961) 82–87. ⟨20⟩
[925] O. Goldschmidt, D. Hochbaum, A. Levin, and E. Olinick, *The SONET edge-partition problem*, Networks 41 (2003) 13–23. ⟨494⟩
[926] S. W. Golomb, *Algebraic constructions for Costas arrays*, J. Combin. Theory A 37 (1984) 13–21. ⟨360⟩
[927] S. W. Golomb, T. Etzion, and H. Taylor, *Polygonal path constructions for tuscan-k squares*, Ars Combin. 30 (1990) 97–140. ⟨653, 654, 656⟩
[928] S. W. Golomb and G. Gong, *Signal Design for Good Correlation*, Cambridge Univ. Press, New York, 2005. ⟨317⟩
[929] S. W. Golomb and H. Taylor, *Constructions and properties of Costas arrays*, Proc. IEEE 72 (1984) 1143–1163. ⟨360⟩
[930] ———, *Tuscan squares—A new family of combinatorial designs*, Ars Combin. 20-B (1985) 115–132. ⟨656⟩
[931] K. Gopalakrishnan and D. R. Stinson, *A simple analysis of the error probability of two-point based sampling*, Inf. Process. Lett. 60 (1996) 91–96. ⟨389⟩
[932] D. M. Gordon, G. Kuperberg, and O. Patashnik, *New constructions for covering designs*, J. Combin. Des. 3 (1995) 269–284. ⟨373⟩
[933] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968. ⟨820, 847⟩
[934] ———, *Finite Simple Groups*, Plenum, New York, 1982. ⟨842⟩
[935] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups*, Amer. Math. Soc., Providence RI, 1994. ⟨842⟩
[936] E. J. Gorth, *Generation of binary sequences with controllable complexity*, IEEE Trans. Inform. Theory 17 (1971) 288–296. ⟨616⟩
[937] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, Wiley, New York, 1983. ⟨142⟩
[938] P. Govaerts, D. Jungnickel, L. Storme, and J. A. Thas, *Some new maximal sets of mutually orthogonal latin squares*, Des. Codes Crypt. 29 (2003) 141–147. ⟨189⟩
[939] R. A. H. Gower, *Defining sets for the Steiner triple systems from affine spaces*, J. Combin. Des. 5 (1997) 155–175. ⟨384⟩
[940] R. L. Graham, S.-Y. R. Li, and W. C. W. Li, *On the structure of t-designs*, SIAM J. Alg. Disc. Meth. 1 (1980) 8–14. ⟨645, 790⟩
[941] M. J. Grannell and T. S. Griggs, *A Steiner system* $S(5, 6, 108)$, Discrete Math. 125 (1994) 183–186. ⟨766⟩
[942] M. J. Grannell, T. S. Griggs, and M. Knor, *Biembeddings of latin squares and hamiltonian decompositions*, Glasg. Math. J. 46 (2004) 443–457. ⟨489⟩
[943] M. J. Grannell, T. S. Griggs, and R. A. Mathon, *Some Steiner* 5*-designs with* 108 *and* 132 *points*, J. Combin. Des. 1 (1993) 213–238. ⟨107, 766⟩
[944] ———, *Steiner systems* $S(5, 6, v)$ *with* $v = 72$ *and* 84, Math. Comp. 67 (1998) 357–359. ⟨110⟩

[945] M. J. Grannell, T. S. Griggs, and E. Mendelsohn, *A small basis for four-line configurations in Steiner triple systems*, J. Combin. Des. 3 (1995) 51–59. ⟨68⟩
[946] M. J. Grannell, T. S. Griggs, and K. A. S. Quinn, *All admissible* 3-$(v, 4, \lambda)$ *directed designs exist*, J. Combin. Math. Combin. Comput. 35 (2000) 65–70. ⟨442⟩
[947] M. J. Grannell, T. S. Griggs, and J. Širáň, *Surface embeddings of Steiner triple systems*, J. Combin. Des. 6 (1998) 325–336. ⟨489⟩
[948] ——, *Recursive constructions for triangulations*, J. Graph Theory 39 (2002) 87–107. ⟨488⟩
[949] M. J. Grannell, T. S. Griggs, and C. A. Whitehead, *The resolution of the anti-Pasch conjecture*, J. Combin. Des. 8 (2000) 300–309. ⟨68⟩
[950] A. Granville, H.-D. O. F. Gronau, and R. C. Mullin, *On a problem of Hering concerning orthogonal covers of* $\vec{K}_n$, J. Combin. Theory A 72 (1995) 345–350. ⟨248⟩
[951] A. Granville, A. Moisiadis, and R. S. Rees, *Nested Steiner n-cycle systems and perpendicular arrays*, J. Combin. Math. Combin. Comput. 3 (1988) 163–167. ⟨545, 547⟩
[952] J. E. Graver and W. B. Jurkat, *Algebra structures for general designs*, J. Algebra 23 (1972) 574–589. ⟨645⟩
[953] ——, *The module structure of integral designs*, J. Combin. Theory A 15 (1973) 75–90. ⟨790⟩
[954] B. D. Gray and C. Ramsay, *On a conjecture of Mahmoodian and Soltankhah regarding the existence of* (v, k, t) *trades*, Ars Combin. 48 (1998) 191–194. ⟨644⟩
[955] ——, *On the number of Pasch configurations in a Steiner triple system*, Bull. Inst. Combin. Appl. 24 (1998) 105–112. ⟨68⟩
[956] K. Gray, *On the minimum number of blocks defining a design*, Bull. Austral. Math. Soc. 41 (1990) 97–112. ⟨383⟩
[957] M. Greig, *Some balanced incomplete block design constructions*, Congr. Numer. 77 (1990) 121–134. ⟨44, 48, 401⟩
[958] ——, *Some group divisible design constructions*, J. Combin. Math. Combin. Comput. 27 (1998) 33–52. ⟨43, 53, 56, 405⟩
[959] ——, *Designs from projective planes and PBD bases*, J. Combin. Des. 7 (1999) 341–374. ⟨45, 51, 55, 238, 240, 241, 242, 250, 251, 253, 254⟩
[960] ——, *Some pairwise balanced designs*, Electron. J. Comb. 7 (2000) R13. ⟨250, 252, 253, 254⟩
[961] ——, *Recursive constructions of balanced incomplete block designs with block size of* 7, 8 *or* 9, Ars Combin. 60 (2001) 3–54. ⟨72, 127⟩
[962] ——, *Finite linear spaces. II*, Des. Codes Crypt. 27 (2002) 25–47. ⟨508, 512⟩
[963] ——, *Constructions using balanced n-ary designs*, in Designs 2002, W. D. Wallis, ed., Kluwer, Boston, 2003, 227–254. ⟨331, 332⟩
[964] ——, *Rectangular PBIBDs and uniform base factorizations*, preprint (2005). ⟨125, 127⟩
[965] ——, *Log tables and block designs*, Bull. Inst. Combin. Appl. (to appear). ⟨124, 406⟩
[966] M. Greig and R. J. R. Abel, *Resolvable balanced incomplete block designs with a block size of* 8, Des. Codes Crypt. 11 (1997) 123–140. ⟨127⟩
[967] M. Greig, M. Grüttmüller, and S. Hartmann, *Pairwise balanced designs whose block size set includes seven and thirteen*, preprint. ⟨254⟩
[968] M. Greig, H. Haanpää, and P. Kaski, *On the coexistence of conference matrices and near resolvable* 2-$(2k+1, k, k-1)$ *designs*, J. Combin. Theory A 113 (2006) 703–711. ⟨126⟩
[969] T. S. Griggs and J. P. Murphy, 101 *anti-Pasch Steiner triple systems of order* 19, J. Combin. Math. Combin. Comput. 13 (1993) 129–141. ⟨770⟩
[970] T. S. Griggs and A. Rosa, *Large sets of Steiner triple systems*, in Surveys in Combinatorics, 1995, Cambridge Univ. Press, Cambridge, 1995, 25–39. ⟨66⟩
[971] ——, *An invariant for one-factorizations of the complete graph*, Ars Combin. 42 (1996) 77–88. ⟨780⟩

[972] V. Grishukhin, *Regular two-graphs from the even unimodular lattice $E_8 \oplus E_8$*, Europ. J. Combin. 18 (1997) 397–401. ⟨881⟩
[973] H.-D. O. F. Gronau, M. Grüttmüller, S. Hartmann, U. Leck, and V. Leck, *On orthogonal double covers of graphs*, Des. Codes Crypt. 27 (2002) 49–91. ⟨486⟩
[974] H.-D. O. F. Gronau, D. L. Kreher, and A. C. H. Ling, *Super-simple $(v, 5, 2)$-designs*, Discrete Appl. Math. 138 (2004) 65–77. ⟨635⟩
[975] H.-D. O. F. Gronau, R. C. Mullin, and C. Pietsch, *The closure of all subsets of $\{3, 4, \ldots, 10\}$ which include* 3, Ars Combin. 41 (1995) 129–161. ⟨233, 249⟩
[976] H.-D. O. F. Gronau and J. Prestin, *Some results on designs with repeated blocks*, Rostock. Math. Kolloq. (1982) 15–37. ⟨36, 37⟩
[977] A. Groner, *Duplicate Bridge Direction*, Baron Barclay Bridge Supplies, Louisville KY, 1993. ⟨503, 504, 599, 600, 601, 606⟩
[978] H. Gropp, *The elementary abelian Steiner systems $S(2, 4, 49)$*, Discrete Math. 64 (1987) 87–90. ⟨38⟩
[979] ——, *Configurations and the Tutte conjecture*, Ars Combin. 29 (1990) 171–177. ⟨269⟩
[980] ——, *On the history of configurations*, in Internat. Symp. Structures in Mathematical Theories, A. Díez, J. Echeverría, and A. Ibarra, eds., Universidad del País Vasco, Bilbao, 1990, 263–268. ⟨355⟩
[981] ——, *The construction of all configurations $(12_4, 16_3)$*, Ann. Discrete Math. 51 (1992) 85–91. ⟨354⟩
[982] ——, *Non-symmetric configurations with deficiencies* 1 *and* 2, Ann. Discrete Math. 52 (1992) 227–239. ⟨354⟩
[983] ——, *Configurations and $(r, 1)$-designs*, Discrete Math. 129 (1994) 113–137. ⟨355⟩
[984] ——, *Non-symmetric configurations with natural index*, Discrete Math. 124 (1994) 87–98. ⟨354⟩
[985] ——, *On symmetric spatial configurations*, Discrete Math. 125 (1994) 201–209. ⟨355⟩
[986] ——, *Blocking set free configurations and their relations to digraphs and hypergraphs*, Discrete Math. 165/166 (1997) 349–360. ⟨355⟩
[987] ——, *Existence and enumeration of configurations*, Bayreuth. Math. Schr. 74 (2005) 123–129. ⟨354, 355⟩
[988] B. H. Gross, *Intersection triangles and block intersection numbers of Steiner systems*, Math. Zeitschr. 139 (1974) 87–104. ⟨105⟩
[989] J. L. Gross and J. Yellen, eds., *Handbook of Graph Theory*, CRC Press, Boca Raton FL, 2004. ⟨740⟩
[990] T. Grundhöfer, *A synthetic construction of the Figueroa planes*, J. Geom. 26 (1986) 191–201. ⟨726⟩
[991] M. Grüttmüller, *On the existence of mandatory representation designs with block sizes* 3 *and k*, J. Combin. Des. 8 (2000) 122–131. ⟨234⟩
[992] T. A. Gulliver and M. Harada, *Extremal double circulant type II codes over $\mathbb{Z}_4$ and construction of* 5*-$(24, 10, 36)$ designs*, Discrete Math. 194 (1999) 129–137. ⟨683⟩
[993] A. Gunawardena, *On two-graphs of ovoids in $O_{2n+1}(q)$*, Europ. J. Combin. 18 (1997) 857–858. ⟨881⟩
[994] A. Gunawardena and G. E. Moorhouse, *The nonexistence of ovoids in $O_9(q)$*, Europ. J. Combin. 18 (1997) 171–173. ⟨881⟩
[995] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math. 78 (1984) 127–130. ⟨794⟩
[996] R. Gupta, S. A. Smolka, and S. Bhaskar, *On randomization in sequential and distributed algorithms*, ACM Computing Surveys 26 (1994) 7–86. ⟨391⟩
[997] S. C. Gupta, *Generating generalised cyclic designs with factorial balance*, Commun. Stat. 16 (1987) 1885–1900. ⟨564⟩
[998] S. C. Gupta and S. Kageyama, *Optimal complete diallel crosses*, Biometrika 81 (1994) 420–424. ⟨540⟩

[999] S. C. Gupta and M. Singh, *Partially balanced incomplete block designs with nested rows and columns*, Utilitas Math. 40 (1991) 291–302. ⟨565⟩
[1000] A. Gyárfás and J. Lehel, *Packing trees of different order into K_n*, in Combinatorics, A. Hajnal and V. T. Sós, eds., North-Holland, Amsterdam, 1978, 463–469. ⟨479⟩
[1001] Z. Habbas, M. Krajecki, and D. Singer, *Parallelizing combinatorial search in shared memory*, in Proceedings of the fourth European Workshop on OpenMP, Roma, Italy, 2002. ⟨616⟩
[1002] E. Haberberger, *Isomorphieklassifikation von Inzidenzstrukturen mit dem Lattice-Climbing-Verfahren am Beispiel von t-Designs*, Bayreuth. Math. Schr. 68 (2004) 1–78. ⟨97⟩
[1003] J. Hadamard, *Résolution d'une question relative aux déterminants*, Bull. des Sciences Math. 17 (1893) 240–246. ⟨14, 274⟩
[1004] L. Haddad, *On the chromatic numbers of Steiner triple systems*, J. Combin. Des. 7 (1999) 1–10. ⟨69⟩
[1005] W. H. Haemers, *Eigenvalue Techniques in Design and Graph Theory*, Mathematisch Centrum, Amsterdam, 1980. ⟨37, 118⟩
[1006] ——, *Regular 2-graphs and extensions of partial geometries*, Europ. J. Combin. 12 (1991) 115–123. ⟨881⟩
[1007] ——, *There exists no $(76, 21, 2, 7)$ strongly regular graph*, in Finite Geometry and Combinatorics, A. Beutelspacher, F. Buekenhout, J. Doyen, F. De Clerck, J. A. Thas, and J. W. P. Hirschfeld, eds., Cambridge Univ. Press, 1993, 175–176. ⟨580, 857⟩
[1008] W. H. Haemers and E. Spence, *The pseudo-geometric graphs for generalised quadrangles of order $(3, t)$*, Europ. J. Combin. 22 (2001) 839–845. ⟨856⟩
[1009] W. H. Haemers, C. Weug, and P. Delsarte, *Linear programming bounds for codes and designs*, Technical Note N96, M.B.L.E. Lab. de Recherches, Brussels, Belgium (1974). ⟨84⟩
[1010] R. Häggkvist, *A lemma on cycle decompositions*, Ann. Discrete Math. 27 (1985) 227–232. ⟨375⟩
[1011] H.-R. Halder and W. Heise, *Einführung in die Kombinatorik*, Hanser Verlag, München, 1976. ⟨103⟩
[1012] M. Hall Jr., *Cyclic projective planes*, Duke Math. J. 14 (1947) 1079–1090. ⟨17⟩
[1013] ——, *A survey of difference sets*, Proc. Amer. Math. Soc. 7 (1956) 975–986. ⟨40, 41, 49, 53, 118⟩
[1014] ——, *The Theory of Groups*, Macmillan, New York, 1959. ⟨820, 822, 847⟩
[1015] ——, *Automorphism of Steiner triple systems*, IBM J. Res. Develop. 4 (1960) 406–472. ⟨499⟩
[1016] ——, *Combinatorial Theory*, Wiley, New York, 2nd ed., 1986. ⟨35, 36, 37, 58, 123, 690, 701, 787⟩
[1017] M. Hall Jr. and W. S. Connor, *An embedding theorem for balanced incomplete block designs*, Canad. J. Math. 6 (1954) 35–41. ⟨113⟩
[1018] M. Hall Jr., R. Lane, and D. Wales, *Designs derived from permutation groups*, J. Combin. Theory 8 (1970) 12–22. ⟨118⟩
[1019] M. Hall Jr. and H. J. Ryser, *Cyclic incidence matrices*, Canad. J. Math. 3 (1951) 495–502. ⟨17, 112⟩
[1020] M. Hall Jr. and J. D. Swift, *Determination of Steiner triple systems of order 15*, Math. Tables Aids Comput. 9 (1955) 146–152. ⟨15⟩
[1021] M. Hamada and N. Balakrishnan, *Analysing unreplicated factorial experiments: A review with some new proposals*, Statist. Sinica 8 (1998) 1–41. ⟨445⟩
[1022] M. Hamada and C. F. J. Wu, *Analysis of designed experiments with complex aliasing*, J. Qual. Technol. 24 (1992) 130–137. ⟨454⟩
[1023] N. Hamada, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes*, Hiroshima Math. J. 3 (1973) 153–226. ⟨686, 687, 788⟩

[1024] N. Hamada and T. Helleseth, *A characterization of some* $\{2v_2+v_3, 3v_1+v_2; 3, 3\}$*-minihypers and some* $[15, 4, 9; 3]$*-codes with* $b_2 = 0$, J. Stat. Plann. Infer. 56 (1996) 129–146. ⟨857⟩

[1025] N. Hamada and H. Ohmori, *On the BIB design having the minimum p-rank*, J. Combin. Theory A 18 (1975) 131–140. ⟨687⟩

[1026] A. M. Hamel, W. H. Mills, R. C. Mullin, R. S. Rees, D. R. Stinson, and J. X. Yin, *The spectrum of* PBD$(\{5, k^*\}, v)$ *for* $k = 9, 13$, Ars Combin. 36 (1993) 7–26. ⟨244, 252, 253, 254⟩

[1027] N. Hamilton and R. A. Mathon, *More maximal arcs in Desarguesian projective planes and their geometric structure*, Adv. Geom. 3 (2003) 251–261. ⟨559⟩

[1028] ———, *On the spectrum of non-Denniston maximal arcs in* $PG(2, 2^h)$, Europ. J. Combin. 25 (2004) 415–421. ⟨713⟩

[1029] N. Hamilton and C. T. Quinn, *m-Systems of polar spaces and maximal arcs in projective planes*, Bull. Belg. Math. Soc. Simon Stevin 7 (2000) 237–248. ⟨728⟩

[1030] J. M. Hammersley, *The friendship theorem and the love problem*, in Surveys in Combinatorics, 1983, E. K. Lloyd, ed., Cambridge Univ. Press, 1983, 31–54. ⟨869, 872⟩

[1031] R. W. Hamming, *Error-detecting and error-correcting codes*, Bell Syst. Tech. J. 29 (1950) 147–160. ⟨19, 226⟩

[1032] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory 40 (1994) 301–319. ⟨685⟩

[1033] A. Hanaki and I. Miyamoto, *List of association schemes up to order* 30+. `http://kissme.shinshu-u.ac.jp/as/`, 2005. ⟨330⟩

[1034] H. Hanani, *private communication.* ⟨45, 46⟩

[1035] ———, *On quadruple systems*, Canad. J. Math. 12 (1960) 145–157. ⟨12, 82⟩

[1036] ———, *The existence and construction of balanced incomplete block designs*, Ann. Math. Stat. 32 (1961) 361–386. ⟨19⟩

[1037] ———, *On some tactical configurations*, Canad. J. Math. 15 (1963) 702–722. ⟨658⟩

[1038] ———, *Truncated finite planes*, in Combinatorics, T. S. Motzkin, ed., Amer. Math. Soc., Providence RI, 1971, 115–120. ⟨658, 660⟩

[1039] ———, *On balanced incomplete block designs with blocks having five elements*, J. Combin. Theory A 12 (1972) 184–201. ⟨19⟩

[1040] ———, *On resolvable balanced incomplete block designs*, J. Combin. Theory A 17 (1974) 275–289. ⟨38, 41, 45, 50, 56⟩

[1041] ———, *On transversal designs*, in Combinatorics, M. Hall Jr. and J. H. van Lint, eds., Math. Centrum, Amsterdam, 1974, 42–52. ⟨220⟩

[1042] ———, *Balanced incomplete block designs and related designs*, Discrete Math. 11 (1975) 255–369. ⟨19, 35, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 72, 79, 236, 238, 245, 250, 251, 254, 261⟩

[1043] ———, *A class of three-designs*, J. Combin. Theory A 26 (1979) 1–19. ⟨103, 658⟩

[1044] ———, *BIBD's with block-size seven*, Discrete Math. 77 (1989) 89–96. ⟨38, 45, 72, 245⟩

[1045] H. Hanani, A. Hartman, and E. S. Kramer, *On three-designs of small order*, Discrete Math. 45 (1983) 75–97. ⟨85⟩

[1046] H. Hanani, D. Ornstein, and V. T. Sós, *On the lottery problem*, Magyar Tud. Acad. Mat. Kutató Int. Közl. 9 (1964) 155–158. ⟨20, 514⟩

[1047] H. Hanani, D. K. Ray-Chaudhuri, and R. M. Wilson, *On resolvable designs*, Discrete Math. 3 (1972) 343–357. ⟨42, 45, 48, 49, 56⟩

[1048] T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields*, Math. Comp. 59 (1992) 639–643, S47–S50. ⟨813⟩

[1049] M. Harada, *New* 5*-designs constructed from the lifted Golay code over* $\mathbb{Z}_4$, J. Combin. Des. 6 (1998) 225–229. ⟨683⟩

[1050] M. Harada, C. W. H. Lam, and V. D. Tonchev, *Symmetric* $(4, 4)$*-nets and generalized Hadamard matrices over groups of order* 4, Des. Codes Crypt. 34 (2005) 71–87. ⟨687, 688⟩

[1051] M. Harada and A. Munemasa, *A quasi-symmetric* 2-$(49, 9, 6)$ *design*, J. Combin. Des. 10 (2002) 173–179. ⟨580, 689⟩
[1052] M. Harada, A. Munemasa, and V. D. Tonchev, *A characterization of designs related to an extremal doubly-even self-dual code of length* 48, Ann. Comb. 9 (2005) 189–198. ⟨580, 688⟩
[1053] M. Harada and P. R. J. Östergård, *On the classification of self-dual codes over* $\mathbb{F}_5$, Graphs Combin. 19 (2003) 203–214. ⟨40⟩
[1054] M. Harada and V. D. Tonchev, *Singly-even self-dual codes and Hadamard matrices*, Lect. Notes Comp. Sci. 948 (1995) 279–284. ⟨682⟩
[1055] F. Harary, *Graph Theory*, Addison-Wesley, Reading MA, 1969. ⟨732, 740⟩
[1056] F. Harary and E. M. Palmer, *Graphical Enumeration*, Academic Press, New York, 1973. ⟨732, 740⟩
[1057] F. Harary, R. W. Robinson, and N. C. Wormald, *Isomorphic factorisations III. Complete multipartite graphs*, Lect. Notes Math. 686 (1978) 47–54. ⟨485⟩
[1058] R. H. Hardin and N. J. A. Sloane, *A new approach to the construction of optimal designs*, J. Stat. Plann. Infer. 37 (1993) 339–369. ⟨542⟩
[1059] A. Hartman, *Halving the complete design*, Ann. Discrete Math. 34 (1987) 207–224. ⟨99⟩
[1060] ——, *The fundamental construction for* 3*-designs*, Discrete Math. 124 (1994) 107–132. ⟨658, 659⟩
[1061] ——, *Software and hardware testing using combinatorial covering suites*, in Graph Theory, Combinatorics and Algorithms: Interdisciplinary Applications, M. C. Golumbic and I. B.-A. Hartman, eds., Springer, 2005, 237–266. ⟨362, 365⟩
[1062] A. Hartman and K. Heinrich, *Pairwise balanced designs with holes*, in Graphs, Matrices and Designs, R. S. Rees, ed., Dekker, New York, 1993, 171–204. ⟨233⟩
[1063] A. Hartman and K. T. Phelps, *Steiner quadruple systems*, in [724], 1992, 205–240. ⟨105, 110⟩
[1064] S. Hartmann, *Superpure digraph designs*, J. Combin. Des. 10 (2002) 239–255. ⟨635⟩
[1065] W. Harvey and T. Winterer, *Solving the MOLR and social golfers problems*, Lect. Notes Comp. Sci. 3709 (2005) 286–300. ⟨191⟩
[1066] J. Haselgrove and J. Leech, *A tournament design problem*, Amer. Math. Monthly March (1977) 198–201. ⟨20, 334⟩
[1067] G. Havas, J. L. Lawrence, C. Ramsay, A. P. Street, and E. Ş. Yazici, *Defining set spectra for designs can have arbitrarily large gaps*, preprint. ⟨384, 385⟩
[1068] P. Healey, *Construction of balanced doubles schedules*, J. Combin. Theory A 29 (1980) 280–286. ⟨535, 537⟩
[1069] G. Heathcote, *Linear spaces on* 16 *points*, J. Combin. Des. 1 (1993) 359–378. ⟨269⟩
[1070] A. S. Hedayat, *A complete solution to the existence and nonexistence of Knut Vik designs*, J. Combin. Theory A 22 (1977) 331–337. ⟨149⟩
[1071] ——, *The theory of trade-off for* t*-designs*, in Coding Theory and Design Theory II, D. K. Ray-Chaudhuri, ed., Springer, New York, 1990, 101–126. ⟨648⟩
[1072] A. S. Hedayat and S. Kageyama, *The family of* t*–designs-Part I*, J. Stat. Plann. Infer. 4 (1980) 173–212. ⟨97⟩
[1073] A. S. Hedayat, D. Raghavarao, and E. Seiden, *Further contributions to the theory of F-squares design*, Ann. Statist. 3 (1975) 712–716. ⟨466⟩
[1074] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays*, Springer, New York, 1999. ⟨224, 226, 227, 228, 365, 419, 466⟩
[1075] A. S. Hedayat, J. Stufken, and W. G. Zhang, *Virtually balanced incomplete block designs for* $v = 22$, $k = 8$, *and* $\lambda = 4$, J. Combin. Des. 3 (1995) 195–201. ⟨542⟩
[1076] L. Heffter, *Über das Problem der Nachbargebiete*, Math. Ann. 38 (1891) 479–508. ⟨16⟩

[1077] ——, *Über Nachbarconfigurationen, Tripelsysteme und metacyklische Gruppen*, Deutsche Mathem. Vereinig. Jahresber. 5 (1896) 67–69. ⟨16⟩
[1078] ——, *Über Tripelsysteme*, Math. Ann. 49 (1897) 101–112. ⟨16⟩
[1079] K. Heinrich, *Latin squares with and without subsquares of prescribed type*, in [685], 1991, 101–148. ⟨144, 145, 194, 211⟩
[1080] ——, *Path-decompositions*, Le Matematiche (Catania) 47 (1992) 241–258. ⟨479⟩
[1081] ——, *Graph decompositions and designs*, in The CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz, eds., CRC Press, Boca Raton FL, 1996, 361–366. ⟨482⟩
[1082] K. Heinrich and P. Horak, *Isomorphic factorizations of trees*, J. Graph Theory 19 (1995) 187–199. ⟨486⟩
[1083] K. Heinrich, P. Horak, and A. Rosa, *On Alspach's conjecture*, Discrete Math. 77 (1989) 97–121. ⟨374⟩
[1084] K. Heinrich, G. H. J. Van Rees, and W. D. Wallis, *A general construction for equidistant permutation arrays*, in Graph Theory and Related Topics, J. A. Bondy and U. S. R. Murty, eds., Academic Press, New York, 1979, 247–252. ⟨570⟩
[1085] K. Heinrich and L. Zhu, *Existence of orthogonal latin squares with aligned subsquares*, Discrete Math. 59 (1984) 69–78. ⟨209⟩
[1086] ——, *Incomplete self-orthogonal latin squares*, J. Austral. Math. Soc. A 42 (1987) 365–384. ⟨218⟩
[1087] D. Held and M.-O. Pavčević, *Some new Hadamard designs with* 79 *points admitting automorphisms of order* 13 *and* 19, Discrete Math. 238 (2001) 61–65. ⟨44, 54⟩
[1088] L. Hellerstein, G. A. Gibson, R. M. Karp, R. M. Katz, and D. A. Patterson, *Coding techniques for handling failures in large disk arrays*, Algorithmica 12 (1994) 182–208. ⟨520⟩
[1089] T. Helleseth and P. V. Kumar, *Sequences with low correlation*, in Handbook of Coding Theory, Vol. I, II, V. S. Pless, W. C. Huffman, and R. A. Brualdi, eds., North-Holland, Amsterdam, 1998, 1765–1853. ⟨315⟩
[1090] T. Helleseth, P. V. Kumar, and H. Martinsen, *A new family of ternary sequences with ideal two-level autocorrelation function*, Des. Codes Crypt. 23 (2001) 157–166. ⟨423⟩
[1091] T. Helleseth, C. Rong, and K. Yang, *On t-designs from codes over* $\mathbb{Z}_4$, Discrete Math. 238 (2001) 67–80. ⟨685⟩
[1092] S. H. Heuss, *The Ship Captain's Problem*, PhD thesis, Auburn University, 2003. ⟨376⟩
[1093] H. Hevia and S. Ruiz, *Decompositions of complete graphs into caterpillars*, Rev. Mat. Apl. 9 (1987) 55–62. ⟨485⟩
[1094] K. Hicks, C. F. Laywine, and G. L. Mullen, *Frequency magic squares*, Utilitas Math. 62 (2002) 3–12. ⟨471⟩
[1095] J. Higham, *Row-complete latin squares of every composite order exist*, J. Combin. Des. 6 (1998) 63–77. ⟨656⟩
[1096] D. G. Higman, *Invariant relations, coherent configurations and generalized polygons*, in Combinatorics, M. Hall and J. H. van Lint, eds., Math. Centre Tracts 57, Amsterdam, 1974, 27–43. ⟨855⟩
[1097] ——, *Coherent configurations I*, Geom. Ded. 4 (1975) 1–32. ⟨325⟩
[1098] D. G. Higman and C. C. Sims, *A simple group of order* 44, 352, 000, Math. Zeitschr. 105 (1968) 110–113. ⟨858⟩
[1099] G. Higman, *On the simple group of D.G. Higman and C.C. Sims*, Illinois J. Math. 13 (1969) 74–80. ⟨118, 861⟩
[1100] A. J. W. Hilton, *Factorizations of regular graphs of high degree*, J. Graph Theory 9 (1985) 193–196. ⟨741⟩
[1101] A. J. W. Hilton and M. Johnson, *Some results on the Oberwolfach problem*, J. London Math. Soc. 64 (2001) 513–522. ⟨375⟩
[1102] A. J. W. Hilton and J. Wojciechowski, *Semiregular factorization of simple graphs*, AKCE Int. J. Graphs Comb. 2 (2005) 57–62. ⟨741⟩

[1103] D. S. Hirschberg, *Bounds on the number of string subsequences*, Lect. Notes Comp. Sci. (1999) 115–122. ⟨386⟩
[1104] J. W. P. Hirschfeld, *Finite Projective Spaces Of Three Dimensions*, Oxford University Press, New York, 1985. ⟨729⟩
[1105] ——, *Projective Geometries Over Finite Fields*, Oxford University Press, New York, 2nd ed., 1998. ⟨559, 561, 729⟩
[1106] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: Update 2001*, in Finite Geometries, A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas, eds., Kluwer, Dordrecht, 2001, 201–246. ⟨710, 711, 712, 713, 714, 715, 716, 718, 729⟩
[1107] J. W. P. Hirschfeld and T. Szőnyi, *Constructions of large arcs and blocking sets in finite planes*, Europ. J. Combin. 12 (1991) 499–511. ⟨713⟩
[1108] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford University Press, New York, 1991. ⟨557, 558, 559, 561, 729⟩
[1109] T. Hishida, K. Ishikawa, M. Jimbo, S. Kageyama, and S. Kuriki, *Nonexistence of a nested BIB design NB*$(10, 15, 2, 3)$, J. Combin. Math. Combin. Comput. 36 (2001) 55–63. ⟨535⟩
[1110] T. Hishida and M. Jimbo, *Constructions of balanced incomplete block designs with nested rows and columns*, J. Stat. Plann. Infer. 106 (2002) 47–56. ⟨539⟩
[1111] B. Hnich, S. Prestwich, and E. Selensky, *Constraint-based approaches to the covering test problem*, Lect. Notes Comp. Sci. 3419 (2005) 172–186. ⟨363, 365⟩
[1112] C. Y. Ho, *Finite projective planes with abelian transitive collineation groups*, J. Algebra 208 (1998) 533–550. ⟨342⟩
[1113] S. A. Hobart and A. E. Brouwer, *Parameters of directed strongly regular graphs*. `http://www.cwi.nl/~aeb/math/dsrg/dsrg.html`. ⟨869, 872⟩
[1114] S. A. Hobart and T. J. Shaw, *A note on a family of directed strongly regular graphs*, Europ. J. Combin. 20 (1999) 819–820. ⟨870, 872⟩
[1115] A. M. Hobbs, B. A. Bourgeois, and J. Kasiraj, *Packing trees in complete graphs*, Discrete Math. 67 (1987) 27–42. ⟨479⟩
[1116] A. J. Hoffman and R. R. Singleton, *On Moore graphs with diameters* 2 *and* 3, IBM J. Res. Develop. 4 (1960) 497–504. ⟨856⟩
[1117] D. G. Hoffman and D. L. Kreher, *The bigraphical* t*-wise balanced designs of index* 1, J. Combin. Des. 2 (1994) 41–48. ⟨492, 658⟩
[1118] D. G. Hoffman, C. C. Lindner, and C. A. Rodger, *A partial* $2k$*-cycle system of order* n *can be embedded in a* $2k$*-cycle system of order* $kn = c(k)$*,* $k \geq 3$, Discrete Math. 261 (2003) 325–336. ⟨380⟩
[1119] D. G. Hoffman, C. A. Rodger, and A. Rosa, *Maximal sets of* 2*-factors and Hamiltonian cycles*, J. Combin. Theory B 57 (1993) 69–76. ⟨754⟩
[1120] K. Hoffman and R. Kunze, *Linear Algebra*, Prentice-Hall, Englewood Cliffs NJ, 2nd ed., 1971. ⟨790⟩
[1121] S. G. Hoggar, *t-Designs in projective spaces*, Europ. J. Combin. 3 (1982) 233–254. ⟨621, 622⟩
[1122] P. Höhler, *Eine Verallgemeinerung von orthogonalen lateinischen Quadraten auf höhere Dimensionen*, Diss. Dokt. Math. Eidgenöss, Techn. Hochschule Zürich, 1970. ⟨471⟩
[1123] I. Holyer, *The NP-completeness of edge-coloring*, SIAM J. Comput. 10 (1981) 718–720. ⟨741⟩
[1124] W. H. Holzmann and H. Kharaghani, *An infinite class of complex D-optimal designs*, Congr. Numer. 99 (1994) 285–289. ⟨298⟩
[1125] ——, *On the Plotkin arrays*, Australas. J. Combin. 22 (2000) 287–299. ⟨286⟩
[1126] ——, *On weak amicable T-sequences*, J. Combin. Des. (to appear). ⟨286⟩
[1127] W. H. Holzmann, H. Kharaghani, J. R. Seberry, and B. Tayfeh-Rezaie, *On orthogonal designs in order* 48, J. Stat. Plann. Infer. 128 (2005) 311–325. ⟨294⟩
[1128] W. H. Holzmann, H. Kharaghani, and B. Tayfeh-Rezaie, *All triples for orthogonal designs of order* 40, Discrete Math. (to appear). ⟨294⟩

[1129] A. Hoorfar and G. B. Khosrovshahi, *On the existence of trades of large volumes*, Ars Combin. 73 (2004) 45–48. ⟨644⟩
[1130] ——, *On the nonexistence of Steiner t-(v, k) trades*, Ars Combin. 75 (2005) 195–204. ⟨645⟩
[1131] K. J. Horadam, *Hadamard Matrices*, Princeton University Press, Springer, Princeton and Oxford, 2006. ⟨306⟩
[1132] P. Horak and I. J. Dejter, *Completing latin squares: Critical sets II*, J. Combin. Des. to appear. ⟨148⟩
[1133] J. D. Horton, *Hamilton path tournament designs*, Ars Combin. 27 (1989) 69–74. ⟨336⟩
[1134] ——, *Orthogonal starters in finite abelian groups*, Discrete Math. 79 (1989/90) 265–278. ⟨624, 627⟩
[1135] H. Hotelling, *Some improvements in weighing and other experimental techniques*, Ann. Math. Stat. 15 (1944) 297–305. ⟨19⟩
[1136] S. K. Houghten, D. Ashlock, and J. Lenarz, *Bounds on optimal edit-metric codes*, Tech. Report CS-05-07, Computer Science, Brock University, 2005. ⟨387, 388⟩
[1137] S. K. Houghten, C. W. H. Lam, L. H. Thiel, and J. A. Parker, *The extended quadratic residue code is the only* $(48, 24, 12)$ *self-dual doubly-even code*, IEEE Trans. Inform. Theory 49 (2003) 53–59. ⟨688⟩
[1138] S. K. Houghten, L. H. Thiel, J. Janssen, and C. W. H. Lam, *There is no* $(46, 6, 1)$ *block design*, J. Combin. Des. 9 (2001) 60–71. ⟨36, 72⟩
[1139] J. Hsiang, D. F. Hsu, and Y.-P. Shieh, *On the hardness of counting problems of complete mappings*, Discrete Math. 277 (2004) 87–100. ⟨346⟩
[1140] D. F. Hsu, *Cyclic Neofields and Combinatorial Designs*, Springer, 1980. ⟨349⟩
[1141] J. Q. Hu, *Optimal traffic grooming for wavelength-division-multiplexing rings with all-to-all uniform traffic*, OSA J. Optical Networks 1 (2002) 32–42. ⟨495⟩
[1142] C. Huang, *Resolvable balanced bipartite designs*, Discrete Math. 14 (1976) 319–335. ⟨480⟩
[1143] J. H. Huang and S. S. Skiena, *Gracefully labeling prisms*, Ars Combin. 38 (1994) 225–242. ⟨400⟩
[1144] R. Huang and G.-C. Rota, *On the relations of various conjectures on latin squares and straightening coefficients*, Discrete Math. 128 (1994) 225–236. ⟨151⟩
[1145] X. Hubaut, *Two new families of* 4*-designs*, Discrete Math. 9 (1974) 247–249. ⟨82, 85⟩
[1146] ——, *Strongly regular graphs*, Discrete Math. 13 (1975) 357–381. ⟨868⟩
[1147] M. Huber, *On highly symmetric combinatorial designs*, preprint. ⟨340⟩
[1148] ——, *The classification of flag-transitive Steiner* 3*-designs*, Adv. Geom. 5 (2005) 195–221. ⟨340⟩
[1149] M. Hudelson, V. Klee, and D. Larman, *Largest j-simplices in d-cubes: some relatives of the Hadamard maximum determinant problem*, Lin. Alg. Appl. 241/243 (1996) 519–598. ⟨297, 298⟩
[1150] W. C. Huffman, *Automorphisms of codes with applications to extremal doubly even codes of length* 48, IEEE Trans. Inform. Theory 28 (1982) 511–521. ⟨690⟩
[1151] W. C. Huffman and V. D. Tonchev, *The existence of extremal self-dual* $[50, 25, 10]$ *codes and quasi-symmetric* 2*-*$(49, 9, 6)$ *designs*, Des. Codes Crypt. 6 (1995) 97–106. ⟨51, 580, 689, 853, 862⟩
[1152] D. R. Hughes, *On t-designs and groups*, Amer. J. Math. 87 (1965) 761–778. ⟨82, 85⟩
[1153] D. R. Hughes and F. C. Piper, *Projective Planes*, Springer, New York, 1973. ⟨727, 729⟩
[1154] S. H. Y. Hung and N. S. Mendelsohn, *Directed triple systems*, J. Combin. Theory A 14 (1973) 310–318. ⟨19⟩
[1155] ——, *On Howell designs*, J. Combin. Theory A 16 (1974) 174–198. ⟨20, 501, 504⟩
[1156] F. K. Hwang, *Crisscross latin squares*, J. Combin. Theory A 27 (1979) 371–375. ⟨149⟩

[1157] ——, *How to design round robin schedules*, in Combinatorics, Computing and Complexity, D. Z. Du and G. D. Hu, eds., Kluwer, Dordrecht, 1989, 142–160. ⟨592⟩
[1158] F. K. Hwang and V. T. Sós, *Non-adaptive hypergeometric group testing*, Stud. Sci. Math. Hung. 22 (1987) 257–263. ⟨633⟩
[1159] H. L. Hwang, *On the structure of* (v, k, t) *trades*, J. Stat. Plann. Infer. 13 (1986) 179–191. ⟨644⟩
[1160] H. Ibrahim and W. D. Wallis, *An enumeration of triad designs*, J. Combin. Inf. Syst. Sci. (to appear). ⟨603⟩
[1161] J. E. Iiams, *On difference sets in groups of order* $4p^2$, J. Combin. Theory A 72 (1995) 256–276. ⟨426⟩
[1162] ——, *Lander's tables are complete!* in Difference Sets, Sequences and Their Correlation Properties, Kluwer, Dordrecht, 1999, 239–257. ⟨435⟩
[1163] Y. J. Ionin, *A technique for constructing symmetric designs*, Des. Codes Crypt. 14 (1998) 147–158. ⟨115, 117⟩
[1164] ——, *Applying balanced generalized weighing matrices to construct block designs*, Electron. J. Comb. 8 (2001) Research Paper 12, 15 pp. ⟨115, 116, 117⟩
[1165] ——, *Regular Hadamard matrices generating infinite families of symmetric designs*, Des. Codes Crypt. 32 (2004) 227–233. ⟨117⟩
[1166] Y. J. Ionin and H. Kharaghani, *Doubly regular digraphs and symmetric designs*, J. Combin. Theory A 101 (2003) 35–48. ⟨312, 313⟩
[1167] ——, *New families of strongly regular graphs*, J. Combin. Des. 11 (2003) 208–217. ⟨313⟩
[1168] ——, *A recursive construction for new symmetric designs*, Des. Codes Crypt. 35 (2005) 303–310. ⟨117⟩
[1169] Y. J. Ionin and K. Mackenzie-Fleming, *A technique for constructing non-embeddable quasi-residual designs*, J. Combin. Des. 10 (2002) 160–172. ⟨114⟩
[1170] Y. J. Ionin and M. S. Shrikhande, *Combinatorics of Symmetric Designs*, Cambridge Univ. Press, Cambridge, UK, 2006. ⟨115, 308, 313, 578, 582⟩
[1171] T. Ishihara, *Cameron's construction of two-graphs*, Discrete Math. 215 (2000) 283–291. ⟨877⟩
[1172] N. Ito, J. S. Leon, and J. Q. Longyear, *Classification of* 3-$(24, 12, 5)$ *designs and* 24*-dimensional Hadamard matrices*, J. Combin. Theory A 31 (1981) 66–93. ⟨36⟩
[1173] T. Ito, *Designs in a coset geometry: Delsarte theory revisited*, Europ. J. Combin. 25 (2004) 229–238. ⟨330⟩
[1174] A. V. Ivanov, *Constructive enumeration of incidence systems*, Ann. Discrete Math. 26 (1985) 227–246. ⟨36, 39, 42, 44, 46, 50, 53⟩
[1175] S. Iwasaki and T. Meixner, *A remark on the action of* $PGL(2, q)$ *and* $PSL(2, q)$ *on the projective line*, Hokkaido Math. J. 26 (1997) 203–209. ⟨82⟩
[1176] B. Jackson, *Edge-disjoint Hamilton cycles in regular graphs of large degree*, J. London Math. Soc. 19 (1979) 13–16. ⟨375⟩
[1177] W.-A. Jackson and K. M. Martin, *A combinatorial interpretation of ramp schemes*, Australas. J. Combin. 14 (1996) 51–60. ⟨636, 639⟩
[1178] M. Jacroux, *A note on the determination and construction of minimal orthogonal main-effect plans*, Technometrics 34 (1992) 92–96. ⟨548, 549⟩
[1179] ——, *On the construction of minimal partially replicated orthogonal main-effect plans*, Technometrics 35 (1993) 32–36. ⟨549⟩
[1180] ——, *A and MV-efficient block designs for comparing a set of controls to a set of test treatments*, Sankhyā B 64 (2002) 107–127. ⟨542⟩
[1181] C. Jaillet and M. Krajecki, *Solving the Langford problem in parallel*, in Proc. 3rd International Symposium on Parallel and Distributed Computing (ISPDC 2004), 2004, 83–90. ⟨616⟩
[1182] Z. Janko, *The existence of symmetric designs with parameters* $(189, 48, 12)$, J. Combin. Theory A 80 (1997) 334–338. ⟨118⟩
[1183] ——, *The existence of symmetric designs with parameters* $(105, 40, 15)$, J. Combin. Des. 7 (1999) 17–19. ⟨56, 118⟩

[1184] Z. Janko and V. D. Tonchev, *New designs with block size* 7, J. Combin. Theory A 83 (1998) 152–157. ⟨45, 72⟩
[1185] Z. Janko and Tran van Trung, *The existence of a symmetric block design for* $(70, 24, 8)$, Mitt. Math. Sem. Giessen (1984) 17–18. ⟨40, 41, 42, 118⟩
[1186] ——, *Construction of a new symmetric block design for* $(78, 22, 6)$ *with the help of tactical decompositions*, J. Combin. Theory A 40 (1985) 451–455. ⟨118⟩
[1187] ——, *Construction of two symmetric block designs for* $(71, 21, 6)$, Discrete Math. 55 (1985) 327–328. ⟨118⟩
[1188] ——, *A new biplane of order* 9 *with a small automorphism group*, J. Combin. Theory A 42 (1986) 305–309. ⟨36⟩
[1189] J. C. M. Janssen, *On even and odd latin squares*, J. Combin. Theory A 69 (1995) 173–181. ⟨151⟩
[1190] R. Jarrett, *A review of bounds for the efficiency factor of block designs*, Austral. J. Statist. 31 (1989) 118–129. ⟨541⟩
[1191] J. Jedwab and M. G. Parker, *There are no Barker arrays having more than two dimensions*, preprint. ⟨317⟩
[1192] L. Ji, *On the 3BD-closed set* $B_3(\{4, 5\})$, Discrete Math. 287 (2004) 55–67. ⟨660⟩
[1193] ——, *On the 3BD-closed set* $B_3(\{4, 5, 6\})$, J. Combin. Des. 12 (2004) 92–102. ⟨660⟩
[1194] ——, *Existence of large sets of disjoint group-divisible designs with block size three and type* $2^n 4^1$, J. Combin. Des. 13 (2005) 302–312. ⟨260⟩
[1195] ——, *A new existence proof for large sets of disjoint Steiner triple systems*, J. Combin. Theory A 112 (2005) 308–327. ⟨99⟩
[1196] ——, *Asymptotic determination of the last packing number of quadruples*, Des. Codes Crypt. 38 (2006) 83–95. ⟨551, 553⟩
[1197] L. Ji, D. Wu, and L. Zhu, *Existence of generalized Steiner systems* $GS(2, 4, v, 2)$, Des. Codes Crypt. 36 (2005) 83–99. ⟨259⟩
[1198] L. Ji and L. Zhu, *Resolvable Steiner quadruple systems for the last* 23 *orders*, SIAM J. Disc. Math. 19 (2005) 420–430. ⟨106⟩
[1199] Z. Jiang, *Rotational Steiner Triple Systems*, PhD thesis, University of Waterloo, Canada, 1995. ⟨616⟩
[1200] M. Jimbo, *Recursive constructions for cyclic BIB designs and their generalizations*, Discrete Math. 116 (1993) 79–95. ⟨410⟩
[1201] T. Johansson, *Lower bounds on the probability of deception in authentication with arbitration*, IEEE Trans. Inform. Theory 40 (1994) 1573–1585. ⟨611⟩
[1202] ——, *Further results on asymmetric authentication schemes*, Inform. Comput. 151 (1999) 100–133. ⟨611⟩
[1203] J. A. John and S. M. Lewis, *Factorial experiments in generalised cyclic row-column designs*, J. Roy. Statist. Soc. B 45 (1983) 245–251. ⟨454⟩
[1204] J. A. John and D. J. Street, *Bounds for the efficiency factor of row-column designs*, Biometrika 79 (1992) 658–661. ⟨542⟩
[1205] J. A. John and E. R. Williams, *Cyclic and Computer-Generated Designs*, Chapman and Hall, London, 1995. ⟨541, 542⟩
[1206] D. M. Johnson, A. L. Dulmage, and N. S. Mendelsohn, *Orthomorphisms of groups of orthogonal latin squares*, Canad. J. Math. 13 (1961) 356–172. ⟨164⟩
[1207] N. L. Johnson, *private communication*. ⟨38⟩
[1208] ——, *The translation planes of order* 16 *that admit nonsolvable collineation groups*, Math. Zeitschr. 185 (1984) 355–372. ⟨38⟩
[1209] N. L. Johnson and S. E. Payne, *Flocks of Laguerre planes and associated geometries*, in Mostly Finite Geometries, Dekker, New York, 1997, 51–122. ⟨475, 477⟩
[1210] S. M. Johnson, *A new upper bound for error-correcting codes*, IRE Trans. 8 (1962) 203–207. ⟨700⟩
[1211] T. Johnson, *Block Design for Piano*, Editions 75, Paris, 2005. ⟨79⟩
[1212] ——, *Kirkman's Ladies: Rational Harmonies in Three Voices*, Editions 75, Paris, 2005. ⟨13⟩
[1213] L. K. Jørgensen, *Directed strongly regular graphs*. `http://www.math.aau.dk/~leif/research/dsrg-table.html`. ⟨872⟩

[1214] ——, *Search for directed strongly regular graphs*. Report R-99-2016, Department of Mathematical Sciences, Aalborg University, 1999. ⟨872⟩
[1215] ——, *Directed strongly regular graphs with $\mu = \lambda$*, Discrete Math. 231 (2001) 289–293. ⟨870, 873⟩
[1216] ——, *Non-existence of directed strongly regular graphs*, Discrete Math. 264 (2003) 111–126. ⟨871, 872, 873⟩
[1217] L. K. Jørgensen and M. Klin, *Switching of edges in strongly regular graphs. I. A family of partial difference sets on* 100 *vertices*, Electron. J. Comb. 10 (2003) R17. ⟨858⟩
[1218] J.-H. Ju and V. O. K. Li, *An optimal topology-transparent scheduling method in multihop packet radio networks*, IEEE/ACM Trans. Networking 6 (1998) 298–306. ⟨632⟩
[1219] S. Jukna, *Extremal Combinatorics*, Springer-Verlag, Berlin, 2001. ⟨391⟩
[1220] D. Jungnickel, *Composition theorems for difference families and regular planes*, Discrete Math. 23 (1978) 151–158. ⟨399⟩
[1221] ——, *On difference matrices, resolvable transversal designs and generalized Hadamard matrices*, Math. Zeitschr. 167 (1979) 49–60. ⟨411, 412⟩
[1222] ——, *On automorphism groups of divisible designs*, Canad. J. Math. 34 (1982) 257–297. ⟨302, 313, 730⟩
[1223] ——, *The number of designs with classical parameters grows exponentially*, Geom. Ded. 16 (1984) 167–178. ⟨40, 41, 47, 56, 699⟩
[1224] ——, *Quasimultiples of biplanes and residual biplanes*, Ars Combin. 19 (1985) 179–186. ⟨36, 37, 39, 41, 43, 44, 48, 51, 54⟩
[1225] ——, *Quasimultiples of projective and affine planes*, J. Geom. 26 (1986) 172–181. ⟨36, 39, 40, 42, 45, 49, 52, 56⟩
[1226] ——, *Latin squares, their geometries and their groups. A survey*, in Coding Theory and Design Theory II, D. K. Ray-Chaudhuri, ed., Springer, New York, 1990, 166–225. ⟨189⟩
[1227] ——, *On automorphism groups of divisible designs. II. Group invariant generalised conference matrices*, Arch. Math. (Basel) 54 (1990) 200–208. ⟨313⟩
[1228] ——, *On the existence of small quasimultiples of affine and projective planes of arbitrary order*, Discrete Math. 85 (1990) 177–189. ⟨37⟩
[1229] ——, *Maximal partial spreads and transversal-free translation nets*, J. Combin. Theory A 62 (1993) 66–92. ⟨189, 561⟩
[1230] ——, *Maximal sets of mutually orthogonal latin squares*, in Finite Fields and Applications, Cambridge Univ. Press, Cambridge, 1996, 129–153. ⟨193⟩
[1231] D. Jungnickel and H. Kharaghani, *Balanced generalized weighing matrices and their applications*, Le Matematiche 59 (2004) 225–261. ⟨313⟩
[1232] D. Jungnickel, V. C. Mavron, and T. P. McDonough, *The geometry of frequency squares*, J. Combin. Theory A 96 (2001) 376–387. ⟨467⟩
[1233] D. Jungnickel, R. C. Mullin, and S. A. Vanstone, *The spectrum of α-resolvable block designs with block size* 3, Discrete Math. 97 (1991) 269–277. ⟨130⟩
[1234] D. Jungnickel and A. Pott, *A new class of symmetric (v, k, λ)-designs*, Des. Codes Crypt. 4 (1994) 319–325. ⟨117⟩
[1235] D. Jungnickel and V. D. Tonchev, *Exponential number of quasi-symmetric SDP designs and codes meeting the Grey–Rankin bound*, Des. Codes Crypt. 1 (1991) 247–253. ⟨580, 582, 694, 695⟩
[1236] ——, *On symmetric and quasi-symmetric designs with the symmetric difference property and their codes*, J. Combin. Theory A 59 (1992) 40–50. ⟨38, 44, 45, 580, 582, 694, 696⟩
[1237] ——, *Perfect codes and balanced generalized weighing matrices*, Finite Fields Appl. 5 (1999) 294–300. ⟨313⟩
[1238] ——, *Perfect codes and balanced generalized weighing matrices. II*, Finite Fields Appl. 8 (2002) 155–165. ⟨313⟩

[1239] D. Jungnickel and K. Vedder, *Simple quasidoubles of projective planes*, Aequat. Math. 34 (1987) 96–100. ⟨36, 38, 39, 40, 42, 45, 49, 52, 56⟩
[1240] R. N. Kacker, E. S. Lagergren, and J. J. Filliben, *Taguchi's fixed element arrays are fractional factorials*, J. Qual. Technol. 23 (1991) 107–116. ⟨451⟩
[1241] S. Kageyama, *A survey of resolvable solutions of balanced incomplete block designs*, Rev. Inst. Internat. Statist. 40 (1972) 269–273. ⟨35, 36, 37, 38, 40, 43, 45, 49, 53⟩
[1242] ———, *Reduction of associate classes for block designs and related combinatorial arrangements*, Hiroshima Math. J. 4 (1974) 527–618. ⟨562⟩
[1243] ———, *A resolvable solution of* BIBD$(18, 51, 17, 6, 5)$, Ars Combin. 15 (1983) 315–316. ⟨38⟩
[1244] ———, *A property of t-wise balanced designs*, Ars Combin. 31 (1991) 237–238. ⟨658⟩
[1245] S. Kageyama and A. S. Hedayat, *The family of t-designs—Part II*, J. Stat. Plann. Infer. 7 (1982/83) 257–287. ⟨97⟩
[1246] S. Kageyama and Y. Miao, *A construction of resolvable designs*, Utilitas Math. 46 (1994) 49–54. ⟨126⟩
[1247] ———, *A construction for resolvable designs and its generalizations*, Graphs Combin. 14 (1998) 11–24. ⟨265⟩
[1248] Q. D. Kang, *Large sets of combinatorial designs*, Adv. Math. (China) 32 (2003) 269–284. ⟨534⟩
[1249] Q. D. Kang, Y. X. Chang, and G. Yang, *The spectrum of self-converse DTS*, J. Combin. Des. 2 (1994) 415–425. ⟨442⟩
[1250] S. Kantor, *Die Configurationen* $(3, 3)_{10}$, Sitzungsber. Akad. Wiss. Wien, Math.-Nat. Kl. 84 (1881) 1291–1314. ⟨14⟩
[1251] W. M. Kantor, *private communication.* ⟨43, 45⟩
[1252] ———, *Characterizations of finite projective and affine spaces*, Canad. J. Math. 21 (1969) 64–75. ⟨851⟩
[1253] ———, *Symplectic groups, symmetric designs, and line ovals*, J. Algebra 33 (1975) 43–58. ⟨694⟩
[1254] ———, *Generalized quadrangles associated with $G_2(q)$*, J. Combin. Theory A 29 (1980) 212–219. ⟨474, 476⟩
[1255] ———, *Exponential numbers of two-weight codes, difference sets and symmetric designs*, Discrete Math. 46 (1983) 95–98. ⟨701⟩
[1256] ———, *Classification of 2-transitive symmetric designs*, Graphs Combin. 1 (1985) 165–166. ⟨112⟩
[1257] ———, *Homogeneous designs and geometric lattices*, J. Combin. Theory A 38 (1985) 66–74. ⟨342⟩
[1258] ———, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. Algebra 106 (1987) 15–45. ⟨342⟩
[1259] ———, *2-transitive and flag-transitive designs*, Wiley, New York, 1993, 13–30. ⟨341⟩
[1260] ———, *Automorphisms and isomorphisms of symmetric and affine designs*, J. Algeb. Combin. 3 (1994) 307–338. ⟨113⟩
[1261] ———, *Note on GMW designs*, Electron. J. Comb. 22 (2001) 63–69. ⟨423⟩
[1262] S. Kapralov and S. Topalova, *Enumeration of* 2-$(21, 6, 3)$ *designs with automorphisms of order* 7 *or* 5, Ars Combin. 48 (1998) 135–146. ⟨36⟩
[1263] P. Kaski, *Isomorph-free exhaustive generation of designs with prescribed groups of automorphisms*, SIAM J. Disc. Math. 19 (2005) 664–690. ⟨36⟩
[1264] P. Kaski, L. B. Morales, P. R. J. Östergård, D. A. Rosenblueth, and C. Velarde, *Classification of resolvable* 2-$(14, 7, 12)$ *and* 3-$(14, 7, 5)$ *designs*, J. Combin. Math. Combin. Comput. 47 (2003) 65–74. ⟨43⟩
[1265] P. Kaski and P. R. J. Östergård, *There exists no* $(15, 5, 4)$ *RBIBD*, J. Combin. Des. 9 (2001) 357–362. ⟨37, 762⟩
[1266] ———, *Enumeration of balanced ternary designs*, Discrete Appl. Math. 138 (2004) 133–141. ⟨332⟩
[1267] ———, *Miscellaneous classification results for* 2*-designs*, Discrete Math. 280 (2004) 65–75. ⟨36, 37⟩

[1268] ——, *The Steiner triple systems of order* 19, Math. Comp. 73 (2004) 2075–2092. ⟨15, 36, 60, 62, 269, 759, 775, 781⟩
[1269] ——, *There exist non-isomorphic STS*(19) *with equivalent point codes*, J. Combin. Des. 12 (2004) 443–448. ⟨691⟩
[1270] ——, *One-factorizations of regular graphs of order* 12, Electron. J. Comb. 12, Research Paper 2, 25 pp. (2005). ⟨748, 762⟩
[1271] ——, *Classification Algorithms for Codes and Designs*, Springer, Berlin, 2006. ⟨37, 38, 41, 44, 50, 58, 152, 280, 755, 758, 762, 775, 780, 782⟩
[1272] ——, *There exists no symmetric configuration with 33 points and line size 6*, preprint (2006). ⟨354⟩
[1273] P. Kaski, P. R. J. Östergård, and O. Pottonen, *The Steiner quadruple systems of order 16*, J. Combin. Theory A (to appear). ⟨106, 692⟩
[1274] A. D. Keedwell, *Sequenceable groups: A survey*, in Finite Geometries and Designs, P. J. Cameron, J. W. P. Hirschfield, and D. R. Hughes, eds., Cambridge Univ. Press, Cambridge, 1980, 205–215. ⟨352⟩
[1275] ——, *Critical sets in latin squares and related matters: An update*, Utilitas Math. 65 (2004) 97–131. ⟨148⟩
[1276] L. M. Kelly and S. Nwankpa, *Affine embeddings of Sylvester–Gallai designs*, J. Combin. Theory A 14 (1973) 422–438. ⟨269⟩
[1277] A. B. Kempe, *A memoir on the theory of mathematical form*, Phil. Trans. Ser. I 177 (1886) 1–70. ⟨14⟩
[1278] G. T. Kennedy and V. S. Pless, *On designs and formally self-dual codes*, Des. Codes Crypt. 4 (1994) 43–55. ⟨682⟩
[1279] T. Kepka and P. Němec, *Commutative Moufang loops and distributive groupoids of small orders*, Czechoslovak Math. J. 31(106) (1981) 633–669. ⟨849⟩
[1280] M. S. Keranen, R. S. Rees, and A. C. H. Ling, *The spectrum of α-resolvable block designs with block size four*, J. Combin. Des. 9 (2001) 1–16. ⟨132⟩
[1281] J. D. Key, *Ternary codes of Steiner triple systems*, J. Combin. Des. 2 (1994) 25–30. ⟨701⟩
[1282] J. D. Key and F. E. Sullivan, *Codes of Steiner triple and quadruple systems*, Des. Codes Crypt. 3 (1993) 117–125. ⟨701⟩
[1283] J. D. Key and V. D. Tonchev, *Computational results for the known biplanes of order* 9, in Geometry, Combinatorial Designs and Related Structures, J. W. P. Hirschfeld, S. S. Magliveras, and M. J. De Resmini, eds., Cambridge Univ. Press, Cambridge, 1997, 113–122. ⟨114⟩
[1284] H. Kharaghani, *Arrays for orthogonal designs*, J. Combin. Des. 8 (2000) 166–173. ⟨286⟩
[1285] ——, *On the twin designs with the Ionin-type parameters*, Electron. J. Comb. 7 (2000). 11 pp. ⟨117⟩
[1286] H. Kharaghani and B. Tayfeh-Rezaie, *Some new orthogonal designs in orders* 32 *and* 40, Discrete Math. 279 (2004) 317–324. ⟨282, 294⟩
[1287] ——, *A Hadamard matrix of order* 428, J. Combin. Des. 13 (2005) 435–440. ⟨277, 762⟩
[1288] G. B. Khosrovshahi and S. Ajoodani-Namini, *A new basis for trades*, SIAM J. Disc. Math. 3 (1990) 364–372. ⟨646⟩
[1289] G. B. Khosrovshahi, R. Laue, and B. Tayfeh-Rezaie, *On large sets of size four*, Bayreuth. Math. Schr. 74 (2005) 136–144. ⟨99⟩
[1290] G. B. Khosrovshahi, H. R. Maimani, and R. Torabi, *On trades: An update*, Discrete Appl. Math. 95 (1999) 361–376. ⟨644, 646, 647, 648⟩
[1291] ——, *An automorphism-free* 4-(15, 5, 5) *design*, J. Combin. Math. Combin. Comput. 37 (2001) 197–192. ⟨85⟩
[1292] G. B. Khosrovshahi, M. Mohammad-Noori, and B. Tayfeh-Rezaie, *Classification of* 6-(14, 7, 4) *designs with nontrivial automorphism group*, J. Combin. Des. 10 (2002) 180–194. ⟨81⟩
[1293] G. B. Khosrovshahi and B. Tayfeh-Rezaie, *Root cases of large sets of t-designs*, Discrete Math. 263 (2003) 143–155. ⟨99⟩

[1294] ———, *Large sets of t-designs through partitionable sets: A survey*, Discrete Math. (to appear). ⟨98, 99, 101⟩
[1295] R. E. Kibler, *A summary of noncyclic difference sets, $k < 20$*, J. Combin. Theory A 25 (1978) 62–67. ⟨430, 431, 432, 433⟩
[1296] J. Kiefer, *Balanced block designs and generalized Youden designs I. Construction (patchwork)*, Ann. Statist. 3 (1975) 109–118. ⟨673⟩
[1297] ———, *Construction and optimality of generalized Youden designs*, in A Survey of Statistical Design and Linear Models, J. N. Srivastava, ed., North-Holland, Amsterdam, 1975, 333–353. ⟨542⟩
[1298] H. K. Kim and V. Lebedev, *On optimal superimposed codes*, J. Combin. Des. 12 (2004) 79–91. ⟨635⟩
[1299] H. Kimura, *Extremal doubly even $(56, 28, 12)$ codes and Hadamard matrices of order 28*, Australas. J. Combin. 10 (1994) 153–161. ⟨683⟩
[1300] T. P. Kirkman, *On a problem in combinations*, Cambridge and Dublin Math. J. 2 (1847) 191–204. ⟨12, 15, 59⟩
[1301] ———, *Note on a unanswered prize question*, Cambridge and Dublin Math. J. 5 (1850) 255–262. ⟨14⟩
[1302] ———, *On the triads made with fifteen things*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. 37 (1850) 169–171. ⟨13⟩
[1303] ———, *Query VI*, Lady's and Gentleman's Diary (1850) 48. ⟨12⟩
[1304] ———, *On the perfect r-partitions of $r^2 - r + 1$*, Transactions of the Historic Society of Lancashire and Cheshire (1857) 127–142. ⟨14⟩
[1305] ———, *On the puzzle of the fifteen young ladies*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. 23 (1862) 198–204. ⟨13, 14⟩
[1306] ———, *Solutions of three problems proposed by W. Lea*, Educational Times Reprints 11 (1869) 97–99. ⟨17⟩
[1307] K. Kishen, *On the design of experiments for weighing and making other types of measurements*, Ann. Math. Stat. 16 (1945) 294–300. ⟨19⟩
[1308] ———, *On the construction of latin and hyper-graeco-latin cubes and hypercubes*, J. Indian Soc. Agric. Statistics 2 (1949) 20–48. ⟨468⟩
[1309] A. Klappenecker and M. Rötteler, *Mutually unbiased bases are complex projective 2-designs*, in Proc. 2005 IEEE International Symposium on Information Theory, IEEE, 2005, 1740–1744. ⟨621⟩
[1310] J. P. C. Kleijnen, *A practical comment on resolution IV designs: Bad properties of quantitative factors*, Commun. Stat. Theory Methods 16 (1987) 805–812. ⟨448⟩
[1311] M. Klin, A. Munemasa, M. Muzychuk, and P.-H. Zieschang, *Directed strongly regular graphs obtained from coherent algebras*, Lin. Alg. Appl. 377 (2004) 83–109. ⟨869, 870, 872⟩
[1312] M. Klin, C. Pech, and P.-H. Zieschang, *Flag algebras of block designs: I. Initial notions, Steiner 2-designs, and generalized quadrangles*. Report MATH-AL-10-1998, Technische Universität Dresden. ⟨870⟩
[1313] T. Kløve, *Bounds and construction for difference triangle sets*, IEEE Trans. Inform. Theory 35 (1989) 879–886. ⟨439, 440⟩
[1314] E. Knill, A. Schliep, and D. C. Torney, *Interpretation of pooling experiments using the Markov chain Monte Carlo method*, J. Comp. Biol. 3 (1996) 395–406. ⟨575⟩
[1315] D. E. Knuth, *Dancing links*, in Millennial Perspectives in Computer Science, J. Davies, B. Roscoe, and J. Woodcock, eds., Palgrave, Basingstoke, England, 2000, 187–214. ⟨758⟩
[1316] A. Koblinsky, *Confounding in relation to duality of finite abelian groups*, Lin. Alg. Appl. 70 (1985) 321–347. ⟨465⟩
[1317] ———, *Orthogonal factorial designs for quantitative factors*, Stat. Decisions Suppl. 2 (1985) 275–285. ⟨448⟩
[1318] W. L. Kocay, D. R. Stinson, and S. A. Vanstone, *On strong starters in cyclic groups*, Discrete Math. 56 (1985) 45–60. ⟨625, 762⟩
[1319] W. L. Kocay and G. H. J. Van Rees, *Some nonisomorphic $(4t + 4, 8t + 6, 4t + 3, 2t + 2, 2t + 1)$-BIBDs*, Discrete Math. 92 (1991) 159–172. ⟨37, 39, 44, 47⟩

[1320] E. Köhler, *Über den allgemeinen Gray-Code und die Nichtexistenz einiger t-Designs*, in Graphen in Forschung und Unterricht, Festschrift K. Wagner, R. Bodendieck, ed., Franzbecker, Salzdetfurth, Germany, 1985, 102–111. ⟨87⟩
[1321] T. Kölmel, *Symmetric* $(49, 16, 5)$ *designs*, Ars Combin. 38 (1994) 47–55. ⟨38⟩
[1322] T. H. Koornwinder, *A note on the absolute bound for systems of lines*, Proc. KNAW A 79 (1976) 152–153. ⟨855⟩
[1323] L. E. Kopilovich, *Difference sets in noncyclic abelian groups*, Cybernetics 25 (1989) 153–157. ⟨435⟩
[1324] G. Korchmáros, *Ovali nei piani di Hall di ordine dispari*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 56 (1974) 315–317. ⟨728⟩
[1325] J. Korevaar and J. L. H. Meyers, *Chebyshev-type quadrature on multidimensional domains*, J. Approx. Theory 79 (1994) 144–164. ⟨620⟩
[1326] A. Kotzig, *Decompositions of complete graphs into isomorphic cubes*, J. Combin. Theory B 31 (1981) 292–296. ⟨480, 484⟩
[1327] A. Kotzig and J. Labelle, *Strongly hamiltonian graphs*, Utilitas Math. 14 (1978) 99–116. ⟨752⟩
[1328] S. Koubi, M. Mata, and N. Shalaby, *Using directed hill-climbing for the construction of difference triangle sets*, IEEE Trans. Inform. Theory 51 (2005) 335–339. ⟨439⟩
[1329] C. Koukouvinos, S. Kounias, and J. R. Seberry, *Supplementary difference sets and optimal designs*, Discrete Math. 88 (1991) 49–58. ⟨297⟩
[1330] C. Koukouvinos, S. Kounias, J. R. Seberry, C. H. Yang, and J. Yang, *Multiplication of sequences with zero autocorrelation*, Australas. J. Combin. 10 (1994) 5–15. ⟨321⟩
[1331] C. Koukouvinos, N. Platis, and J. R. Seberry, *Necessary and sufficient conditions for some two variable orthogonal designs in order* 36, Congr. Numer. 114 (1996) 129–139. ⟨295⟩
[1332] C. Koukouvinos and J. R. Seberry, *New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function—A review*, J. Stat. Plann. Infer. 81 (1999) 153–182. ⟨292, 293⟩
[1333] E. S. Kramer, *Some t-designs for* $t \geq 4$ *and* $v = 17, 18$, Congr. Numer. 14 (1975) 443–460. ⟨84, 85, 86, 87, 766⟩
[1334] ———, *Some results on t-wise balanced designs*, Ars Combin. 15 (1983) 179–192. ⟨658, 659, 660⟩
[1335] ———, *The t-designs using* $M_{21} \simeq PSL_3(4)$ *on* 21 *points*, Ars Combin. 17 (1984) 191–208. ⟨85, 86, 87⟩
[1336] ———, *An* $S_3(3, 5, 21)$ *using graphs*, Discrete Math. 81 (1990) 223–224. ⟨491⟩
[1337] E. S. Kramer, D. W. Leavitt, and S. S. Magliveras, *Construction procedures for t-designs and the existence of new simple* 6*-designs*, Ann. Discrete Math. 26 (1985) 247–273. ⟨85, 86, 87, 92⟩
[1338] E. S. Kramer and S. S. Magliveras, *Some mutually disjoint Steiner systems*, J. Combin. Theory A 17 (1974) 39–43. ⟨85, 86, 87⟩
[1339] E. S. Kramer, S. S. Magliveras, and R. A. Mathon, *The Steiner systems* $S(2, 4, 25)$ *with nontrivial automorphism group*, Discrete Math. 77 (1989) 137–157. ⟨36, 882⟩
[1340] E. S. Kramer, S. S. Magliveras, and E. A. O'Brien, *Some new large sets of t-designs*, Australas. J. Combin. 7 (1993) 189–193. ⟨82⟩
[1341] E. S. Kramer and R. A. Mathon, *Proper* $S(t, K, \nu)$*'s for* $t \geq 3$, $\nu \leq 16$, $|K| > 1$ *and their extensions*, J. Combin. Des. 3 (1995) 411–425. ⟨660⟩
[1342] E. S. Kramer and D. M. Mesner, *Intersections among Steiner systems*, J. Combin. Theory A 16 (1974) 273–285. ⟨85⟩
[1343] ———, *t-designs on hypergraphs*, Discrete Math. 15 (1976) 263–296. ⟨84, 85, 490, 763⟩
[1344] E. S. Kramer, Q.-R. Wu, S. S. Magliveras, and Tran van Trung, *Some perpendicular arrays for arbitrarily large t*, Discrete Math. 96 (1991) 101–110. ⟨545⟩
[1345] I. Krasikov and Y. Roditty, *On a reconstruction problem for sequences*, J. Combin. Theory A 77 (1997) 344–348. ⟨386⟩

[1346] V. Krčadinac, *Steiner 2-designs $S(2,4,28)$ with nontrivial automorphisms*, Glas. Mat. III 37(57) (2002) 259–268. ⟨36⟩
[1347] ——, *Steiner 2-designs $S(2,5,41)$ with automorphisms of order 3*, J. Combin. Math. Combin. Comput. 43 (2002) 83–99. ⟨36⟩
[1348] ——, *Konstrukcija i klasifikacija konačnih struktura pomoću računala*, PhD thesis, University of Zagreb, 2004. ⟨354⟩
[1349] ——, *Some new Steiner 2-designs $S(2,4,37)$*, Ars Combin. 78 (2006) 127–135. ⟨36⟩
[1350] D. L. Kreher, *An infinite family of (simple) 6-designs*, J. Combin. Des. 1 (1993) 277–280. ⟨92, 94⟩
[1351] D. L. Kreher, Y. M. Chee, D. de Caen, C. J. Colbourn, and E. S. Kramer, *Some new simple t-designs*, J. Combin. Math. Combin. Comput. 7 (1990) 53–90. ⟨84, 85, 86, 87, 491⟩
[1352] D. L. Kreher and S. P. Radziszowski, *The existence of simple 6-$(14,7,4)$ designs*, J. Combin. Theory A 43 (1986) 237–243. ⟨81, 86, 766⟩
[1353] ——, *Finding simple t-designs by using basis reduction*, Congr. Numer. 55 (1986) 235–244. ⟨764, 765, 766⟩
[1354] ——, *New t-designs found by basis reduction*, Congr. Numer. 59 (1987) 155–164. ⟨85⟩
[1355] ——, *Simple 5-$(28,6,\lambda)$ designs from $PSL_2(27)$*, Ann. Discrete Math. 34 (1987) 315–318. ⟨89⟩
[1356] D. L. Kreher and R. S. Rees, *A hole-size bound for incomplete t-wise balanced designs*, J. Combin. Des. 9 (2001) 269–284. ⟨659⟩
[1357] ——, *On the maximum size of a hole in an incomplete t-wise balanced design with specified minimum block size*, in Codes and Designs, K. T. Arasu and A. Seress, eds., de Gruyter, Berlin, 2002, 179–186. ⟨659⟩
[1358] D. L. Kreher, G. F. Royle, and W. D. Wallis, *A family of resolvable regular graph designs*, Discrete Math. 156 (1996) 269–275. ⟨602⟩
[1359] D. L. Kreher and D. R. Stinson, *Small group-divisible designs with block size four*, J. Stat. Plann. Infer. 58 (1997) 111–118. ⟨257⟩
[1360] ——, *Combinatorial Algorithms: Generation, Enumeration, and Search*, CRC Press, Boca Raton, 1999. ⟨758, 764, 779, 780, 782⟩
[1361] M. G. Kreĭn, *Hermitian-positive kernels II*, Amer. Math. Soc. Transl. Ser. 2 34 (1963) 109–164. ⟨855⟩
[1362] R. A. Kristiansen and M. G. Parker, *Binary sequences with merit factor > 6.3*, IEEE Trans. Inform. Theory 50 (2004) 3385–3389. ⟨317⟩
[1363] A. M. Kshirsagar and S. A. N. Stehouwer, *Efficiency of Bailey's trigonometric levels in factorial experiments*, Commun. Stat. Theory Methods 16 (1987) 1655–1673. ⟨448⟩
[1364] S. Küçükçifçi, *The number of 8-cycles in 2-factorizations of K_{2n} minus a 1-factor*, Utilitas Math. 61 (2002) 225–237. ⟨377⟩
[1365] R. O. Kuehl, *Design of Experiments: Statistical Principles of Research Design and Analysis*, Duxbury, Pacific Grove, 2000. ⟨445⟩
[1366] P. V. Kumar, R. A. Scholtz, and L. R. Welch, *Generalized bent functions and their properties*, J. Combin. Theory A 40 (1985) 90–107. ⟨339⟩
[1367] J. Kunert, *A note on optimal designs with a non-orthogonal row-column-structure*, J. Stat. Plann. Infer. 37 (1993) 265–270. ⟨542⟩
[1368] T. Kunkle and D. G. Sarvate, *Balanced (part) ternary designs*, in The CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz, eds., CRC Press, Boca Raton FL, 1996, 233–238. ⟨331⟩
[1369] A. H. Lachlan, *Two conjectures regarding the stability of ω-categorical theories*, Fund. Math. 81 (1973/74) 133–145. ⟨505⟩
[1370] C. W. H. Lam, *How reliable is a computer-based proof?* Math. Intelligencer 12 (1990) 8–12. ⟨775⟩
[1371] ——, *The search for a finite projective plane of order 10*, Amer. Math. Monthly 98 (1991) 305–318. ⟨701⟩

[1372] C. W. H. Lam, R. Bilous, L. H. Thiel, B. Li, G. H. J. Van Rees, S. P. Radziszowski, W. H. Holzmann, and H. Kharaghani, *There is no* $(22, 8, 4)$ *block design*, J. Combin. Des. (to appear). ⟨36, 72, 74, 762⟩
[1373] C. W. H. Lam, G. Kolesova, and L. H. Thiel, *A computer search for finite projective planes of order* 9, Discrete Math. 92 (1991) 187–195. ⟨36⟩
[1374] C. W. H. Lam, S. Lam, and V. D. Tonchev, *Bounds on the number of affine, symmetric, and Hadamard designs and matrices*, J. Combin. Theory A 92 (2000) 186–196. ⟨37, 39, 40, 54, 699⟩
[1375] ——, *Bounds on the number of Hadamard designs of even order*, J. Combin. Des. 9 (2001) 363–378. ⟨38, 41⟩
[1376] C. W. H. Lam and Y. Miao, *On cyclically resolvable cyclic Steiner* 2*-designs*, J. Combin. Theory A 85 (1999) 194–207. ⟨404⟩
[1377] C. W. H. Lam, Y. Miao, and M. Mishima, *Cyclically resolvable cyclic Steiner* 2*-systems* $S(2, 4, 52)$, J. Stat. Plann. Infer. 95 (2001) 245–256. ⟨38⟩
[1378] C. W. H. Lam, L. H. Thiel, and S. Swiercz, *The nonexistence of finite projective planes of order* 10, Canad. J. Math. 41 (1989) 1117–1123. ⟨36, 111, 762, 775, 776⟩
[1379] C. W. H. Lam, L. H. Thiel, and V. D. Tonchev, *On quasi-symmetric* 2*-*$(28, 12, 11)$ *and* 2*-*$(36, 16, 12)$ *designs*, Des. Codes Crypt. 5 (1995) 43–55. ⟨44, 580, 694, 701⟩
[1380] C. W. H. Lam and V. D. Tonchev, *Classification of affine resolvable* 2*-*$(27, 9, 4)$ *designs*, J. Stat. Plann. Infer. 56 (1996) 187–202. Correction: 86 (2000), 277-278. ⟨37, 699, 701⟩
[1381] ——, *A new bound on the number of designs with classical affine parameters*, Des. Codes Crypt. 27 (2002) 111–117. ⟨37⟩
[1382] P. Lambossy, *Sur une manière de différencier les fonctions cycliques d'une forme donnée*, Comment. Math. Helv. 3 (1931) 69–102. ⟨16⟩
[1383] E. R. Lamken, *Constructions for resolvable and near resolvable BIBDs*, in Coding Theory and Design Theory II, D. K. Ray-Chaudhuri, ed., Springer, New York, 1990, 236–250. ⟨130⟩
[1384] ——, *Generalized balanced tournament designs*, Trans. Amer. Math. Soc. 318 (1990) 473–490. ⟨336⟩
[1385] ——, *The existence of doubly near resolvable* $(v, 3, 2)$ *BIBDs*, J. Combin. Des. 2 (1994) 427–440. ⟨130⟩
[1386] ——, *The existence of doubly resolvable* $(v, 3, 2)$*-BIBDs*, J. Combin. Theory A 72 (1995) 50–76. ⟨130, 336⟩
[1387] ——, *A few more partitioned balanced tournament designs*, Ars Combin. 43 (1996) 121–134. ⟨335, 589⟩
[1388] ——, *The existence of partitioned generalized balanced tournament designs with block size* 3, Des. Codes Crypt. 11 (1997) 37–71. ⟨336⟩
[1389] ——, *The existence of* $KS_3(v, 2, 4)$, Discrete Math. 186 (1998) 195–216. ⟨131⟩
[1390] ——, *Room squares and self-orthogonal latin squares*, preprint (2005). ⟨585⟩
[1391] ——, *Designs with orthogonal resolutions and decompositions of edge-colored complete graphs*, preprint (2006). ⟨130⟩
[1392] ——, *Stadium balanced arrays*, preprint (2006). ⟨594⟩
[1393] E. R. Lamken, W. H. Mills, and R. S. Rees, *Resolvable minimum coverings with quadruples*, J. Combin. Des. 6 (1998) 431–450. ⟨372, 602⟩
[1394] E. R. Lamken and S. A. Vanstone, *Designs with mutually orthogonal resolutions*, Europ. J. Combin. 7 (1986) 249–257. ⟨502⟩
[1395] ——, *Elliptic semiplanes and group divisible designs with orthogonal resolutions*, Aequat. Math. 30 (1986) 80–92. ⟨731⟩
[1396] ——, *Balanced tournament designs and related topics*, Discrete Math. 77 (1989) 159–176. ⟨335, 336⟩
[1397] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge Univ. Press, Cambridge, 1983. ⟨113, 421, 422, 435, 788, 790⟩
[1398] I. Landjev and S. Topalova, *New symmetric* $(61, 16, 4)$ *designs invariant under the dihedral group of order* 10, Serdica Math. J. 24 (1998) 179–186. ⟨38⟩

[1399] R. Laue, *Construction of combinatorial objects—A tutorial*, Bayreuth. Math. Schr. 43 (1993) 53–96. ⟨764⟩
[1400] ——, *Halvings on small point sets*, J. Combin. Des. 7 (1999) 233–241. ⟨99⟩
[1401] ——, *Constructing objects up to isomorphism, simple* 9*-designs with small parameters*, in Algebraic Combinatorics and Applications, A. Betten, A. Kohnert, R. Laue, and A. Wassermann, eds., Springer, Berlin, 2001, 232–260. ⟨91, 96, 97, 766⟩
[1402] ——, *Solving isomorphism problems for* t*-designs*, in Designs 2002, W. D. Wallis, ed., Kluwer, 2003, 277–300. ⟨97⟩
[1403] ——, *Resolvable* t*-designs*, Des. Codes Crypt. 32 (2004) 277–301. ⟨82, 110⟩
[1404] R. Laue, S. S. Magliveras, and A. Wassermann, *New large sets of* t*-designs*, J. Combin. Des. 9 (2001) 40–59. ⟨98, 101⟩
[1405] R. Laue, G. R. Omidi, B. Tayfeh-Rezaie, and A. Wassermann, *New large sets of* t*-designs with prescribed automorphism groups*, J. Combin. Des. (to appear). ⟨98, 99⟩
[1406] R. Laue, H. Vogel, and A. Wassermann, *Simple* 8*-*$(40, 12, \lambda)$ *designs from* $PSL(4, 3)$, Bayreuth. Math. Schr. 74 (2005) 233–238. ⟨96⟩
[1407] K. M. Lawrence, *A combinatorial characterization of* (t, m, s)*-nets in base* b, J. Combin. Des. 4 (1996) 275–293. ⟨643⟩
[1408] C. F. Laywine, *A geometric construction for sets of mutually orthogonal frequency squares*, Utilitas Math. 35 (1989) 95–102. ⟨466⟩
[1409] ——, *Complete sets of orthogonal frequency squares and affine resolvable designs*, Utilitas Math. 43 (1993) 161–170. ⟨466⟩
[1410] ——, *An affine design with* $v = m^{2h}$ *and* $k = m^{2h-1}$ *not equivalent to a complete set of* $F(m^h; m^{h-1})$ *MOFS*, J. Combin. Des. 7 (1999) 331–340. ⟨467⟩
[1411] C. F. Laywine and D. McCarthy, *A complete set of type 0 hypercubes not equivalent to a latin set*, J. Combin. Math. Combin. Comput. 41 (2002) 123–131. ⟨470⟩
[1412] C. F. Laywine and G. L. Mullen, *Generalizations of Bose's equivalence between complete sets of mutually orthogonal latin squares and affine planes*, J. Combin. Theory A 61 (1992) 13–35. ⟨466⟩
[1413] ——, *Discrete Mathematics Using Latin Squares*, Wiley, New York, 1998. ⟨152, 470, 471⟩
[1414] ——, *A table of lower bounds for the number of mutually orthogonal frequency squares*, Ars Combin. 59 (2001) 85–96. ⟨466⟩
[1415] ——, *A hierarchy of complete orthogonal structures*, Ars Combin. 63 (2002) 75–88. ⟨470⟩
[1416] C. F. Laywine, G. L. Mullen, and G. Whittle, *d-dimensional hypercubes and the Euler and MacNeish conjectures*, Monatsh. Math. 119 (1995) 223–238. ⟨469, 470, 471⟩
[1417] F. Lazebnik and A. Thomason, *Orthomorphisms and the construction of projective planes*, Math. Comp. 73 (2004) 1547–1557. ⟨346⟩
[1418] W. Lea, *Solution of the question 2244*, Educational Times Reprints 9 (1868) 35–36. ⟨17⟩
[1419] T. C. Y. Lee, *Tools for constructing RBIBDs, Frames, NRBs and SOLSSOMs*, PhD thesis, University of Waterloo, 1995. ⟨127⟩
[1420] T. C. Y. Lee and S. C. Furino, *A translation of J.X. Lu's "An existence theory for resolvable balanced incomplete block designs"*, J. Combin. Des. 3 (1995) 321–340. ⟨132⟩
[1421] E. Lehmer, *On residue difference sets*, Canad. J. Math. 5 (1953) 425–432. ⟨116⟩
[1422] J.-G. Lei, *Completing the spectrum for* LGDD(m^v), J. Combin. Des. 5 (1997) 1–11. ⟨260⟩
[1423] ——, *On large sets of Kirkman systems with holes*, Discrete Math. 254 (2002) 259–274. ⟨66⟩
[1424] A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982) 515–534. ⟨765⟩

[1425] H. W. Lenstra and M. Zieve, *A family of exceptional polynomials in characteristic three*, in Finite Fields and Applications, S. Cohen and H. Niederreiter, eds., Cambridge Univ. Press, Cambridge, 1992, 209–218. ⟨573⟩
[1426] H. Lenz, *Some remarks on pairwise balanced designs*, Mitt. Math. Sem. Giessen 165 (1984) 49–62. ⟨250, 251⟩
[1427] V. K. Leont′ev and Y. G. Smetanin, *Reconstruction of vectors from sets of their fragments*, Dokl. Akad. Nauk SSSR 302 (1988) 1319–1322. ⟨386⟩
[1428] K. H. Leung, S. L. Ma, and B. Schmidt, *Nonexistence of abelian difference sets: Lander's conjecture for prime power orders*, Trans. Amer. Math. Soc. 356 (2004) 4343–4358. ⟨422⟩
[1429] K. H. Leung and B. Schmidt, *Asymptotic nonexistence of difference sets in dihedral groups*, J. Combin. Theory A (2002) 261–280. ⟨426⟩
[1430] ——, *The field descent method*, Des. Codes Crypt. 36 (2005) 171–188. ⟨275, 426⟩
[1431] N. Levanon, *Radar Principles*, Wiley, New York, 1988. ⟨358, 360, 361⟩
[1432] V. I. Levenshtein, *The application of Hadamard matrices to a problem in coding*, Problemy Kibernet. 5 (1961) 123–136. ⟨698⟩
[1433] ——, *Binary codes capable of correcting deletions, insertions, and reversals*, Soviet Physics Dokl. 10 (1965) 707–710. ⟨386, 387⟩
[1434] ——, *Asymptotically optimum binary code with correction of losses of one and or two adjacent bits*, Problemy Cybern. 19 (1967) 293–298. (Russian). ⟨387⟩
[1435] ——, *Elements of coding theory*, in Discrete Mathematics and Math. Problems of Cybernetics, Nauka, Moscow, 1974, 207–305. ⟨386⟩
[1436] ——, *Perfect deletion-correcting codes as combinatorial designs*, in Second International Workshop Algebraic and Combinatorial Coding Theory, Leningrad, 1990, 137–140. ⟨388⟩
[1437] ——, *On perfect codes in deletion and insertion metric*, Discrete Math. Appl. 2 (1992) 241–258. ⟨387, 388, 442⟩
[1438] ——, *Universal bounds for codes and designs*, in Handbook of Coding Theory, Vol. I, V. S. Pless, W. C. Huffman, and R. A. Brualdi, eds., North-Holland, Amsterdam, 1998, 499–648. ⟨622⟩
[1439] ——, *Equivalence of Delsarte's bounds for codes and designs in symmetric association schemes, and some applications*, Discrete Math. 197/198 (1999) 515–536. ⟨110⟩
[1440] ——, *Efficient reconstruction of sequences from their subsequences or supersequences*, J. Combin. Theory A 93 (2001) 310–332. ⟨386⟩
[1441] ——, *Bounds for deletion/insertion correcting codes*, in Proc. 2002 IEEE International Symp Information Theory, IEEE, 2002. ⟨387⟩
[1442] F. W. Levi, *Finite Geometrical Systems*, University of Calcutta, Calcutta, 1942. ⟨14⟩
[1443] S. M. Lewis, *Composite generalised cyclic row-column designs*, Sankhyā B 48 (1986) 373–379. ⟨454⟩
[1444] P. C. Li, *Combining genetic algorithms and simulated annealing for constructing lotto designs*, J. Combin. Math. Combin. Comput. 45 (2003) 109–121. ⟨773, 774⟩
[1445] P. C. Li and G. H. J. Van Rees, *Lotto design tables*, J. Combin. Des. 10 (2002) 335–359. ⟨514⟩
[1446] W. Li and C. J. Nachtsheim, *Model-robust factorial designs*, Technometrics 42 (2000) 345–352. ⟨454⟩
[1447] Y. S. Liaw, *More $\mathbb{Z}$-cyclic Room squares*, Ars Combin. 52 (1999) 228–238. ⟨585, 625⟩
[1448] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 2nd ed., 1997. ⟨569, 572, 574, 657⟩
[1449] M. W. Liebeck, *The classification of finite linear spaces with flag transitive automorphism groups of affine type*, J. Combin. Theory A 84 (1998) 196–235. ⟨341⟩
[1450] M. W. Liebeck, C. E. Praeger, and J. Saxl, *On the O'Nan–Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. A 44 (1988) 389–396. ⟨825⟩

[1451] C. Lin and T. W. Shyu, *A necessary and sufficient condition for the star decomposition of complete graphs*, J. Graph Theory 23 (1996) 361–364. ⟨479⟩
[1452] D. K. J. Lin and N. R. Draper, *Projection properties of Plackett and Burman designs*, Technometrics 34 (1992) 423–428. ⟨454⟩
[1453] C. C. Lindner, *A note on disjoint Steiner quadruple systems*, Ars Combin. 3 (1977) 271–276. ⟨84⟩
[1454] ———, *A survey of embedding theorems for Steiner systems*, Ann. Discrete Math. 7 (1980) 175–202. ⟨159⟩
[1455] ———, *Quasigroup identities and orthogonal arrays*, in Surveys in Combinatorics, 1983, E. K. Lloyd, ed., Cambridge Univ. Press, London, 1983, 77–105. ⟨153, 155, 157, 158⟩
[1456] ———, *Embedding theorems for partial latin squares*, in [685], 1991, 217–265. ⟨159⟩
[1457] ———, *Il primo amore non si scorda mai or an up-to-date survey of small embeddings for partial even-cycle systems*, J. Geom. 76 (2003) 183–199. ⟨380⟩
[1458] C. C. Lindner, R. C. Mullin, and D. R. Stinson, *On the spectrum of resolvable orthogonal arrays invariant under the Klein group K_4*, Aequat. Math. 26 (1983) 176–183. ⟨216⟩
[1459] C. C. Lindner, R. C. Mullin, and G. H. J. Van Rees, *Separable orthogonal arrays*, Utilitas Math. 31 (1987) 25–32. ⟨545⟩
[1460] C. C. Lindner and C. A. Rodger, *Decomposition into cycles. II. Cycle systems*, in [724], 1992, 325–369. ⟨159, 374, 378, 379⟩
[1461] ———, *Embedding directed and undirected partial cycle systems of index $\lambda > 1$*, J. Combin. Des. 1 (1993) 113–123. ⟨380⟩
[1462] C. C. Lindner and A. Rosa, *Construction of large sets of almost disjoint Steiner triple systems*, Canad. J. Math. 27 (1975) 256–260. ⟨65⟩
[1463] ———, *On the existence of automorphism free Steiner triple systems*, J. Algebra 34 (1975) 430–443. ⟨38, 39, 40, 41, 42, 44, 46, 47, 48, 49, 51, 54⟩
[1464] ———, *Steiner triple systems having a prescribed number of triples in common*, Canad. J. Math. 27 (1975) 1166–1175. ⟨65⟩
[1465] C. C. Lindner and D. R. Stinson, *Steiner pentagon systems*, Discrete Math. 52 (1984) 67–74. ⟨155⟩
[1466] V. Linek and Z. Jiang, *Extended Langford sequences with small defects*, J. Combin. Theory A 84 (1998) 38–54. ⟨613⟩
[1467] V. Linek and S. Mor, *On partitions of $\{1, ..., 2m+1\}\setminus\{k\}$ into differences $d, ..., d+m-1$: Extended Langford sequences of large defect*, J. Combin. Des. 12 (2004) 421–442. ⟨613⟩
[1468] A. C. H. Ling, *Pairwise Balanced Designs and Related Codes*, PhD thesis, University of Waterloo, 1997. ⟨233⟩
[1469] ———, *Difference triangle sets from affine planes*, IEEE Trans. Inform. Theory 48 (2002) 2399–2401. ⟨439, 440⟩
[1470] A. C. H. Ling and C. J. Colbourn, *Concerning the generating set of $\mathbb{Z}_{\geq n}$*, Congr. Numer. 114 (1996) 65–72. ⟨254⟩
[1471] ———, *Pairwise balanced designs with block sizes* 8, 9 *and* 10, J. Combin. Theory A 77 (1997) 228–245. ⟨252⟩
[1472] A. C. H. Ling, C. J. Colbourn, M. J. Grannell, and T. S. Griggs, *Construction techniques for anti-Pasch Steiner triple systems*, J. London Math. Soc. (2) 61 (2000) 641–657. ⟨68⟩
[1473] A. C. H. Ling, X. J. Zhu, C. J. Colbourn, and R. C. Mullin, *Pairwise balanced designs with consecutive block sizes*, Des. Codes Crypt. 10 (1997) 203–222. ⟨251, 252⟩
[1474] J. Liu and D. R. Lick, *On λ-fold equipartite Oberwolfach problem with uniform table sizes*, Ann. Comb. 7 (2003) 315–323. ⟨375, 376⟩
[1475] W. Liu, *Suzuki groups and automorphisms of finite linear spaces*, Discrete Math. 269 (2003) 181–190. ⟨342⟩
[1476] W. Liu, S. Zhou, H. Li, and X. Fang, *Finite linear spaces admitting a Ree simple group*, Europ. J. Combin. 25 (2004) 311–325. ⟨342⟩

[1477] Y. Liu and A. Dean, *k-circulant supersaturated designs*, Technometrics 46 (2004) 32–43. ⟨453⟩
[1478] Z. Liu and H. Shen, *Embeddings of almost resolvable triple systems*, Discrete Math. 261 (2003) 383–398. ⟨381⟩
[1479] D. Livingstone and A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Zeitschr. 90 (1965) 393–403. ⟨821⟩
[1480] J. Q. Longyear, *A survey of nested designs*, J. Stat. Plann. Infer. 5 (1981) 181–187. ⟨537⟩
[1481] A. V. López and M. A. García Sánchez, *On the existence of abelian difference sets with* $100 < k \leq 150$, J. Combin. Math. Combin. Comput. 23 (1997) 97–112. ⟨435⟩
[1482] J. X. Lu, *On large sets of disjoint Steiner triple systems I, II, and III*, J. Combin. Theory A 34 (1983) 140–182. ⟨13, 65, 98, 99⟩
[1483] ——, *On large sets of disjoint Steiner triple systems IV, V, and VI*, J. Combin. Theory A 37 (1984) 136–192. ⟨13, 65, 99⟩
[1484] ——, *Collected Works on Combinatorial Designs*, Inner Mongolia People's Press, Hunhot, Mongolia, 1990. ⟨13, 67⟩
[1485] Y. Lu and L. Zhu, *On the existence of triplewhist tournaments TWh(v)*, J. Combin. Des. 5 (1997) 249–256. ⟨666⟩
[1486] M. G. Luby, *A simple parallel algorithm for the maximal independent set problem*, SIAM J. Comput. 15 (1986) 1036–1053. ⟨390⟩
[1487] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, *Analysis of low density codes and improved designs using irregular graphs*, IEEE Trans. Inform. Theory 47 (2001) 585–598. ⟨521, 522, 523⟩
[1488] E. Lucas, *Récréations mathématiques, Vol. 2*, Gauthier-Villars, Paris, 1883. ⟨15⟩
[1489] H. Lüneburg, *Translation Planes*, Springer, Berlin, 1980. ⟨729⟩
[1490] C. X. Ma, K. T. Fang, and J. K. Lin, *On the isomorphism of fractional factorial designs*, J. Complexity 17 (2001) 86–97. ⟨449⟩
[1491] S. Ma and Y. X. Chang, *Constructions of optimal optical orthogonal codes with weight five*, J. Combin. Des. 13 (2005) 54–69. ⟨322, 556, 628⟩
[1492] S. L. Ma and B. Schmidt, *Difference sets corresponding to a class of symmetric designs*, Des. Codes Crypt. 10 (1997) 223–236. ⟨424, 435⟩
[1493] A. Macfarlane, *Lectures on Ten British Mathematicians of the Nineteenth Century*, Wiley, New York, 1916. ⟨22⟩
[1494] D. MacKay, *Good error-correcting codes based on very sparse matrices*, IEEE Trans. Inform. Theory 45 (1999) 399–431. ⟨520⟩
[1495] C. Mackenzie and J. R. Seberry, *Maximal q-ary codes and Plotkin's bound*, Ars Combin. 26B (1988) 37–50. ⟨698⟩
[1496] K. Mackenzie-Fleming, *A recursive construction for* 2*-designs*, Des. Codes Crypt. 13 (1998) 159–164. ⟨39⟩
[1497] K. Mackenzie-Fleming and K. W. Smith, *An infinite family of non-embeddable quasi-residual designs*, J. Stat. Plann. Infer. 73 (1998) 77–83. ⟨46⟩
[1498] P. A. MacMahon, *Combinatory Analysis*, Cambridge Univ. Press, Cambridge, 1915. ⟨15⟩
[1499] H. F. MacNeish, *Euler squares*, Ann. Math. (NY) 23 (1922) 221–227. ⟨12, 16, 162⟩
[1500] A. J. Macula, *A simple construction of d-disjunct matrices with certain constant weights*, Discrete Math. 162 (1996) 311–312. ⟨575⟩
[1501] ——, *Error-correcting nonadaptive group testing with* d^e*-disjunct matrices*, Discrete Appl. Math. 80 (1997) 217–222. ⟨575⟩
[1502] F. J. MacWilliams, *An historical survey*, in Error Correcting Codes, H. B. Mann, ed., Wiley, 1968, 3–13. ⟨19⟩
[1503] F. J. MacWilliams and H. B. Mann, *On the p-rank of the design matrix of a difference set*, Inf. Control 12 (1968) 474–488. ⟨686⟩
[1504] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, *Self-dual codes over* GF(4), J. Combin. Theory A 25 (1978) 288–318. ⟨87, 90, 683⟩

[1505] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977. ⟨225, 329, 330, 680, 684, 685, 701⟩
[1506] B. M. Maenhaut and I. M. Wanless, *Atomic latin squares of order eleven*, J. Combin. Des. 12 (2004) 12–34. ⟨143, 146⟩
[1507] B. M. Maenhaut, I. M. Wanless, and B. S. Webb, *Subsquare-free latin squares of odd order*, Europ. J. Combin. (to appear). ⟨145, 150⟩
[1508] S. S. Magliveras and D. W. Leavitt, *Simple* 6-$(33, 8, 36)$ *designs from* $\mathrm{P\Gamma L}_2(32)$, in Computational Group Theory, M. D. Atkinson, ed., Academic Press, London, 1984, 337–352. ⟨94, 97, 766⟩
[1509] S. S. Magliveras and T. E. Plambeck, *New infinite families of simple* 5*-designs*, J. Combin. Theory A 44 (1987) 105. ⟨81, 82⟩
[1510] M. Maheo, *Strongly graceful graphs*, Discrete Math. 29 (1980) 39–46. ⟨480⟩
[1511] A. Mahmoodi, *Equidistant Permutation Arrays*, M.Sc. thesis, University of Toronto, 1991. ⟨570⟩
[1512] ———, *Combinatorial and Algorithmic Aspects of Directed Designs*, PhD thesis, University of Toronto, 1996. ⟨443⟩
[1513] A. Mahmoodi and R. A. Mathon, *Enumeration and analysis of small equidistant permutation arrays*, Congr. Numer. 87 (1992) 5–25. ⟨570⟩
[1514] E. S. Mahmoodian and N. Soltankhah, *Intersections of directed quadruple systems*, Utilitas Math. 47 (1995) 161–165. ⟨444⟩
[1515] ———, *Intersections of* 2-$(v, 4, 1)$ *directed designs*, J. Combin. Math. Combin. Comput. 20 (1996) 225–236. ⟨444⟩
[1516] J. M. Mahoney and J. E. Angus, *Estimability and efficiency in nearly orthogonal* $2^{m_1} \times 3^{m_2}$ *deletion designs*, Statist. Sinica 3 (1993) 197–207. ⟨465⟩
[1517] C. L. Mallows and N. J. A. Sloane, *Two-graphs, switching classes and Euler graphs are equal in number*, SIAM J. Appl. Math. 28 (1975) 876–880. ⟨876⟩
[1518] Y. I. Manin, *Cubic Forms*, North-Holland, Amsterdam, 1974. ⟨499⟩
[1519] A. Mann and N. D. Tuan, *Block-transitive point-imprimitive t-designs*, Geom. Ded. 88 (2001) 81–90. ⟨343⟩
[1520] H. B. Mann, *The construction of orthogonal latin squares*, Ann. Math. Stat. 13 (1942) 418–423. ⟨12⟩
[1521] B. Manvel, A. Meyerowitz, A. Schwenk, K. Smith, and P. Stockmeyer, *Reconstruction of sequences*, Discrete Math. 94 (1991) 209–219. ⟨386⟩
[1522] F. Margot, *Small covering designs by branch-and-cut*, Math. Program. 94B (2003) 207–220. ⟨759⟩
[1523] R. J. Martin and J. A. Eccleston, *Optimal incomplete block designs for general dependence structures*, J. Stat. Plann. Infer. 28 (1991) 67–81. ⟨542⟩
[1524] W. J. Martin, *Design systems: Combinatorial characterizations of Delsarte t-designs via partially ordered sets*, in Codes and Association Schemes, A. Barg and S. Litsyn, eds., Amer. Math. Soc., Providence RI, 2001, 223–239. ⟨330⟩
[1525] W. J. Martin and B. E. Sagan, *A new notion of transitivity for groups and sets of permutations*, J. London Math. Soc. 73 (2005) 1–13. ⟨547⟩
[1526] W. J. Martin and D. R. Stinson, *Association schemes for ordered orthogonal arrays and* (T, M, S)*-nets*, Canad. J. Math. 51 (1999) 326–346. ⟨643⟩
[1527] J. Martinet, ed., *Réseaux Euclidiens, Designs Sphériques et Formes Modulaires*, L'Enseignement Mathématique, Geneva, 2001. ⟨618, 622⟩
[1528] V. Martinetti, *Sulle configurazioni piane* μ_3, Ann. Mat. Pura Appl. 15 (1887) 1–26. ⟨14⟩
[1529] L. Martínez, D. Ž. Đoković, and A. Vera-López, *Existence question for difference families and construction of some new families*, J. Combin. Des. 12 (2004) 256–270. ⟨774⟩
[1530] S. S. Martirosyan and C. J. Colbourn, *Recursive constructions for covering arrays*, Bayreuth. Math. Schr. 74 (2005) 266–275. ⟨362, 365⟩
[1531] S. S. Martirosyan and Tran van Trung, *On t-covering arrays*, Des. Codes Crypt. 32 (2004) 323–339. ⟨362, 363, 365⟩

[1532] A. Maschietti, *Difference sets and hyperovals*, Des. Codes Crypt. 14 (1998) 89–98. ⟨423⟩
[1533] R. A. Mathon, *private communication.* ⟨36, 37⟩
[1534] ———, *Sample graphs for isomorphism testing*, Congr. Numer. 21 (1978) 499–517. ⟨777⟩
[1535] ———, *Symmetric conference matrices of order* $pq^2 + 1$, Canad. J. Math. 30 (1978) 321–331. ⟨855, 879⟩
[1536] ———, *A note on the graph isomorphism counting problem*, Inf. Process. Lett. 8 (1979) 131–132. ⟨757⟩
[1537] ———, *Constructions for cyclic Steiner 2-designs*, Ann. Discrete Math. 34 (1987) 353–362. ⟨51, 397, 400⟩
[1538] ———, *On self-complementary strongly regular graphs*, Discrete Math. 69 (1988) 263–281. ⟨882⟩
[1539] ———, *Computational methods in design theory*, in Surveys in Combinatorics, 1991, A. D. Keedwell, ed., Cambridge Univ. Press, Cambridge, 1991, 101–117. ⟨765⟩
[1540] ———, *Searching for spreads and packings*, in Geometry, Combinatorial Designs and Related Structures, J. W. P. Hirschfeld, S. S. Magliveras, and M. J. De Resmini, eds., Cambridge Univ. Press, Cambridge, 1997, 161–176. ⟨98⟩
[1541] ———, *A new family of partial geometries*, Geom. Ded. 73 (1998) 11–19. ⟨560⟩
[1542] ———, *New maximal arcs in Desarguesian planes*, J. Combin. Theory A 97 (2002) 353–368. ⟨559, 713⟩
[1543] R. A. Mathon and D. Lomas, *A census of* 2-$(9, 3, 3)$ *designs*, Australas. J. Combin. 5 (1992) 145–158. ⟨36⟩
[1544] R. A. Mathon, K. T. Phelps, and A. Rosa, *Small Steiner triple systems and their properties*, Ars Combin. 15 (1983) 3–110. Correction: 16 (1983), 286. ⟨36⟩
[1545] R. A. Mathon and C. Pietsch, *On the family of* 2-$(7, 3, \lambda)$ *designs.* unpublished. ⟨37, 38, 42, 46, 48, 51⟩
[1546] R. A. Mathon and A. Rosa, *Note on the number of certain Steiner 2-designs and their resolutions.* unpublished. ⟨37, 40, 47⟩
[1547] ———, *A census of Mendelsohn triple systems of order nine*, Ars Combin. 4 (1977) 309–315. ⟨36⟩
[1548] ———, *Some results on the existence and enumeration of BIBDs*, Tech. Report Math. 125-December-1985, McMaster University, Hamilton ON, 1985. ⟨36, 37, 38, 39, 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56⟩
[1549] ———, *On the* $(15, 5, \lambda)$*-family of BIBDs*, Discrete Math. 77 (1989) 205–216. ⟨40⟩
[1550] R. A. Mathon and G. F. Royle, *The translation planes of order* 49, Des. Codes Crypt. 5 (1995) 57–72. ⟨727⟩
[1551] R. A. Mathon and E. Spence, *On* 2-$(45, 12, 3)$ *designs*, J. Combin. Des. 4 (1996) 155–175. ⟨36⟩
[1552] R. A. Mathon and A. P. Street, *Overlarge sets and partial geometries*, J. Geom. 60 (1997) 85–104. ⟨560⟩
[1553] R. A. Mathon and Tran van Trung, *Unitals and unitary polarities in symmetric designs*, Des. Codes Crypt. 10 (1997) 237–250. ⟨113⟩
[1554] ———, *Directed t-packings and directed t-Steiner systems*, Des. Codes Crypt. 18 (1999) 187–198. ⟨388, 442, 444⟩
[1555] R. A. Mathon and S. A. Vanstone, *On the existence of doubly resolvable Kirkman systems and equidistant permutation arrays*, Discrete Math. 30 (1980) 157–172. ⟨570⟩
[1556] I. Matulić-Bedenić, K. Horvatić-Baldasar, and E. Kramer, *Construction of new symmetric designs with parameters* $(66, 26, 10)$, J. Combin. Des. 3 (1995) 405–410. ⟨43⟩
[1557] T. C. Maund, *Bases for Permutation Groups*, PhD thesis, Oxford University, 1989. ⟨851⟩
[1558] V. C. Mavron, T. P. McDonough, and G. L. Mullen, *The geometry of sets of orthogonal frequency hypercubes*, preprint. ⟨469, 470⟩

[1559] V. C. Mavron, T. P. McDonough, and C. A. Pallikaros, *A difference matrix construction and a class of balanced generalized weighing matrices*, Archiv der Mathematik 76 (2001) 259–264. ⟨414⟩
[1560] V. C. Mavron, T. P. McDonough, and V. D. Tonchev, *On affine designs and Hadamard designs with line spreads*, Discrete Math. (to appear). ⟨687⟩
[1561] D. McCarthy and S. A. Vanstone, *On the structure of regular pairwise balanced designs*, Discrete Math. 25 (1979) 237–244. ⟨583⟩
[1562] E. McClintock, *On the most perfect forms of magic squares, with methods for their production*, Amer. J. Math. 19 (1897) 99–120. ⟨524, 525⟩
[1563] T. P. McDonough, V. C. Mavron, and C. A. Pallikaros, *Generalised Hadamard matrices and translations*, J. Stat. Plann. Infer. 86 (2000) 527–533. ⟨306⟩
[1564] R. L. McFarland, *A family of difference sets in non-cyclic groups*, J. Combin. Theory A 15 (1973) 1–10. ⟨116⟩
[1565] ——, *Difference sets in abelian groups of order* $4p^2$, Mitt. Math. Semin. Giessen 192 (1989) 1–70. ⟨425⟩
[1566] R. B. McFeat and A. Neumaier, *Some tuple system constructions with applications to resolvable designs*, J. Combin. Theory A 36 (1984) 92–100. ⟨50⟩
[1567] G. McGuire, *Quasi-symmetric designs and codes meeting the Grey–Rankin bound*, J. Combin. Theory A 78 (1997) 280–291. ⟨576⟩
[1568] G. McGuire and H. N. Ward, *Characterization of certain minimal rank designs*, J. Combin. Theory A 83 (1998) 42–56. ⟨695⟩
[1569] B. D. McKay, `nauty` *user's guide (version 1.5)*, Tech. Report TR-CS-90-02, Computer Science Department, Australian National University, 1990. ⟨776, 777, 778, 779, 782⟩
[1570] ——, `autoson`—*A distributed batch system for Unix workstation networks (version 1.3)*, Tech. Report TR-CS-96-03, Computer Science Department, Australian National University, 1996. ⟨781⟩
[1571] ——, *Isomorph-free exhaustive generation*, J. Algorithms 26 (1998) 306–324. ⟨761, 781, 782⟩
[1572] B. D. McKay, J. C. McLeod, and I. M. Wanless, *The number of transversals in a latin square*, Des. Codes Crypt. 40 (2006) 269–284. ⟨143⟩
[1573] B. D. McKay, A. Meynert, and W. J. Myrvold, *Small latin squares, quasigroups and loops*, J. Combin. Des. (to appear). ⟨15, 136, 748⟩
[1574] B. D. McKay and S. P. Radziszowski, *The nonexistence of* 4-$(12, 6, 6)$ *designs*, in Computational and Constructive Design Theory, W. D. Wallis, ed., Kluwer, Dordrecht, 1996, 177–188. ⟨84, 762, 781⟩
[1575] B. D. McKay and E. Rogoyski, *Latin squares of order* 10, Electron. J. Comb. 2 (1995) N3. ⟨143⟩
[1576] B. D. McKay and G. F. Royle, *The transitive graphs with at most* 26 *vertices*, Ars Combin. 30 (1990) 161–176. ⟨736⟩
[1577] B. D. McKay and E. Spence, *The classification of regular two-graphs on* 36 *and* 38 *vertices*, Australas. J. Combin. 24 (2001) 293–300. ⟨855, 880, 882⟩
[1578] B. D. McKay and R. G. Stanton, *Isomorphism of two large designs*, Ars Combin. 6 (1978) 87–90. ⟨43⟩
[1579] B. D. McKay and I. M. Wanless, *On the number of latin squares*, Ann. Comb. 9 (2005) 335–344. ⟨142, 748, 767, 768⟩
[1580] I. McKinnon, *Bridge Directing Complete*, McKinnon, Sydney, 1979. ⟨600, 601, 606⟩
[1581] R. A. McLean and V. L. Anderson, *Applied Fractional Factorial Designs*, Dekker, New York, 1984. ⟨446, 455⟩
[1582] K. Meagher, *Covering Arrays on Graphs: Qualitative Independence Graphs and Extremal Set Partition Theory*, PhD thesis, University of Ottawa, Canada, 2005. ⟨365⟩
[1583] K. Meagher and B. Stevens, *Group construction of covering arrays*, J. Combin. Des. 13 (2005) 70–77. ⟨363, 365⟩
[1584] K. Mehlhorn, *Data Structures and Algorithms 1*, Springer, Berlin, 1984. ⟨566⟩

[1585] E. Mendelsohn and P. Rodney, *The existence of court balanced tournament designs*, Discrete Math. 133 (1994) 207–216. ⟨595⟩
[1586] N. S. Mendelsohn, *A natural generalization of Steiner triple systems*, in Computers in Number Theory, A. O. L. Atkin and B. J. Birch, eds., Academic Press, London, 1971, 323–338. ⟨19, 70, 531, 534⟩
[1587] ——, *Perfect cyclic designs*, Discrete Math. 20 (1977/78) 63–68. ⟨532⟩
[1588] N. S. Mendelsohn and S. H. Y. Hung, *On the Steiner systems $S(3, 4, 14)$ and $S(4, 5, 15)$*, Utilitas Math. 1 (1972) 5–95. ⟨17, 43, 85, 106⟩
[1589] J. Meng, *Some new orthogonal arrays of strength* 2, Master's thesis, Michigan Tech. Univ., Houghton MI, 1995. ⟨414⟩
[1590] G. Menichetti, *q-Archi completi nei piani di Hall di ordine $q = 2^k$*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 56 (1974) 518–525. ⟨728⟩
[1591] P. K. Menon, *On difference sets whose parameters satisfy a certain relation*, Proc. Amer. Math. Soc. 13 (1962) 739–745. ⟨116⟩
[1592] M. Meringer, *Fast generation of regular graphs and construction of cages*, J. Graph Theory 30 (1999) 137–146. ⟨735⟩
[1593] E. Merlin, *Configurations*, Encyc. des Sciences Math. 3.2 (1913) III.9, 144–160. ⟨14⟩
[1594] M. Meszka and A. Rosa, *Perfect 1-factorizations of K_{16} with nontrivial automorphism group*, J. Combin. Math. Combin. Comput. 47 (2003) 97–111. ⟨753⟩
[1595] N. Metropolis, A. W. Rosenbluth, M. N. Rosenbluth, A. H. Teller, and E. Teller, *Equation of state calculations by fast computing machines*, J. Chem. Phys. 21 (1953) 1087–1092. ⟨771⟩
[1596] K. Metsch, *Improvement of Bruck's completion theorem*, Des. Codes Crypt. 1 (1991) 99–116. ⟨163, 189⟩
[1597] ——, *Linear Spaces with Few Lines*, Springer, Berlin, 1991. ⟨270, 506, 507, 508, 512⟩
[1598] Y. Miao, *Some constructions and uses of double group divisible designs*, Bull. Inst. Combin. Appl. 10 (1994) 66–72. ⟨235⟩
[1599] Y. Miao and L. Zhu, *Pairwise balanced designs with block sizes $5t+1$*, Ars Combin. 32 (1991) 239–251. ⟨253⟩
[1600] ——, *On resolvable BIBDs with block size five*, Ars Combin. 39 (1995) 261–275. ⟨127⟩
[1601] ——, *Perfect Mendelsohn designs with block size six*, Discrete Math. 143 (1995) 189–207. ⟨531⟩
[1602] T. S. Michael, *The p-ranks of skew Hadamard designs*, J. Combin. Theory A 73 (1996) 170–171. ⟨788⟩
[1603] G. L. Miller, *On the $n^{\log n}$ isomorphism technique*, in Proc. Twelfth Annual ACM Symp. Theory of Computing, New York, 1980, ACM, 225–235. ⟨60⟩
[1604] J. Miller, *Langford's problem*. `http://www.lclark.edu/~miller/langford.html`, 2004. ⟨615, 616⟩
[1605] W. H. Mills, *private communication*. ⟨45⟩
[1606] ——, *A new block design*, Congr. Numer. 14 (1975) 461–465. ⟨40⟩
[1607] ——, *Two new block designs*, Utilitas Math. 7 (1975) 73–75. ⟨39, 42, 344⟩
[1608] ——, *Some mutually orthogonal latin squares*, Congr. Numer. 19 (1977) 473–487. ⟨170⟩
[1609] ——, *The construction of balanced incomplete block designs with $\lambda = 1$*, Congr. Numer. 20 (1978) 131–148. ⟨39, 41⟩
[1610] ——, *The construction of BIBDs using nonabelian groups*, Congr. Numer. 21 (1978) 519–526. ⟨44⟩
[1611] ——, *A new 5-design*, Ars Combin. 6 (1978) 193–195. ⟨107⟩
[1612] ——, *The construction of balanced incomplete block designs*, Congr. Numer. 23 (1979) 73–86. ⟨37⟩
[1613] ——, *On the existence of H designs*, Congr. Numer. 79 (1990) 129–141. ⟨660⟩
[1614] W. H. Mills and R. C. Mullin, *Coverings and packings*, in [724], 1992, 371–399. ⟨366, 373, 550, 556⟩

[1615] ———, *On λ-covers of pairs by quintuples: v odd*, J. Combin. Theory A 67 (1994) 245–272. ⟨246⟩
[1616] C. J. Mitchell, *An infinite family of symmetric designs*, Discrete Math. 26 (1979) 247–250. ⟨116⟩
[1617] C. J. Mitchell and F. C. Piper, *Key storage in secure networks*, Discrete Appl. Math. 21 (1988) 215–228. ⟨632⟩
[1618] J. T. Mitchell, *Duplicate Whist*, McClurg, Chicago, 1891. ⟨16⟩
[1619] N. Miyamoto, H. Mizuno, and S. Shinohara, *Optical orthogonal codes obtained from conics on finite projective planes*, Finite Fields Appl. 10 (2004) 405–411. ⟨322⟩
[1620] E. Modiano and P. Lin, *Traffic grooming in WDM networks*, IEEE Communications Magazine 39 (2001) 124–129. ⟨494⟩
[1621] H. Mohacsy and D. K. Ray-Chaudhuri, *A construction for infinite families of Steiner 3-designs*, J. Combin. Theory A 94 (2001) 127–141. ⟨82, 103⟩
[1622] M. Mohammad-Noori and B. Tayfeh-Rezaie, *Backtracking algorithm for finding t-designs*, J. Combin. Des. 11 (2003) 240–248. ⟨765⟩
[1623] D. C. Montgomery, *Design and Analysis of Experiments*, Wiley, New York, 6th ed., 2005. ⟨445, 446, 450, 454⟩
[1624] E. H. Moore, *Concerning triple systems*, Math. Ann. 43 (1893) 271–285. ⟨15⟩
[1625] ———, *The group of holoedric transformation into itself of a given group*, Bull. Amer. Math. Soc. 1 (1895) 61–66. ⟨15⟩
[1626] ———, *Tactical memoranda I–III*, Amer. J. Math. 18 (1896) 264–303. ⟨15, 16⟩
[1627] ———, *Concerning the general equations of the seventh and eighth degrees*, Math. Ann. 51 (1899) 417–444. ⟨15⟩
[1628] L. B. Morales, *Constructing difference families through an optimization approach: Six new BIBDs*, J. Combin. Des. 8 (2000) 261–273. ⟨39, 40, 41, 42, 46, 404, 774⟩
[1629] ———, *Two new 1-rotational* $(36, 9, 8)$ *and* $(40, 10, 9)$ *RBIBDs*, J. Combin. Math. Combin. Comput. 36 (2001) 119–126. ⟨50, 54⟩
[1630] ———, *Constructing some PBIBD(2)s by tabu search algorithm*, J. Combin. Math. Combin. Comput. 43 (2002) 65–82. ⟨565, 773, 774⟩
[1631] ———, *private communication*, 2006. ⟨127⟩
[1632] L. B. Morales and C. Velarde, *A complete classification of* $(12, 4, 3)$*-RBIBDs*, J. Combin. Des. 9 (2001) 385–400. ⟨36, 759⟩
[1633] ———, *Enumeration of resolvable* 2-$(10, 5, 16)$ *and* 3-$(10, 5, 6)$ *designs*, J. Combin. Des. 13 (2005) 108–119. ⟨51⟩
[1634] I. H. Morgan, *Properties of complete sets of mutually equiorthogonal frequency hypercubes*, Ann. Comb. 1 (1997) 377–389. ⟨470, 471⟩
[1635] ———, *Construction of complete sets of mutually orthogonal frequency hypercubes*, Discrete Math. 186 (1998) 237–251. ⟨470⟩
[1636] J. P. Morgan, *Nested designs*, in Design and Analysis of Experiments, S. Ghosh and C. R. Rao, eds., North-Holland, Amsterdam, 1996, 939–976. ⟨539, 540⟩
[1637] J. P. Morgan and R. A. Bailey, *Optimal design with many blocking factors*, Ann. Statist. 28 (2000) 553–577. ⟨540⟩
[1638] J. P. Morgan, D. A. Preece, and D. H. Rees, *Nested balanced incomplete block designs*, Discrete Math. 231 (2001) 351–389. ⟨535, 540⟩
[1639] J. P. Morgan and N. Uddin, *Some constructions for rectangular, latin square and pseudo-cyclic nested row-column designs*, Utilitas Math. 38 (1990) 43–51. ⟨565⟩
[1640] R. Moufang, *Zur Struktur von Alternativkörpern*, Math. Ann. 110 (1935) 416–430. ⟨18⟩
[1641] C. A. Mount-Campbell and J. B. Neuhardt, *On the number of* 2^{n-p} *fractional factorials of resolution III*, Commun. Stat. Theory Methods 10 (1981) 2101–2111. ⟨451⟩
[1642] R. Mukerjee and C. F. J. Wu, *Minimum aberration designs for mixed factorials in terms of complementary sets*, Statist. Sinica 11 (2001) 225–239. ⟨453⟩

[1643] A. C. Mukhopadhyay, *Construction of some series of orthogonal arrays*, Sankhyā B43 (1981) 81–92. ⟨220, 227⟩

[1644] P. Mulder, *Kirkman-systemen.* Academisch Proefschrift ter verkrijging van den graad van doctor in de Wis-en Natuurkunde aan de Rijksuniversiteit te Groningen, Leiden, 1917. ⟨13⟩

[1645] G. L. Mullen, *Polynomial representation of complete sets of mutually orthogonal frequency squares of prime power order*, Discrete Math. 69 (1988) 79–84. ⟨466, 469⟩

[1646] ———, *Permutation polynomials over finite fields*, in Finite Fields, Coding Theory with Advances in Communications and Computing, G. L. Mullen and P. J.-S. Shiue, eds., Dekker, New York, 1993, 131–151. ⟨574⟩

[1647] ———, *A candidate for the next Fermat problem*, Math. Intelligencer 17 (1995) 18–22. ⟨193⟩

[1648] ———, *Permutation polynomials: A matrix analogue of Schur's conjecture and a survey of recent results*, Finite Fields Appl. 1 (1995) 242–258. ⟨574⟩

[1649] G. L. Mullen and W. C. Schmid, *An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes*, J. Combin. Theory A 76 (1996) 164–174. ⟨643⟩

[1650] R. C. Mullin, *On a PBD generating set problem of Rosa*, Ars Combin. 27 (1989) 75–84. ⟨254⟩

[1651] R. C. Mullin, B. Gardner, K. Metsch, and G. H. J. Van Rees, *Some properties of finite bases for the Rosa set*, Utilitas Math. 38 (1990) 299–215. ⟨254⟩

[1652] R. C. Mullin, A. C. H. Ling, R. J. R. Abel, and F. E. Bennett, *On the closure of subsets of $\{4, 5, \ldots, 9\}$ which contain* 4, Ars Combin. 45 (1997) 33–76. ⟨250, 251⟩

[1653] R. C. Mullin and E. Nemeth, *On furnishing Room squares*, J. Combin. Theory 7 (1969) 266–272. ⟨13⟩

[1654] R. C. Mullin, P. J. Schellenberg, G. H. J. Van Rees, and S. A. Vanstone, *On the construction of perpendicular arrays*, Utilitas Math. 18 (1980) 141–160. ⟨545⟩

[1655] R. C. Mullin and R. G. Stanton, *Group matrices and balanced weighing designs*, Utilitas Math. 8 (1975) 277–301. ⟨309, 313⟩

[1656] R. C. Mullin and W. D. Wallis, *The existence of Room squares*, Aequat. Math. 13 (1975) 1–7. ⟨20⟩

[1657] R. C. Mullin and J. X. Yin, *On packings of pairs by quintuples: $v \equiv 3, 9$ or* 17 (mod 20), Ars Combin. 35 (1993) 161–171. ⟨551⟩

[1658] A. Munemasa, *Flag-transitive 2-designs arising from line-spreads in $PG(2n-1, 2)$*, Geom. Ded. 77 (1999) 209–213. ⟨341⟩

[1659] A. Munemasa and V. D. Tonchev, *A new quasi-symmetric 2-$(56, 16, 6)$ design obtained from codes*, Discrete Math. 284 (2004) 231–234. ⟨580, 689⟩

[1660] M. Muzychuk and Q. Xiang, *Symmetric Bush-type Hadamard matrices of order $4m^4$ exist for all odd m*, Proc. Amer. Math. Soc. 134 (2006) 2197–2204. ⟨277, 280⟩

[1661] R. H. Myers and D. C. Montgomery, *Response Surface Methodology: Process and Product Optimization Using Designed Experiments*, Wiley, New York, 2nd ed., 2002. ⟨448⟩

[1662] G. P. Nagy, *Algebraic Commutative Moufang Loops*, PhD thesis, Universität Erlangen-Nürnberg, 2000. ⟨850⟩

[1663] K. R. Nair, *Certain inequality relationships among the combinatorial parameters of incomplete block designs*, Sankhyā 6 (1943) 255–259. ⟨790⟩

[1664] H. K. Nandi, *On the relation between certain types of tactical configurations*, Bull. Calcutta Math. Soc. 37 (1945) 92–94. ⟨19⟩

[1665] ———, *Enumeration of non-isomorphic solutions of balanced incomplete block designs*, Sankhyā 7 (1946) 305–312. ⟨36⟩

[1666] M. Naor and A. Shamir, *Visual cryptography*, Lect. Notes Comp. Sci. 950 (1995) 1–12. ⟨639⟩

[1667] V. Napolitano, *On some finite linear spaces with few lines*, Australas. J. Combin. 31 (2005) 145–160. ⟨508⟩

[1668] C. St. J. A. Nash-Williams, *Problem*, in Combinatorial Theory and Its Applications, III, North-Holland, Amsterdam, 1970, 1153–1195. ⟨64⟩
[1669] A. V. Nazarok, *Five pairwise orthogonal latin squares of order* 21, Issled. oper. i ASU (1991) 54–56. ⟨165⟩
[1670] E. Netto, *Zur Theorie der Tripelsysteme*, Math. Ann. 42 (1893) 143–152. ⟨15, 59⟩
[1671] ———, *Lehrbuch der Combinatorik*, Teubner, Leipzig, 1927. 2nd ed. (with notes by V. Brun and Th. Skolem). ⟨16⟩
[1672] A. Neumaier, *New inequalities for the parameters of an association scheme*, Lect. Notes Math. 885 (1981) 365–367. ⟨855⟩
[1673] ———, *Completely regular two-graphs*, Arch. Math. 38 (1982) 378–384. ⟨881⟩
[1674] ———, *Regular sets and quasi-symmetric* 2*-designs*, in Combinatorial Theory, D. Jungnickel and K. Vedder, eds., Springer, Berlin, 1982, 258–275. ⟨580, 853⟩
[1675] N. K. Nguyen and A. J. Miller, *A review of some exchange algorithms for constructing discrete D-optimal designs*, Comput. Stat. Data Anal. 14 (1992) 489–498. ⟨542⟩
[1676] W. Nickel, A. C. Niemeyer, C. O'Keefe, T. Penttila, and C. E. Praeger, *The block-transitive, point-imprimitive* 2*-*$(729, 8, 1)$ *designs*, Appl. Algebra Engrg. Comm. Comput. 3 (1992) 47–61. ⟨344⟩
[1677] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987) 273–337. ⟨639, 640, 641⟩
[1678] ———, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, PA, 1992. ⟨639, 640⟩
[1679] ———, *High-dimensional numerical integration*, in Applied Mathematics Entering the 21st Century, J. M. Hill and R. Moore, eds., SIAM, Philadelphia, 2004, 337–351. ⟨643⟩
[1680] ———, *Constructions of* (t, m, s)*-nets and* (t, s)*-sequences*, Finite Fields Appl. 11 (2005) 578–600. ⟨641, 643⟩
[1681] A. Niemeyer, W. Nickel, et al., *Computational group theory system GAP*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany (1993). ⟨820⟩
[1682] S. Niskanen and P. R. J. Östergård, *Cliquer user's guide, version 1.0*, Tech. Report T48, Communications Laboratory, Helsinki University of Technology, 2003. ⟨776, 779⟩
[1683] R. Noda, *On orthogonal arrays of strength* 3 *and* 5 *achieving Rao's bound*, Graphs Combin. 2 (1986) 277–282. ⟨226⟩
[1684] ———, *Some inequalities for Steiner systems*, Europ. J. Combin. 19 (1998) 375–376. ⟨102⟩
[1685] G. Nordh, *Generalizations of Skolem sequences*, Master's thesis, Department of Mathematics, Linköpings Universitat, Sweden, 2003. ⟨613⟩
[1686] H. W. Norton, *The* 7×7 *squares*, Ann. Eugenics 9 (1939) 269–307. ⟨18⟩
[1687] J. Novák, *A note on disjoint cyclic Steiner triple systems*, in Recent Advances in Graph Theory, Academia, Prague, 1975, 439–440. ⟨70⟩
[1688] K. J. Nurmela, *Upper bounds for covering arrays by tabu search*, Discrete Appl. Math. 138 (2004) 143–152. ⟨363, 365⟩
[1689] K. J. Nurmela, M. K. Kaikkonen, and P. R. J. Östergård, *New constant weight codes from linear permutation groups*, IEEE Trans. Inform. Theory 43 (1997) 1623–1630. ⟨774⟩
[1690] K. J. Nurmela and P. R. J. Östergård, *Upper bounds for covering designs by simulated annealing*, Congr. Numer. 96 (1993) 93–111. ⟨773⟩
[1691] ———, *New coverings of* t*-sets with* $(t + 1)$*-sets*, J. Combin. Des. 7 (1999) 217–226. ⟨774⟩
[1692] W. Oberschelp, *Lotto-Garantiesysteme und Block-Pläne*, Mathematisch-Phys. Semesterberichte XIX (1972) 55–67. ⟨84⟩
[1693] H. Ohmori, *Classification of weighing matrices of order* 13 *and weight* 9, Discrete Math. 116 (1993) 55–78. ⟨288⟩
[1694] C. M. O'Keefe, A. A. Pascasio, and T. Penttila, *Hyperovals in Hall planes*, Europ. J. Combin. 13 (1992) 195–199. ⟨728⟩

[1695] E. S. O'Keefe, *Verification of a conjecture of Th. Skolem*, Math. Scand. 9 (1961) 80–82. ⟨16⟩

[1696] K. Ollerenshaw and H. Bondi, *Magic squares of order four*, Philos. Trans. Roy. Soc. London A 306 (1982) 443–532. ⟨528⟩

[1697] M. A. Ollis, *Sequenceable groups and related topics*, Electron. J. Comb. DS#10. ⟨352⟩

[1698] C. L. Olsen and D. L. Kreher, *Steiner graphical t-wise balanced designs of type* n^r, J. Stat. Plann. Infer. 86 (2000) 535–566. ⟨492, 493⟩

[1699] R. Omrani, O. Moreno, and P. V. Kumar, *Improved Johnson bounds for optical orthogonal codes with* $\lambda > 1$ *and some optimal constructions*, in Proc. International Symp. Information Theory, IEEE, 2005, 259–263. ⟨322⟩

[1700] M. E. O'Nan, *Sharply 2-transitive sets of permutations*, in Proceedings of the Rutgers Group Theory Year, M. Aschbacher, D. Gorenstein, R. Lyons, M. E. O'Nan, C. C. Sims, and W. Feit, eds., Cambridge Univ. Press, Cambridge, 1985, 63–67. ⟨544⟩

[1701] O. Ore and B. A. Hausmann, *Theory of quasi-groups*, Amer. J. Math. 59 (1937) 983–1004. ⟨18⟩

[1702] W. P. Orrick, *The maximal* $\{-1, 1\}$*-determinant of order* 15, Metrika 62 (2005) 195–219. ⟨297⟩

[1703] P. R. J. Östergård, *Constructing covering codes by tabu search*, J. Combin. Des. 5 (1997) 71–80. ⟨774⟩

[1704] ———, *Enumeration of* 2-$(12, 3, 2)$ *designs*, Australas. J. Combin. 22 (2000) 227–231. ⟨36⟩

[1705] ———, *There are* $270,474,142$ *nonisomorphic* 2-$(9, 4, 6)$ *designs*, J. Combin. Math. Combin. Comput. 37 (2001) 173–176. ⟨38⟩

[1706] ———, *Constructing combinatorial objects via cliques*, in Surveys in Combinatorics, 2005, B. S. Webb, ed., Cambridge Univ. Press, Cambridge, 2005, 57–82. ⟨779⟩

[1707] P. R. J. Östergård and P. Kaski, *Enumeration of* 2-$(9, 3, \lambda)$ *designs and their resolutions*, Des. Codes Crypt. 27 (2002) 131–137. ⟨36, 38, 39, 51⟩

[1708] P. R. J. Östergård and O. Pottonen, *Classification of directed and hybrid triple systems*, Bayreuth. Math. Schr. 74 (2005) 276–291. ⟨444⟩

[1709] O. P. Osuna, *There are* 1239 *triple systems STS*(31) *of* 2*-rank* 27, Des. Codes Crypt. 40 (2006) 187–190. ⟨692⟩

[1710] P. J. Owens and D. A. Preece, *Complete sets of pairwise orthogonal latin squares of order* 9, J. Combin. Math. Combin. Comput. 18 (1995) 83–96. ⟨171⟩

[1711] J. G. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992. ⟨848, 852⟩

[1712] J. Ozanam, *Récréations Mathématiques et Physiques, qui contiennent Plusieurs Problémes utiles & agréables, d'Arithmetique, de Geometrie, d'Optique, de Gnomonique, de Cosmographie, de Mécanique, de Pyrotechnie, & de Physique. Avec un Traité nouveau des Horloges Elementaires. 4 vols.*, Jombert, Paris, 1723. Updated edition with commentary by Grandin of first edition from 1694. ⟨11⟩

[1713] R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys. 12 (1933) 311–320. ⟨14, 879⟩

[1714] S. C. Panandikar, *On a family of resolvable BIB designs*, Calcutta Statist. Assoc. Bull. 30 (1981) 123–128. ⟨47, 53⟩

[1715] C. Parker, E. Spence, and V. D. Tonchev, *Designs with the symmetric difference property on* 64 *points and their groups*, J. Combin. Theory A 67 (1994) 23–43. ⟨696⟩

[1716] E. T. Parker, *Computer investigations of orthogonal latin squares of order* 10, Proc. Sympos. Appl. Math 15 (1963) 73–81. ⟨143⟩

[1717] E. T. Parker and A. M. Mood, *Some balanced Howell rotations for duplicate bridge sessions*, Amer. Math. Monthly 62 (1955) 714–716. ⟨600⟩

[1718] D. V. Pasechnik, *Skew-symmetric association schemes with two classes and strongly regular graphs of type* $L(2n - 1, 4n - 1)$, Acta Appl. Math. 29 (1992) 129–138. ⟨854⟩

[1719] A. J. L. Paulus, *Conference matrices and graphs of order* 26. Technische Hogeschool Eindhoven, report WSK 73/06, Eindhoven, 1983, 89 pp. ⟨855⟩
[1720] M.-O. Pavčević and E. Spence, *Some new symmetric designs with* $\lambda = 10$ *having an automorphism of order* 5, Discrete Math. 196 (1999) 257–266. ⟨43, 44⟩
[1721] S. E. Payne, *A new infinite family of generalized quadrangles*, Congr. Numer. 49 (1985) 115–128. ⟨474⟩
[1722] ——, *Flock generalized quadrangles and related structures: An update*, in Generalized Polygons, F. De Clerck, L. Storme, J. A. Thas, and H. Van Maldeghem, eds., Universa Press, 2001, 61–98. ⟨474, 475⟩
[1723] S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles*, Pitman, New York, 1985. ⟨476, 477, 561, 855⟩
[1724] R. A. Pease, *The Taguchi method*, Electron. Design 41 (1993) 85. ⟨465⟩
[1725] D. Pei, *Authentication Codes and Combinatorial Designs*, Chapman and Hall/CRC, Boca Raton FL, 2006. ⟨611⟩
[1726] B. Peirce, *Cyclic solutions of the school-girl puzzle*, Astronomical Journal (U.S.A.) 6 (1860) 169–174. ⟨13⟩
[1727] R. Peltesohn, *Eine Lösung der beiden Heffterschen Differenzenprobleme*, Compositio Math. 6 (1939) 251–257. ⟨16, 17⟩
[1728] T. Penttila and G. F. Royle, *Sets of type* (m, n) *in the affine and projective planes of order nine*, Des. Codes Crypt. 6 (1995) 229–245. ⟨727⟩
[1729] T. Penttila, G. F. Royle, and M. K. Simpson, *Hyperovals in the known projective planes of order* 16, J. Combin. Des. 4 (1996) 59–65. ⟨38, 727⟩
[1730] J. Petersen, *Sur le théorème de Tait*, L'Intermédiaire des Mathématiciens 5 (1898) 225–227. ⟨855⟩
[1731] ——, *Les* 36 *officiers*, Ann. des Math. (1901) 413–416. ⟨12⟩
[1732] C. Peterson, *Tight* 6*-designs*, Osaka J. Math. 14 (1977) 417–435. ⟨329⟩
[1733] W. W. Peterson and E. J. Weldon Jr., *Error-Correcting Codes*, M.I.T. Press, Cambridge MA, 2nd ed., 1972. ⟨701⟩
[1734] H. O. Pflugfelder, *Historical notes on loop theory*, Comment. Math. Univ. Carolin. 41 (2000) 359–370. ⟨22⟩
[1735] K. T. Phelps, *A combinatorial construction of perfect codes*, SIAM J. Alg. Disc. Meth. 4 (1983) 398–403. ⟨680⟩
[1736] ——, *A general product construction for error correcting codes*, SIAM J. Alg. Disc. Meth. 5 (1984) 224–228. ⟨680⟩
[1737] ——, *Isomorphism problems for cyclic block designs*, Ann. Discrete Math. 34 (1987) 385–391. ⟨61⟩
[1738] K. T. Phelps and V. Rödl, *On the algorithmic complexity of coloring simple hypergraphs and Steiner triple systems*, Combinatorica 4 (1984) 79–88. ⟨756⟩
[1739] ——, *Steiner triple systems with minimum independence number*, Ars Combin. 21 (1986) 167–172. ⟨69⟩
[1740] K. T. Phelps and A. Rosa, *Steiner triple systems with rotational automorphisms*, Discrete Math. 33 (1981) 57–66. ⟨406⟩
[1741] K. T. Phelps, A. Rosa, and E. Mendelsohn, *Cyclic Steiner triple systems with cyclic subsystems*, Europ. J. Combin. 10 (1989) 363–367. ⟨61⟩
[1742] N. C. K. Phillips and W. D. Wallis, *All solutions to a tournament problem*, Congr. Numer. 114 (1996) 193–196. ⟨603⟩
[1743] C. Pietsch, *Numbers of nonisomorphic block designs found with DESY*. unpublished. ⟨36, 37, 38, 40, 41, 44⟩
[1744] ——, *On the classification of linear spaces of order* 11, J. Combin. Des. 3 (1995) 185–193. ⟨269⟩
[1745] D. A. Pike and N. Shalaby, *Non-isomorphic perfect one-factorizations from Skolem sequences and starters*, J. Combin. Math. Combin. Comput. 44 (2003) 23–32. ⟨615, 624, 628, 753⟩
[1746] W. Piotrowski, *The solution of the bipartite analogue of the Oberwolfach problem*, Discrete Math. 97 (1991) 339–356. ⟨375⟩

[1747] R. L. Plackett, *Some generalizations in the multifactorial design*, Biometrika 33 (1946) 328–332. ⟨19⟩
[1748] R. L. Plackett and J. P. Burman, *The design of optimum multifactorial experiments*, Biometrika 33 (1946) 305–325. ⟨19⟩
[1749] V. S. Pless, *Symmetry codes over* GF(3) *and new five-designs*, J. Combin. Theory A 12 (1972) 119–142. ⟨682⟩
[1750] ———, *Introduction to the Theory of Error-Correcting Codes*, Wiley, New York, 3rd ed., 1998. ⟨682⟩
[1751] V. S. Pless and V. D. Tonchev, *Self-dual codes over* GF(7), IEEE Trans. Inform. Theory 33 (1987) 723–727. ⟨690⟩
[1752] V. S. Pless, V. D. Tonchev, and J. S. Leon, *On the existence of a certain* $(64, 32, 12)$ *extremal code*, IEEE Trans. Inform. Theory 39 (1993) 214–215. ⟨683⟩
[1753] M. Plotkin, *Binary codes with specified minimum distance*, IRE Trans. 6 (1960) 445–450. ⟨697⟩
[1754] J. Plücker, *System der analytischen Geometrie: Auf neue Betrachtungsweisen gegründet, und insbesondere eine ausführliche Theorie der Curven dritter Ordnung enthaltend*, Duncker and Humblot, Berlin, 1835. ⟨12⟩
[1755] ———, *Theorie der algebraischen Curven: Gegründet auf eine neue Behandlungsweise der analytischen Geometrie*, Marcus, Bonn, 1839. ⟨12⟩
[1756] S. Poljak and Z. Tuza, *On the maximum number of qualitatively independent partitions*, J. Combin. Theory A 51 (1989) 111–116. ⟨362⟩
[1757] C. E. Praeger, *Implications of line-transitivity for designs*, in Finite Geometries, A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas, eds., Kluwer, Dordrecht, 2001, 305–317. ⟨344⟩
[1758] C. E. Praeger and S. Zhou, *Imprimitive flag-transitive symmetric designs*, J. Combin. Theory A 113 (2006) 1381–1395. ⟨343⟩
[1759] D. A. Preece, *Fifty years of Youden squares: A review*, Bull. Inst. Math. Applic. 26 (1990) 65–75. ⟨674⟩
[1760] ———, *Double Youden rectangles of size* 6×11, Math. Scientist 16 (1991) 41–45. ⟨674⟩
[1761] ———, *Double Youden rectangles—An update with examples of size* 5×11, Discrete Math. 125 (1994) 309–317. ⟨674⟩
[1762] D. A. Preece, P. W. Brading, C. W. H. Lam, and M. Côté, *Balanced* 6×6 *designs for* 4 *equally replicated treatments*, Discrete Math. 125 (1994) 319–327. ⟨671⟩
[1763] D. A. Preece, S. C. Pearce, and J. R. Kerr, *Orthogonal designs for three-dimensional experiments*, Biometrika 60 (1973) 349–358. ⟨468⟩
[1764] D. A. Preece and N. C. K. Phillips, *A new type of Freeman–Youden rectangle*, J. Combin. Math. Combin. Comput. 25 (1997) 65–78. ⟨674⟩
[1765] D. A. Preece, D. H. Rees, and J. P. Morgan, *Doubly nested balanced incomplete block designs*, Congr. Numer. 137 (1999) 5–18. ⟨538⟩
[1766] G. Promhouse and S. E. Tavares, *The minimum distance of all binary cyclic codes of odd lengths from* 69 *to* 99, IEEE Trans. Inform. Theory 24 (1978) 438–442. ⟨701⟩
[1767] T. Prvan and D. J. Street, *An annotated bibliography of application papers using certain classes of fractional factorial and related designs*, J. Stat. Plann. Infer. 106 (2002) 245–269. ⟨445⟩
[1768] R. W. Quackenbush, *Near vector spaces over* GF(q) *and* $(v, q+1, 1)$*-BIBD's*, Lin. Alg. Appl. 10 (1975) 259–266. ⟨790⟩
[1769] S. P. Radziszowski and D. L. Kreher, *Solving subset sum problems with the* L^3 *algorithm*, J. Combin. Math. Combin. Comput. 3 (1988) 49–63. ⟨765⟩
[1770] D. Raghavarao, *Constructions and Combinatorial Problems in Design of Experiments*, Wiley, New York, 1971. ⟨224, 228, 298, 563, 564, 790⟩
[1771] M. Rahman and I. F. Blake, *Majority logic decoding using combinatorial designs*, IEEE Trans. Inform. Theory 21 (1975) 585–587. ⟨686⟩

[1772] E. M. Rains, N. J. A. Sloane, and J. Stufken, *The lattice of N-run orthogonal arrays*, J. Stat. Plann. Infer. 102 (2002) 477–500. ⟨227⟩
[1773] D. P. Rajkundlia, *Some techniques for constructing infinite families of BIBDs*, Discrete Math. 44 (1983) 61–96. ⟨43, 53, 116⟩
[1774] K. Ranto, *Infinite families of 3-designs from $\mathbb{Z}_4$-Goethals codes with block size 8*, SIAM J. Disc. Math. 15 (2002) 289–304. ⟨685⟩
[1775] C. R. Rao, *Hypercubes of strength 'd' leading to confounded designs in factorial experiments*, Bull. Calcutta Math. Soc. 38 (1946) 67–78. ⟨19⟩
[1776] ——, *Combinatorial arrangements analogous to orthogonal arrays*, Sankhyā A23 (1961) 283–286. ⟨545⟩
[1777] M. B. Rao, *Group divisible family of* PBIB *designs*, J. Indian Statist. Assoc. 4 (1966) 14–28. ⟨300⟩
[1778] ——, *Balanced orthogonal designs and their application in the construction of some BIB and group divisible designs*, Sankhyā A 32 (1970) 439–448. ⟨300⟩
[1779] D. K. Ray-Chaudhuri and E. J. Schram, *A large set of designs on vector spaces*, J. Number Theory 47 (1994) 247–272. ⟨850⟩
[1780] D. K. Ray-Chaudhuri and N. M. Singhi, *On existence and number of orthogonal arrays*, J. Combin. Theory A 47 (1988) 28–36. Correction: 66 (1994), 327–328. ⟨220⟩
[1781] D. K. Ray-Chaudhuri and R. M. Wilson, *Solution of Kirkman's schoolgirl problem*, Proc. Symp. Pure Math. Amer. Math. Soc. 19 (1971) 187–204. ⟨13, 67⟩
[1782] ——, *The existence of resolvable block designs*, in A Survey of Combinatorial Theory, J. N. Srivastava, ed., North-Holland, Amsterdam, 1973, 361–375. ⟨126, 132⟩
[1783] ——, *On t-designs*, Osaka J. Math. 12 (1975) 737–744. ⟨86, 102, 329, 789⟩
[1784] R. C. Read, *Every one a winner, or, how to avoid isomorphism search when cataloguing combinatorial configurations*, Ann. Discrete Math. 2 (1978) 107–120. ⟨761, 782⟩
[1785] R. C. Read and R. J. Wilson, *An Atlas of Graphs*, Oxford University Press, New York, 1998. ⟨740⟩
[1786] I. S. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, IRE Trans. Inform. Theory 4 (1954) 38–49. ⟨19⟩
[1787] R. S. Rees, *Uniformly resolvable pairwise balanced designs with block sizes two and three*, J. Combin. Theory A45 (1987) 207–225. ⟨131⟩
[1788] ——, *Two new direct product-type constructions for resolvable group-divisible designs*, J. Combin. Des. 1 (1993) 15–26. ⟨264, 265⟩
[1789] ——, *Mandatory representation designs* $\mathrm{MR}(3, k; v)$ *with k even and v odd*, J. Stat. Plann. Infer. (2000) 567–594. ⟨234⟩
[1790] ——, *Truncated transversal designs: A new lower bound on the number of idempotent MOLS of side n*, J. Combin. Theory A 90 (2000) 257–266. ⟨162⟩
[1791] R. S. Rees and N. Shalaby, *Simple and indecomposable twofold cyclic triple systems from Skolem sequences*, J. Combin. Des. 8 (2000) 402–410. ⟨616⟩
[1792] R. S. Rees and D. R. Stinson, *On combinatorial designs with subdesigns*, Discrete Math. 77 (1989) 259–279. ⟨67⟩
[1793] ——, *On the existence of incomplete designs of block size four having one hole*, Utilitas Math. 35 (1989) 119–152. ⟨233⟩
[1794] ——, *Frames with block size four*, Canad. J. Math. 44 (1992) 1030–1049. ⟨264⟩
[1795] ——, *Combinatorial characterizations of authentication codes. II*, Des. Codes Crypt. 7 (1996) 239–259. ⟨609, 611⟩
[1796] R. S. Rees and W. D. Wallis, *The spectrum of maximal sets of one-factors*, Discrete Math. 97 (1991) 357–369. ⟨754⟩
[1797] C. R. Reeves, ed., *Modern Heuristic Techniques for Combinatorial Problems*, Blackwell Scientific Publications, Oxford, 1993. ⟨772⟩
[1798] K. B. Reid and L. W. Beineke, *Tournaments*, in Selected Topics in Graph Theory, L. W. Beineke and R. J. Wilson, eds., Academic Press, London, 1978, 169–204. ⟨606⟩

[1799] M. Reiss, *Ueber eine Steinersche combinatorische Aufgabe, welche im 45sten Bande dieses Journals, seite 181, gestellt worden ist*, J. Reine Angew. Math. 56 (1859) 326–344. ⟨12⟩
[1800] T. Reye, *Geometrie der Lage I, 2nd ed.*, Rümpler, Hannover, 1876. ⟨14⟩
[1801] T. Richardson and R. Urbanke, *The capacity of low density parity check codes under message-passing decoding*, IEEE Trans. Inform. Theory 47 (2001) 599–618. ⟨522⟩
[1802] ———, *Efficient encoding of low-density parity-check codes*, IEEE Trans. Inform. Theory 47 (2001) 638–656. ⟨520⟩
[1803] ———, *Modern Coding Theory*, Cambridge Univ. Press, Cambridge, to appear. ⟨522, 523⟩
[1804] S. Rickard, *Searching for Costas arrays using periodicity properties*, in Proceedings IMA International Conference on Mathematics in Signal Processing VI, Cirencester, UK, 2004. ⟨359, 361⟩
[1805] G. Rinaldi, *Nilpotent 1-factorizations of the complete graph*, J. Combin. Des. 13 (2005) 393–405. ⟨752⟩
[1806] G. Ringel, *Map Color Theorem*, Springer, New York, 1974. ⟨488⟩
[1807] J. P. Robinson and A. J. Bernstein, *A class of binary recurrence codes with limited error propagation*, IEEE Trans. Inform. Theory 13 (1967) 106–113. ⟨439⟩
[1808] P. J. Robinson, *Concerning the Existence and Construction of Orthogonal Designs*, PhD thesis, Australian National University, Canberra, 1975. ⟨284⟩
[1809] R. W. Robinson and N. C. Wormald, *Numbers of cubic graphs*, J. Graph Theory 7 (1983) 463–467. ⟨734⟩
[1810] C. A. Rodger, *Embedding partial Mendelsohn triple systems*, Discrete Math. 65 (1987) 187–196. ⟨159⟩
[1811] ———, *Graph decompositions*, Le Matematiche (Catania) XLV (1990) 119–140. ⟨482⟩
[1812] C. A. Rodger and D. R. Stinson, *Nesting directed cycle systems of even length*, Europ. J. Combin. 13 (1992) 213–218. ⟨381⟩
[1813] Y. Roditty, *Packing and covering of the complete graph III: On the tree packing conjecture*, Scientia A 1 (1988) 81–86. ⟨479⟩
[1814] P. Rodney, *The existence of interval-balanced tournament designs*, J. Combin. Math. Combin. Comput. 19 (1995) 161–170. ⟨595, 596⟩
[1815] D. G. Rogers, *On critical perfect systems of difference sets*, Discrete Math. 135 (1994) 287–301. ⟨439⟩
[1816] C. M. Roney-Dougal, *The primitive permutation groups of degree less than* 2500, J. Algebra 292 (2005) 154–183. ⟨825⟩
[1817] T. G. Room, *A new type of magic square*, Math. Gaz. 39 (1955) 307. ⟨20⟩
[1818] ———, *Polarities and ovals in the Hughes plane*, J. Austral. Math. Soc. 13 (1972) 196–204. ⟨728⟩
[1819] T. G. Room and P. B. Kirkpatrick, *Miniquaternion Geometry*, Cambridge Univ. Press, London, 1971. ⟨171⟩
[1820] A. Rosa, *Poznámka o cyklických Steinerových systémoch trojíc*, Mat. Fyz. Časopis 16 (1966) 285–290. ⟨614⟩
[1821] ———, *On certain valuations of the vertices of a graph*, in Theory of Graphs, P. Rosenstiehl, ed., Gordon and Breach, New York, 1967, 349–355. ⟨482, 483, 484⟩
[1822] ———, *Two-factorizations of the complete graph*, Rend. Sem. Mat. Messina II 9 (2003) 201–210. ⟨375, 376, 377, 382⟩
[1823] A. Rosa and D. R. Stinson, *One-factorizations of regular graphs and Howell designs of small order*, Utilitas Math. 29 (1986) 99–124. ⟨499, 502, 748, 755⟩
[1824] A. Rosa and Š. Znám, *Packing pentagons into complete graphs: How clumsy can you get?* Discrete Math. 128 (1994) 305–316. ⟨379⟩
[1825] A. Rosa and W. D. Wallis, *Premature sets of* 1*-factors or how not to schedule round robin tournaments*, Discrete Appl. Math. 4 (1982) 291–297. ⟨592⟩
[1826] L. A. Rosati, *Unitals in Hughes planes*, Geom. Ded. 27 (1988) 295–299. ⟨728⟩
[1827] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962) 64–94. ⟨798⟩

[1828] R. Roth and D. K. Ray-Chaudhuri, *Hall triple systems and commutative Moufang exponent* 3 *loops: The case of nilpotence class* 2, J. Combin. Theory A 36 (1984) 129–162. ⟨849⟩

[1829] O. S. Rothaus, *On "bent" functions*, J. Combin. Theory A 20 (1976) 300–305. ⟨339, 695, 696⟩

[1830] G. F. Royle and W. D. Wallis, *Constructing bridge club designs*, Bull. Inst. Combin. Appl. 11 (1994) 122–125. ⟨602⟩

[1831] L. D. Rudolph, *A class of majority-logic decodable codes*, IEEE Trans. Inform. Theory 13 (1967) 305–307. ⟨686⟩

[1832] S. Rukavina, *Some new triplanes of order twelve*, Glas. Mat. III 36(56) (2001) 105–125. ⟨37⟩

[1833] B. T. Rumov, *The existence of certain resolvable block designs with group division*, Math. Notes 19 (1976) 376–382. ⟨54⟩

[1834] K. G. Russell, *Balancing carry-over effects in round robin tournaments*, Biometrika 67 (1980) 127–131. ⟨592⟩

[1835] I. Z. Ruzsa, *Solving a linear equation in a set of integers*, Acta Arithmetica 65 (1993) 259–282. ⟨438⟩

[1836] A. Sade, *An omission in Norton's list of* 7×7 *squares*, Ann. Math. Stat. 22 (1951) 306–307. ⟨15⟩

[1837] F. Sagols, L. P. Riccio, and C. J. Colbourn, *Dominated error correcting codes with distance two*, J. Combin. Des. 10 (2002) 294–302. ⟨575⟩

[1838] C. J. Salwach and J. A. Mezzaroba, *The four biplanes with* $k = 9$, J. Combin. Theory A 24 (1978) 141–145. ⟨762⟩

[1839] S. S. Sane, *On a class of symmetric designs*, in Combinatorics and Applications, K. S. Vijayan and N. M. Singhi, eds., Indian Statist. Inst., Calcutta, 1984, 292–302. ⟨40, 47, 53⟩

[1840] S. S. Sane, S. S. Shrikhande, and N. M. Singhi, *Maximal arcs in designs*, Graphs Combin. 1 (1985) 97–106. ⟨114⟩

[1841] D. G. Sarvate, *All directed GDDs with block size three,* $\lambda_1 = 0$*, exist*, Utilitas Math. 26 (1984) 311–317. ⟨442⟩

[1842] ——, *Some results on directed and cyclic designs*, Ars Combin. 19A (1985) 179–190. ⟨442⟩

[1843] S. Savur, *A note on the arrangement of incomplete blocks, when* $k = 3$ *and* $\lambda = 1$, Ann. Eugenics 9 (1939) 45–49. ⟨18⟩

[1844] P. N. Saxena, *A simplified method of enumerating latin squares by MacMahon's differential operators; II. The* 7×7 *latin squares*, J. Indian Soc. Agricultural Statist. 3 (1951) 24–79. ⟨15⟩

[1845] J. Saxl, *On finite linear spaces with almost simple flag-transitive automorphism groups*, J. Combin. Theory A 100 (2002) 322–348. ⟨341⟩

[1846] U. Scarpis, *Sui determinants di valore massimo*, Rend. della R. Istituto Lombardo di Scienze e Lettere (2) 31 (1898) 1441–1446. ⟨14⟩

[1847] P. J. Schellenberg, G. H. J. Van Rees, and S. A. Vanstone, *Four pairwise orthogonal latin squares of order* 15, Ars Combin. 6 (1978) 141–150. ⟨165, 411, 547⟩

[1848] B. Schmalz, *The t-designs with prescribed automorphism group, new simple* 6*-designs*, J. Combin. Des. 1 (1993) 125–170. ⟨93, 97, 766⟩

[1849] B. Schmidt, *Nonexistence of a* $(783, 69, 6)$*-difference set*, Discrete Math. 178 (1998) 283–285. ⟨435⟩

[1850] ——, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. 12 (1999) 929–952. ⟨280⟩

[1851] ——, *Characters and Cyclotomic Fields in Finite Geometry*, Springer, 2002. ⟨422, 424, 435⟩

[1852] D. Schomaker and M. Wirtz, *On binary cyclic codes of length from* 101 *to* 127, IEEE Trans. Inform. Theory 38 (1992) 516–518. ⟨701⟩

[1853] E. Schönhardt, *Über lateinische Quadrate und Unionen*, J. Reine Angew. Math. 163 (1930) 181–230. ⟨15, 18⟩

[1854] S. Schreiber, *Covering all triples on n marks by disjoint Steiner systems*, J. Combin. Theory A 15 (1973) 347–350. ⟨99⟩
[1855] ——, *Some balanced complete block designs*, Israel J. Math. 18 (1974) 31–37. ⟨99⟩
[1856] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. Inform. Theory 51 (2005) 2859–2866. ⟨329⟩
[1857] E. Schröder, *Vorlesungen über die Algebra der Logik, 3 vols.*, B.G. Teubner, Leipzig, 1890-1905. ⟨18⟩
[1858] R. Schürer and W. C. Schmid, *MinT: A database for optimal net parameters*, in Monte Carlo and Quasi-Monte Carlo Methods 2004, H. Niederreiter and D. Talay, eds., Springer, Berlin, 2006. ⟨643⟩
[1859] L. L. Scott Jr., *A condition on Higman's parameters*, Notices Amer. Math. Soc. 20 (1973) A–97 (701–20–45). ⟨855⟩
[1860] E. S. Seah, *Perfect one-factorizations of the complete graph—A survey*, Bull. Inst. Combin. Appl. 1 (1991) 59–70. ⟨755⟩
[1861] E. S. Seah and D. R. Stinson, *An enumeration of nonisomorphic one-factorizations and Howell designs for the graph K_{10} minus a one-factor*, Ars Combin. 21 (1986) 145–161. ⟨755⟩
[1862] ——, *An assortment of new Howell designs*, Utilitas Math. 31 (1987) 175–188. ⟨502, 748⟩
[1863] ——, *A perfect one-factorization for K_{40}*, Congr. Numer. 68 (1989) 211–214. ⟨770⟩
[1864] J. R. Seberry, *Bose's method of differences applied to construct Bhaskar Rao designs*, J. Stat. Plann. Infer. 73 (1998) 215–224. ⟨299⟩
[1865] ——, *Infinite families of generalized Bhaskar Rao designs*, J. Combin. Inf. Syst. Sci. 23 (1998) 455–464. ⟨299⟩
[1866] J. R. Seberry and M. Yamada, *Hadamard matrices, sequences, and block designs*, in [724], 1992, 431–560. ⟨280, 285, 295⟩
[1867] M. Sebille, *Designs: Extensions et groupes primitifs*, Master's thesis, Université Libre de Bruxelles, 1998. ⟨81, 91, 92, 93, 95⟩
[1868] ——, *An extension theorem for t-designs*, Discrete Math. 240 (2001) 197–204. ⟨82⟩
[1869] K. See, S. Y. Song, and J. Stufken, *On a class of partially balanced incomplete block designs with applications in survey sampling*, Commun. Stat. Theory Methods 26 (1997) 1–13. ⟨562⟩
[1870] J. J. Seidel, *Strongly regular graphs with $(-1, 1, 0)$ adjacency matrix having eigenvalue 3*, Lin. Alg. Appl. 1 (1968) 281–298. ⟨855⟩
[1871] ——, *A survey of two-graphs*, Coll. Intern. Teorie Combin., Atti dei convegni Lincei 17, Roma (1976) 481–511. ⟨876, 877, 878, 879⟩
[1872] ——, *Strongly regular graphs*, in Surveys in Combinatorics, 1979, B. Bollobás, ed., Cambridge Univ. Press, London, 1979, 157–180. ⟨855⟩
[1873] ——, *More about two-graphs*, in Fourth Czechoslovakian Symposium on Combinatorics, Graphs and Complexity, J. Nešetřil and M. Fiedler, eds., Elsevier, 1992, 297–309. ⟨881⟩
[1874] J. J. Seidel, A. Blokhuis, and H. A. Wilbrink, *Graphs and association schemes, algebra and geometry*, Tech. Report 83-WSK-02, Department of Mathematics and Computing Sciences, Eindhoven University of Technology, 1983. ⟨112⟩
[1875] J. J. Seidel and D. E. Taylor, *Two-graphs, a second survey*, in Algebraic Methods in Graph Theory, L. Lovász and V. T. Sós, eds., vol. 25, Coll. Math. Soc. J. Bolyai, 1981, 698–711. ⟨879⟩
[1876] J. J. Seidel and S. V. Tsaranov, *Two-graphs, related groups and root systems*, Bull. Soc. Math. Belg. XLII (1990) 695–711. ⟨877⟩
[1877] E. Seiden, *A method of construction of resolvable BIBD*, Sankhyā A 25 (1963) 393–394. ⟨38, 49⟩
[1878] E. Seiden and C. Y. Wu, *A geometric construction of generalized Youden designs for v a power of a prime*, Ann. Statist. 6 (1978) 452–460. ⟨673⟩
[1879] E. Seiden and R. Zemach, *On orthogonal arrays*, Ann. Math. Stat. 37 (1966) 1355–1370. ⟨226⟩

[1880] N. V. Semakov and V. A. Zinov′ev, *Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs*, Problemy Peredači Informacii 4 (1968) 3–10. ⟨698⟩
[1881] ——, *Balanced codes and tactical configurations*, Problemy Peredači Informacii 5 (1969) 28–36. ⟨700⟩
[1882] N. V. Semakov, V. A. Zinov′ev, and G. V. Zaĭcev, *Uniformly close-packed codes*, Problemy Peredači Informacii 7 (1971) 38–50. ⟨684⟩
[1883] Á. Seress, *Permutation Group Algorithms*, Cambridge Univ. Press, Cambridge, 2003. ⟨780⟩
[1884] G. Seroussi and N. H. Bshouty, *Vector sets for exhaustive testing of logic circuits*, IEEE Trans. Inform. Theory 34 (1988) 513–522. ⟨365⟩
[1885] P. D. Seymour and T. Zaslavsky, *Averaging sets: A generalization of mean values and spherical designs*, Adv. Math. 52 (1984) 213–240. ⟨620⟩
[1886] K. R. Shah and B. K. Sinha, *Theory of Optimal Designs*, Springer, Berlin, 1989. ⟨542⟩
[1887] ——, *Optimality aspects of row-column designs with non-orthogonal structure*, J. Stat. Plann. Infer. 36 (1993) 331–346. ⟨542⟩
[1888] N. Shalaby, *Skolem Sequences: Generalizations and Applications*, PhD thesis, McMaster University, Canada, 1992. ⟨613, 616⟩
[1889] ——, *The existence of near-Rosa and hooked near-Rosa sequences*, Discrete Math. 261 (2003) 435–450. ⟨613⟩
[1890] A. Shamir, *How to share a secret*, Comm. ACM 22 (1979) 612–613. ⟨639⟩
[1891] C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J. 27 (1948) 379–423. ⟨19, 519⟩
[1892] ——, *Communication theory of secrecy systems*, Bell Syst. Tech. J. 28 (1949) 656–715. ⟨19, 607, 611⟩
[1893] C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication*, The University of Illinois Press, Urbana, Ill., 1949. ⟨19⟩
[1894] J. Y. Shao and W. D. Wei, *A formula for the number of latin squares*, Discrete Math. 110 (1992) 293–296. ⟨748⟩
[1895] J. B. Shearer, *Some new difference triangle sets*, J. Combin. Math. Combin. Comput. 27 (1998) 65–76. ⟨440⟩
[1896] ——, *Improved LP lower bounds for difference triangle sets*, Electron. J. Comb. 6 (1999) # R31. ⟨439, 440⟩
[1897] ——, *Improved bounds for difference triangle sets*. unpublished, 2006. ⟨440⟩
[1898] M. A. Shokrollahi, *Capacity-achieving sequences*, in Codes, Systems and Graphical Models, B. Marcus and J. Rosenthal, eds., Springer, New York, 2000, 153–166. ⟨521, 523⟩
[1899] M. S. Shrikhande and S. S. Sane, *Quasi-Symmetric Designs*, Cambridge Univ. Press, 1991. ⟨582⟩
[1900] S. S. Shrikhande, *On the non-existence of affine resolvable balanced incomplete block designs*, Sankhyā 11 (1951) 185–186. ⟨47⟩
[1901] ——, *On the dual of some balanced linked block designs*, Biometrics 8 (1952) 66–72. ⟨789⟩
[1902] ——, *The uniqueness of the L_2 association scheme*, Ann. Math. Stat. 30 (1959) 781–798. ⟨855⟩
[1903] ——, *On a two-parameter family of balanced incomplete block designs*, Sankhyā A 24 (1962) 33–40. ⟨40⟩
[1904] ——, *Generalized Hadamard matrices and orthogonal arrays of strength* 2, Canad. J. Math. 16 (1964) 131–141. ⟨412⟩
[1905] ——, *Affine resolvable balanced incomplete block designs: A survey*, Aequat. Math. 14 (1976) 251–269. ⟨220⟩
[1906] S. S. Shrikhande and N. K. Singh, *On a method of constructing symmetrical balance incomplete block designs*, Sankyhā A 24 (1962) 25–32. ⟨277⟩
[1907] ——, *A note on balanced incomplete block designs*, J. Indian Statist. Assoc. 1 (1963) 97–101. ⟨786⟩

[1908] S. S. Shrikhande and N. M. Singhi, *Construction of geometroids*, Utilitas Math. 8 (1975) 187–192. ⟨116⟩
[1909] V. M. Sidel′nikov, *Some k-valued pseudo-random sequences and nearly equidistant codes*, Problemy Peredači Informacii 5 (1969) 16–22. ⟨315⟩
[1910] A. Sidorenko, *What we know and what we do not know about Turán numbers*, Graphs Combin. 11 (1995) 179–199. ⟨651⟩
[1911] T. Siegenthaler, *Correlation-immunity of nonlinear combining functions for cryptographic applications*, IEEE Trans. Inform. Theory 30 (1984) 776–780. ⟨357⟩
[1912] G. P. Sillitto, *An extension property of a class of balanced incomplete block designs*, Biometrika 44 (1957) 278–279. ⟨40⟩
[1913] G. J. Simmons, *Synch-sets: A variant of difference sets*, Congr. Numer. 10 (1974) 625–645. ⟨439⟩
[1914] ——, *A Cartesian product construction for unconditionally secure authentication codes that permit arbitration*, J. Cryptology 2 (1990) 77–104. ⟨611⟩
[1915] ——, *An introduction to shared secret and/or shared control schemes and their application*, in Contemporary Cryptology, IEEE, New York, 1992, 441–497. ⟨639⟩
[1916] ——, *A survey of information authentication*, in Contemporary Cryptology, IEEE, New York, 1992, 379–419. ⟨611⟩
[1917] G. J. Simmons and J. A. Davis, *Pair designs*, Commun. Stat. 4 (1975) 255–272. ⟨595⟩
[1918] J. E. Simpson, *Langford sequences: Perfect and hooked*, Discrete Math. 44 (1983) 97–104. ⟨613⟩
[1919] C. C. Sims, *On the isomorphism of two groups of order* 44,352,000, in The Theory of Finite Groups, R. Brauer and C.-H. Sah, eds., Benjamin, 1969, 101–108. ⟨861⟩
[1920] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. 43 (1938) 377–385. ⟨17, 437⟩
[1921] K. Sinha, R. K. Mitra, and G. M. Saha, *Nested BIB designs, balanced bipartite weighing designs and rectangular designs*, Utilitas Math. 49 (1996) 216–222. ⟨540⟩
[1922] M. Sipser and D. A. Spielman, *Expander codes*, IEEE Trans. Inform. Theory 42 (1996) 1710–1722. ⟨522⟩
[1923] R. R. Sitter and C. F. J. Wu, *Optimal designs for binary response experiments: Fieller, D, and A criteria*, Scand. J. Statist. 20 (1993) 329–341. ⟨542⟩
[1924] T. Skolem, *On certain distributions of integers in pairs with given differences*, Math. Scand. 5 (1957) 57–68. ⟨16⟩
[1925] ——, *Some remarks on the triple systems of Steiner*, Math. Scand. 6 (1958) 273–280. ⟨16⟩
[1926] J. Slaney, M. Fujita, and M. Stickel, *Quasigroup existence problems*, Comput. Math. Applic. 29 (1995) 115–132. ⟨157⟩
[1927] N. J. A. Sloane, *Covering arrays and intersecting codes*, J. Combin. Des. 1 (1993) 51–63. ⟨363, 365⟩
[1928] B. Smetaniuk, *A new construction on latin squares I: A proof of the Evans conjecture*, Ars Combin. 11 (1981) 155–172. ⟨146⟩
[1929] J. D. H. Smith, *Commutative Moufang loops and Bessel functions*, Invent. Math. 67 (1982) 173–187. ⟨849⟩
[1930] K. J. C. Smith, *On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry*, J. Combin. Theory 7 (1969) 122–129. ⟨686⟩
[1931] K. W. Smith, *Non-abelian Hadamard difference sets*, J. Combin. Theory A 70 (1995) 144–156. ⟨425⟩
[1932] M. S. Smith, *On the isomorphism of two simple groups of order* 44,352,000, J. Algebra 41 (1976) 172–174. ⟨861⟩
[1933] P. H. Smith, *Resolvable and Doubly Resolvable Designs with Special Reference to the Scheduling of Duplicate Bridge Tournaments*, PhD thesis, University of Montana, 1977. ⟨597, 606⟩
[1934] L. H. Soicher, *On the structure and classification of SOMAs: Generalizations of mutually orthogonal latin squares*, Electron. J. Comb. 6 (1999) R32. ⟨192, 193⟩

[1935] H. Y. Song, *On aspects of Tuscan squares*, PhD thesis, University of Southern California, 1991. ⟨653, 656, 657⟩
[1936] ——, *On* (n, k)*-sequences*, Discrete Appl. Math. 105 (2000) 183–192. ⟨652⟩
[1937] H. Y. Song and S. W. Golomb, *Generalized Welch–Costas sequences and their applications to vatican squares*, Contemp. Math. 168 (1994) 341–351. ⟨652, 654, 657⟩
[1938] E. Spence, *private communication*. ⟨36, 37, 38, 40, 41, 44⟩
[1939] ——, *A family of difference sets*, J. Combin. Theory A 22 (1977) 103–106. ⟨116⟩
[1940] ——, $(40, 13, 4)$*-designs derived from strongly regular graphs*, in Advances in Finite Geometries and Designs, J. W. P. Hirschfeld, D. R. Hughes, and J. A. Thas, eds., Oxford University Press, New York, 1991, 359–368. ⟨36⟩
[1941] ——, *A complete classification of symmetric* $(31, 10, 3)$ *designs*, Des. Codes Crypt. 2 (1992) 127–136. ⟨36, 762⟩
[1942] ——, *A new family of symmetric* 2-(v, k, λ) *block designs*, Europ. J. Combin. 14 (1993) 131–136. ⟨117⟩
[1943] ——, *Classification of Hadamard matrices of order* 24 *and* 28, Discrete Math. 140 (1995) 185–243. ⟨36, 37⟩
[1944] ——, *Regular two-graphs on* 36 *vertices*, Lin. Alg. Appl. 226-228 (1995) 459–495. ⟨38, 880, 881, 882⟩
[1945] ——, *The complete classification of Steiner systems* $S(2, 4, 25)$, J. Combin. Des. 4 (1996) 295–300. ⟨36, 762⟩
[1946] ——, *All* 2-$(21, 7, 3)$ *designs are residual*, Bull. Belg. Math. Soc. Simon Stevin 5 (1998) 441–445. ⟨36, 114⟩
[1947] ——, *The strongly regular* $(40, 12, 2, 4)$ *graphs*, Electron. J. Comb. 7 (2000) R22. ⟨855⟩
[1948] E. Spence and V. D. Tonchev, *Extremal self-dual codes from symmetric designs*, Discrete Math. 110 (1992) 265–268. ⟨683⟩
[1949] E. Spence, V. D. Tonchev, and Tran van Trung, *A symmetric* 2-$(160, 54, 18)$ *design*, J. Combin. Des. 1 (1993) 65–68. ⟨118⟩
[1950] T. H. Spencer, *Provably good pattern generators for a random pattern test*, Algorithmica 11 (1994) 429–442. ⟨390⟩
[1951] D. A. Spielman, *Faster isomorphism testing of strongly regular graphs*, in Proc. Twenty-eighth Annual ACM Symp. Theory of Computing, New York, 1996, ACM, 576–584. ⟨110⟩
[1952] S. K. Srivastav and J. P. Morgan, *On the class of* 2×2 *balanced incomplete block designs with nested rows and columns*, Commun. Stat. Theory Methods 25 (1996) 1859–1870. ⟨539⟩
[1953] R. G. Stanton and R. C. Mullin, *Construction of Room squares*, Ann. Math. Stat. 39 (1968) 1540–1548. ⟨20⟩
[1954] R. G. Stanton and S. A. Vanstone, *Some theorems on DK-designs*, Ars Combin. 8 (1979) 117–129. ⟨583⟩
[1955] S. K. Stein, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. 52 (1957) 228–256. ⟨20, 158⟩
[1956] J. Steiner, *Combinatorische Aufgabe*, J. Reine Angew. Math. 45 (1853) 181–182. (Gesammelte Werke II, 435–438). ⟨12⟩
[1957] G. Stern, *Tripelsysteme mit Untersystemen*, Arch. Math. (Basel) 33 (1979/80) 204–208. ⟨63⟩
[1958] B. Stevens, *The anti-Oberwolfach solution: Pancyclic* 2*-factorizations of complete graphs*, Theor. Comput. Sci. 297 (2003) 399–424. ⟨376, 377⟩
[1959] B. Stevens and E. Mendelsohn, *New recursive methods for transversal covers*, J. Combin. Des. 7 (1999) 185–203. ⟨773⟩
[1960] ——, *Packing arrays*, Theor. Comput. Sci. 321 (2004) 125–148. ⟨192⟩
[1961] W. L. Stevens, *The completely orthogonalised square*, Ann. Eugenics 9 (1939) 82. ⟨16, 18⟩
[1962] D. R. Stinson, *A general construction for group-divisible designs*, Discrete Math. 33 (1981) 89–94. ⟨244⟩

[1963] ———, *The existence of Howell designs of odd side*, J. Combin. Theory A 32 (1982) 53–65. ⟨499, 504⟩
[1964] ———, *Hill-climbing algorithms for the construction of combinatorial designs*, Ann. Discrete Math. 26 (1985) 321–334. ⟨770, 779⟩
[1965] ———, *The spectrum of nested Steiner triple systems*, Graphs Combin. 1 (1985) 189–191. ⟨70⟩
[1966] ———, *The equivalence of certain incomplete transversal designs and frames*, Ars Combin. 22 (1986) 81–87. ⟨193⟩
[1967] ———, *Frames for Kirkman triple systems*, Discrete Math. 65 (1987) 289–300. ⟨125, 261, 263⟩
[1968] ———, *The combinatorics of authentication and secrecy codes*, J. Cryptology 2 (1990) 23–49. ⟨545, 547, 611⟩
[1969] ———, *Combinatorial characterizations of authentication codes*, Des. Codes Crypt. 2 (1992) 175–187. ⟨611⟩
[1970] ———, *An explication of secret sharing schemes*, Des. Codes Crypt. 2 (1992) 357–390. ⟨639⟩
[1971] ———, *Combinatorial Designs: Construction and Analysis*, Springer, New York, 2004. ⟨228, 391⟩
[1972] ———, *Cryptography: Theory and Practice*, Chapman and Hall/CRC, Boca Raton FL, 3rd ed., 2006. ⟨568, 611, 633, 639⟩
[1973] D. R. Stinson and J. L. Massey, *An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions*, J. Cryptology 8 (1995) 167–173. ⟨356, 357⟩
[1974] D. R. Stinson, Tran van Trung, and R. Wei, *Secure frameproof codes, key distribution patterns, group testing algorithms and related structures*, J. Stat. Plann. Infer. 86 (2000) 595–617. ⟨566, 632, 633⟩
[1975] D. R. Stinson and G. H. J. Van Rees, *Some large critical sets*, Congr. Numer. 34 (1982) 441–456. ⟨384⟩
[1976] D. R. Stinson and S. A. Vanstone, *Some nonisomorphic Kirkman triple systems of order* 39 *and* 51, Utilitas Math. 27 (1985) 199–205. ⟨42⟩
[1977] ———, *A combinatorial approach to threshold schemes*, SIAM J. Disc. Math. 1 (1988) 230–236. ⟨637, 639⟩
[1978] D. R. Stinson, R. Wei, and L. Zhu, *New constructions for perfect hash families and related structures using combinatorial designs and codes*, J. Combin. Des. 8 (2000) 189–200. ⟨566, 567, 635⟩
[1979] ———, *Some new bounds for cover-free families*, J. Combin. Theory A 90 (2000) 224–234. ⟨632⟩
[1980] D. R. Stinson and L. Zhu, *On the existence of MOLS with equal-sized holes*, Aequat. Math. 33 (1987) 96–105. ⟨210⟩
[1981] D. P. Stolle, J. K. Robbennolt, M. Patry, and S. D. Penrod, *Fractional factorial designs for legal psychology*, Behavioral Sciences and the Law 20 (2002) 5–17. ⟨445⟩
[1982] T. Storer, *Cyclotomy and Difference Sets*, Markham, Chicago, 1967. ⟨815, 816⟩
[1983] T. H. Straley, *Scheduling designs for a league tournament*, Ars Combin. 15 (1983) 193–200. ⟨606⟩
[1984] A. P. Street and D. J. Street, *Combinatorics of Experimental Design*, Clarendon Press, Oxford, 1987. ⟨445, 447, 449, 562, 563, 564, 565⟩
[1985] ———, *Latin squares and agriculture: The other bicentennial*, Math. Scientist 13 (1988) 48–55. ⟨17⟩
[1986] D. J. Street, *Bhaskar Rao designs from cyclotomy*, J. Austral. Math. Soc. A 29 (1980) 425–430. ⟨300⟩
[1987] ———, *A note on strongly equi-neighboured designs*, J. Stat. Plann. Infer. 30 (1992) 99–105. ⟨542⟩
[1988] ———, *Constructions for orthogonal main effect plans*, Utilitas Math. 44 (1994) 115–123. ⟨548, 549⟩

[1989] D. J. Street and L. Burgess, *A survey of orthogonal main effect plans and related structures*, Congr. Numer. 99 (1994) 223–239. ⟨549⟩

[1990] D. J. Street and C. A. Rodger, *Some results on Bhaskar Rao designs*, Lect. Notes Math. 829 (1980) 238–245. ⟨300⟩

[1991] A. L. Strehl, *Ternary codes through ternary designs*, Australas. J. Combin. 30 (2004) 21–29. ⟨331⟩

[1992] R. J. Stroeker, *On the diophantine equation* $(2y^2-3)^2 = x^2(3x^2-2)$ *in connection with the existence of nontrivial tight* 4*-designs*, Indag. Math. 43 (1981) 353–358. ⟨329⟩

[1993] S. J. Suchower, *Nonisomorphic complete sets of F-rectangles with varying numbers of symbols*, in Finite Fields: Applications, Theory and Algorithms, G. L. Mullen and P. J.-S. Shiue, eds., Amer. Math. Soc., Providence RI, 1994, 353–362. ⟨467, 468, 471⟩

[1994] Q. Sui and B. Du, *The Oberwolfach problem for a unique* 5*-cycle and all others of length* 3, Utilitas Math. 65 (2004) 243–254. ⟨375⟩

[1995] ——, *The number of triangles in* 2*-factorizations*, J. Combin. Des. 14 (2006) 277–289. ⟨377⟩

[1996] J. J. Sylvester, *Note on the historical origin of the unsymmetrical six-valued function of six letters*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. 21 (1861) 369–377. (Collected Mathematical Papers II, 264–271). ⟨13⟩

[1997] ——, *Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers*, Phil. Mag. 34 (1867) 461–475. ⟨14, 275, 306⟩

[1998] T. Szőnyi, *Complete arcs in non-Desarguesian planes*, Ars Combin. 25 (1988) 169–178. ⟨728⟩

[1999] K. Takeuchi, *A table of difference sets generating balanced incomplete block designs*, Rev. Inst. Internat. Statist. 30 (1962) 361–366. ⟨35, 36, 37, 38, 39, 40, 41, 43, 44⟩

[2000] K. Tanabe, *A criterion for designs in* $\mathbb{Z}_4$*-codes on the symmetrized weight enumerator*, Des. Codes Crypt. 30 (2003) 169–185. ⟨681⟩

[2001] Y. Tang and J. X. Yin, *The combinatorial constructions for a class of optimal optical orthogonal codes*, Science in China A 45 (2002) 1268–1275. ⟨404, 556⟩

[2002] M. R. Tanner, *A recursive approach to low complexity codes*, IEEE Trans. Inform. Theory 27 (1981) 533–547. ⟨520⟩

[2003] H. Tarnanen, *Upper bounds on permutation codes via linear programming*, Europ. J. Combin. 20 (1999) 101–114. ⟨571⟩

[2004] G. Tarry, *Le problème des* 36 *officiers*, Assoc. Franc. Paris 29 (1900) 170–203. ⟨12, 15⟩

[2005] M. Tarsi, *Decomposition of complete multigraphs into stars*, Discrete Math. 26 (1979) 273–278. ⟨479⟩

[2006] D. E. Taylor, *Graphs and block designs associated with the three-dimensional unitary groups*, in Combinatorial Mathematics, D. A. Holton, ed., Springer, Berlin, 1974, 128–131. ⟨854, 880⟩

[2007] ——, *Regular two-graphs*, Proc. London Math. Soc. 35 (1977) 257–274. ⟨854, 879, 880, 881⟩

[2008] L. Teirlinck, *On the maximum number of disjoint triple systems*, J. Geom. 12 (1975) 93–96. ⟨65, 99⟩

[2009] ——, *On making two Steiner triple systems disjoint*, J. Combin. Theory A 23 (1977) 349–350. ⟨64⟩

[2010] ——, *On projective and affine hyperplanes*, J. Combin. Theory A 28 (1980) 290–306. ⟨691, 788⟩

[2011] ——, *On large sets of disjoint quadruple systems*, Ars Combin. 12 (1984) 173–176. ⟨65, 85, 98⟩

[2012] ——, *Non-trivial* t*-designs without repeated blocks exist for all* t, Discrete Math. 65 (1987) 301–311. ⟨20, 82, 547⟩

[2013] ——, *On large sets of disjoint ordered designs*, Ars Combin. 25 (1988) 31–37. ⟨546⟩
[2014] ——, *Locally trivial t-designs and t-designs without repeated blocks*, Discrete Math. 77 (1989) 345–356. ⟨84, 92, 93, 98⟩
[2015] ——, *A completion of Lu's determination of the spectrum for large sets of disjoint Steiner triple systems*, J. Combin. Theory A 57 (1991) 302–305. ⟨13, 65, 99⟩
[2016] ——, *Large sets of disjoint designs and related structures*, in [724], 1992, 561–592. ⟨80, 545, 546⟩
[2017] G. Tenengolts, *Nonbinary codes correcting single deletion or insertion*, IEEE Trans. Inform. Theory 30 (1984) 766–769. ⟨387⟩
[2018] P. Terwilliger, *The subconstituent algebra of an association scheme I*, J. Algeb. Combin. 1 (1992) 363–388. ⟨329⟩
[2019] ——, *The subconstituent algebra of an association scheme II, III*, J. Algeb. Combin. 2 (1993) 73–103 (II), 177–210 (III). ⟨329⟩
[2020] J. A. Thas, *Construction of maximal arcs and partial geometries*, Geom. Ded. 3 (1974) 61–64. ⟨728⟩
[2021] ——, *Partial geometries in finite affine spaces*, Math. Zeitschr. 158 (1978) 1–13. ⟨560, 561⟩
[2022] ——, *Generalized quadrangles and flocks of cones*, Europ. J. Combin. 8 (1987) 441–452. ⟨474⟩
[2023] ——, *Generalized polygons*, in Handbook of Incidence Geometry, F. Buekenhout, ed., North-Holland, Amsterdam, 1995, 383–431. ⟨475, 476, 477⟩
[2024] ——, *Projective geometry over a finite field*, in Handbook of Incidence Geometry, F. Buekenhout, ed., North-Holland, Amsterdam, 1995, 295–347. ⟨559, 561⟩
[2025] ——, *Generalized quadrangles of order* (s, s^2) *III*, J. Combin. Theory A 87 (1999) 247–272. ⟨476⟩
[2026] J. A. Thas and F. De Clerck, *Partial geometries satisfying the axiom of Pasch*, Simon Stevin 51 (1977/78) 123–137. ⟨557, 558⟩
[2027] J. A. Thas, K. Thas, and H. Van Maldeghem, *Translation Generalized Quadrangles*, World Scientific, 2006. ⟨476⟩
[2028] K. Thas, *Symmetry in Finite Generalized Quadrangles*, Birkhäuser, Basel, 2004. ⟨477⟩
[2029] S. Thomas, *Designs over finite fields*, Geom. Ded. 24 (1987) 237–242. ⟨850⟩
[2030] T. M. Thompson, *From Error-Correcting Codes through Sphere Packings to Simple Groups*, Mathematical Association of America, Washington DC, 1983. ⟨19⟩
[2031] D. Tiessen and G. H. J. Van Rees, *Many* $(22, 44, 14, 7, 4)$- *and* $(15, 42, 14, 5, 4)$-*balanced incomplete block designs*, J. Stat. Plann. Infer. 62 (1997) 115–124. ⟨37⟩
[2032] A. Tietäväinen, *On the nonexistence of perfect codes over finite fields*, SIAM J. Appl. Math. 24 (1973) 88–96. ⟨701⟩
[2033] T. W. Tillson, *A hamiltonian decomposition of* K^*_{2m}, $2m \geq 8$, J. Combin. Theory B 29 (1980) 68–74. ⟨655, 656⟩
[2034] J. Tits, *Sur la trialité et certains groupes qui s'en déduisent*, Inst. Hautes Etudes Sci. Publ. Math. 2 (1959) 14–60. ⟨20⟩
[2035] T. Tjur, *An algorithm for the optimization of block designs*, J. Stat. Plann. Infer. 36 (1993) 277–282. ⟨542⟩
[2036] J. A. Todd, *A combinatorial problem*, J. Math. Phys. 12 (1933) 321–333. ⟨14⟩
[2037] D. T. Todorov, *Three mutually orthogonal latin squares of order* 14, Ars Combin. 20 (1985) 45–48. ⟨164, 547⟩
[2038] ——, *Four mutually orthogonal latin squares of order* 20, Ars Combin. 27 (1989) 63–65. ⟨165⟩
[2039] V. D. Tonchev, *Hadamard matrices of order* 28 *with automorphisms of order* 13, J. Combin. Theory A 35 (1983) 43–57. ⟨44⟩
[2040] ——, *Hadamard matrices of order* 28 *with automorphisms of order* 7, J. Combin. Theory A 40 (1985) 62–81. ⟨690⟩
[2041] ——, *A characterization of designs related to dodecads in the Witt system* $S(5, 8, 24)$, J. Combin. Theory A 43 (1986) 219–227. ⟨701⟩

[2042] ——, *A characterization of designs related to the Witt system* $S(5,8,24)$, Math. Zeitschr. 191 (1986) 225–230. ⟨701⟩
[2043] ——, *Quasi-symmetric* 2-$(31,7,7)$ *designs and a revision of Hamada's conjecture*, J. Combin. Theory A 42 (1986) 104–110. ⟨50, 687, 688⟩
[2044] ——, *Quasi-symmetric designs and self-dual codes*, Europ. J. Combin. 7 (1986) 67–73. ⟨580, 582, 687, 688⟩
[2045] ——, *Embedding of the Witt–Mathieu system* $S(3,6,22)$ *in a symmetric* 2-$(78,22,6)$ *design*, Geom. Ded. 22 (1987) 49–75. ⟨41, 118, 580, 689⟩
[2046] ——, *Combinatorial Configurations: Designs, Codes, Graphs*, Longman Scientific & Technical, Harlow, 1988. Translated from the Bulgarian by Robert A. Melter. ⟨493, 680, 701⟩
[2047] ——, *Symmetric designs without ovals and extremal self-dual codes*, Ann. Discrete Math. 37 (1988) 451–457. ⟨683⟩
[2048] ——, *Self-orthogonal designs and extremal doubly even codes*, J. Combin. Theory A 52 (1989) 197–205. ⟨682⟩
[2049] ——, *Self-orthogonal designs*, in Finite Geometries and Combinatorial Designs, E. S. Kramer and S. S. Magliveras, eds., Amer. Math. Soc., Providence RI, 1990, 219–235. ⟨580, 582, 683, 701⟩
[2050] ——, *Quasi-symmetric designs, codes, quadrics, and hyperplane sections*, Geom. Ded. 48 (1993) 295–308. ⟨694, 695, 696⟩
[2051] ——, *A class of Steiner* 4*-wise balanced designs derived from Preparata codes*, J. Combin. Des. 4 (1996) 203–204. ⟨660, 685⟩
[2052] ——, *The uniformly packed binary* $[27,21,3]$ *and* $[35,29,3]$ *codes*, Discrete Math. 149 (1996) 283–288. ⟨696⟩
[2053] ——, *Maximum disjoint bases and constant-weight codes*, IEEE Trans. Inform. Theory 44 (1998) 333–334. ⟨701⟩
[2054] ——, *Linear perfect codes and a characterization of the classical designs*, Des. Codes Crypt. 17 (1999) 121–128. ⟨687⟩
[2055] ——, *A mass formula for Steiner triple systems* $\mathrm{STS}(2^n-1)$ *of* 2*-rank* 2^n-n, J. Combin. Theory A 95 (2001) 197–208. ⟨692⟩
[2056] ——, *A formula for the number of Steiner quadruple systems on* 2^n *points of* 2*-rank* 2^n-n, J. Combin. Des. 11 (2003) 260–274. ⟨692⟩
[2057] ——, *Affine designs and linear orthogonal arrays*, Discrete Math. 294 (2005) 219–222. ⟨699⟩
[2058] ——, *A class of* 2-$(3^n7, 3^{n-1}7, (3^{n-1}7-1)/2)$ *designs*, J. Combin. Des. (to appear). ⟨47⟩
[2059] V. D. Tonchev and R. V. Raev, *Cyclic* 2-$(13,5,5)$ *designs*, C. R. Acad. Bulgare Sci. 35 (1982) 1205–1208. ⟨37⟩
[2060] ——, *Cyclic* 2-$(17,8,7)$ *designs and related doubly-even codes*, C. R. Acad. Bulgare Sci. 35 (1982) 1367–1370. ⟨38⟩
[2061] V. D. Tonchev and R. S. Weishaar, *Steiner triple systems of order* 15 *and their codes*, J. Stat. Plann. Infer. 58 (1997) 207–216. ⟨691, 701⟩
[2062] S. Topalova, *Enumeration of* 2-$(25,5,2)$ *designs with an automorphism of order* 5, J. Combin. Inf. Syst. Sci. 22 (1997) 161–176. ⟨36⟩
[2063] ——, *Construction and Study of Combinatorial Designs with Certain Automorphisms*, PhD thesis, Mathematics, Bulgarian Academy of Sciences, 1998. ⟨39⟩
[2064] ——, *Enumeration of* 2-$(21,5,2)$ *block designs with automorphisms of odd prime order*, Diskretn. Anal. Issled. Oper. Ser. 1 5 (1998) 64–81, 105. ⟨36⟩
[2065] ——, *Symmetric* 2-$(69,17,4)$ *designs with automorphisms of order* 13, J. Stat. Plann. Infer. 95 (2001) 335–339. ⟨38, 767⟩
[2066] ——, *Classification of Hadamard matrices of order* 44 *with automorphisms of order* 7, Discrete Math. 260 (2003) 275–283. ⟨41⟩
[2067] Tran van Trung, *The existence of symmetric block designs with parameters* $(41,16,6)$ *and* $(66,26,10)$, J. Combin. Theory A 33 (1982) 201–204. ⟨43, 44, 118⟩
[2068] ——, *The existence of an infinite family of simple* 5*-designs*, Math. Zeitschr. 187 (1984) 285–287. ⟨81⟩

[2069] ———, *On the construction of t-designs and the existence of some new infinite families of simple* 5*-designs*, Arch. Math. (Basel) 47 (1986) 187–192. ⟨81, 82, 86, 87⟩
[2070] ———, *Nonembeddable quasi-residual designs*, in Finite Geometries and Combinatorial Designs, E. S. Kramer and S. S. Magliveras, eds., Amer. Math. Soc., Providence RI, 1990, 237–278. ⟨113⟩
[2071] ———, *Maximal arcs and related designs*, J. Combin. Theory A 57 (1991) 294–301. ⟨40, 43⟩
[2072] ———, *Recursive constructions for* 3*-designs and resolvable* 3*-designs*, J. Stat. Plann. Infer. 95 (2001) 341–358. ⟨82⟩
[2073] Tran van Trung and S. S. Martirosyan, *New constructions for IPP codes*, Des. Codes Crypt. 35 (2005) 227–239. ⟨567⟩
[2074] M. Trick, *Guide to sports scheduling*. `http://mat.gsia.cmu.edu/~sports/`. ⟨606⟩
[2075] N. D. Tuan, *Simple non-trivial designs with an arbitrary automorphism group*, J. Combin. Theory A 100 (2002) 403–408. ⟨339⟩
[2076] ———, *On a divisibility problem for polynomials and its application to Cameron–Praeger designs*, J. London Math. Soc. (2) 67 (2003) 545–560. ⟨344⟩
[2077] P. Turán, *Research problems*, Magyar Tud. Akad. Mat. Kutató Int. Közl 6 (1961) 417–423. ⟨649⟩
[2078] T. P. Turiel, *A computer program to determine defining contrasts and factor combinations for the two-level fractional factorial designs of resolution III, IV and V*, J. Qual. Technol. 20 (1988) 267–272. ⟨451⟩
[2079] R. J. Turyn, *On c-matrices of arbitrary powers*, Canad. J. Math. 23 (1971) 531–535. ⟨879⟩
[2080] H. Tverberg, *On the decomposition of K_n into complete bipartite graphs*, J. Graph Theory 6 (1982) 493–494. ⟨482⟩
[2081] P. Ullrich, *Officers, playing cards and sheep*, Metrika 56 (2002) 189–204. ⟨22⟩
[2082] K. Ushio, *On balanced claw designs of complete multipartite graphs*, Discrete Math. 38 (1982) 117–119. ⟨480⟩
[2083] F. Vakil and M. Parnes, *On the structure of a class of sets useful in nonadaptive group testing*, J. Stat. Plann. Infer. 39 (1994) 57–69. ⟨562, 630, 633⟩
[2084] E. R. van Dam, W. H. Haemers, and M. B. M. Peek, *Equitable resolvable coverings*, J. Combin. Des. 11 (2003) 113–123. ⟨373, 773⟩
[2085] J. H. van Lint, *Recent results on perfect codes and related topics*, in Combinatorics, M. Hall Jr. and J. H. van Lint, eds., Math. Centrum, Amsterdam, 1974, 158–178. ⟨701⟩
[2086] ———, *Introduction to Coding Theory*, Springer, New York, 1982. ⟨695, 701⟩
[2087] J. H. van Lint and A. Schrijver, *Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields*, Combinatorica 1 (1981) 63–73. ⟨853⟩
[2088] J. H. van Lint and J. J. Seidel, *Equilateral point sets in elliptic geometry*, Proc KNAW A 69; Indag. Math. 28 (1966) 335–348. ⟨878⟩
[2089] J. H. van Lint and V. D. Tonchev, *A class of nonembeddable designs*, J. Combin. Theory A 62 (1993) 252–260. ⟨114⟩
[2090] J. H. van Lint, V. D. Tonchev, and I. N. Landgev, *A new design*, in Coding Theory and Design Theory II, D. K. Ray-Chaudhuri, ed., Springer, New York, 1990, 251–256. ⟨37⟩
[2091] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge Univ. Press, Cambridge, 2nd ed., 2001. ⟨141, 748⟩
[2092] G. H. J. Van Rees and S. A. Vanstone, *Equidistant permutation arrays: A bound*, J. Austral. Math. Soc. A 33 (1982) 262–274. ⟨570⟩
[2093] H. C. A. van Tilborg, *Uniformly Packed Codes*, PhD thesis, Technical University Eindhoven, 1976. ⟨684, 695⟩
[2094] S. A. Vanstone, *Generalized Room squares and related combinatorial designs*, Congr. Numer. 20 (1978) 591–601. ⟨731⟩

[2095] S. A. Vanstone, D. R. Stinson, P. J. Schellenberg, A. Rosa, R. S. Rees, C. J. Colbourn, M. W. Carter, and J. Carter, *Hanani triple systems*, Israel J. Math. 83 (1993) 305–319. ⟨67⟩

[2096] T. M. J. Vasiga, S. C. Furino, and A. C. H. Ling, *The spectrum of α-resolvable block designs with block size four*, J. Combin. Des. 9 (2001) 1–16. ⟨130⟩

[2097] O. Veblen and W. H. Bussey, *Finite projective geometries*, Trans. Amer. Math. Soc. 7 (1906) 241–259. ⟨16⟩

[2098] W. N. Venables and J. A. Eccleston, *Randomized search strategies for finding optimal or near optimal block and row-column designs*, Austral. J. Statist. 35 (1993) 371–382. ⟨542⟩

[2099] A. Vietri, *Cyclic k-cycle systems of order $2kn+k$: A solution of the last open cases*, J. Combin. Des. 12 (2004) 299–301. ⟨382⟩

[2100] K. Vik, *Bedømmelse av feilen på forsøksfelter med og uten malestokk*, Meldinger fra Norges Landbrukshøgskole 4 (1924) 129–181. ⟨17⟩

[2101] F. O. Wagner, *Relational structures and dimensions*, in Automorphisms of First-Order Structures, R. Kaye and D. Macpherson, eds., Oxford University Press, New York, 1994, 153–180. ⟨505, 506⟩

[2102] R. A. Walker II and C. J. Colbourn, *Tabu search for covering arrays using permutation vectors*, preprint. ⟨363, 365⟩

[2103] ——, *Perfect hash families: constructions and tables*, J. Math. Crypt. (to appear). ⟨566, 567⟩

[2104] W. D. Wallis, *Construction of strongly regular graphs using affine designs*, Bull. Austral. Math. Soc. 4 (1971) 41–49. ⟨116⟩

[2105] ——, *Configurations arising from maximal arcs*, J. Combin. Theory A 15 (1973) 115–119. ⟨240⟩

[2106] ——, *The problem of the hospitable golfers*, Ars Combin. 15 (1983) 149–152. ⟨597⟩

[2107] ——, *One-factorizations of complete graphs*, in [724], 1992, 593–631. ⟨593, 597, 743, 755⟩

[2108] ——, *One-Factorizations*, Kluwer, Dordrecht, 1997. ⟨755⟩

[2109] ——, *Triad designs*, Congr. Numer. (to appear). ⟨603⟩

[2110] W. D. Wallis, A. P. Street, and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Springer, Berlin, 1972. ⟨48, 49, 50, 51, 53, 54, 56, 57, 586, 590, 628⟩

[2111] P.-J. Wan, G. Calinescu, L. Liu, and O. Frieder, *Grooming of arbitrary traffic in SONET/WDM BLSRs*, IEEE J. Sel. Areas Commun. 18 (2000) 1995–2003. ⟨494⟩

[2112] J. Wang, *Incomplete group divisible designs with block size four*, J. Combin. Des. 11 (2003) 442–455. ⟨259⟩

[2113] J. Wang and L. Ji, *Existence of $T^*(3, 4, v)$-codes*, J. Combin. Des. 13 (2005) 42–53. ⟨387, 388⟩

[2114] J. Wang and J. X. Yin, *Existence of holey 3-GDDs of type $(u, g^t w^1)$*, Discrete Math. 202 (1999) 249–269. ⟨260⟩

[2115] ——, *Construction for perfect 5-deletion-correcting codes of length 7*, IEEE Trans. Inform. Theory (to appear). ⟨388, 442⟩

[2116] J. F. Wang, *Isomorphic factorizations of complete equipartite graphs—The proof of the Harary–Robinson–Wormald conjecture*, Sci. Sinica A 25 (1982) 1152–1164. ⟨485⟩

[2117] S. P. Wang, *On Self-Orthogonal Latin Squares and Partial Transversals of Latin Squares*, PhD thesis, Ohio State University, 1978. ⟨165, 216⟩

[2118] I. M. Wanless, *Permanents, Matchings and Latin Rectangles*, PhD thesis, Australian National Univ., 1997. ⟨145⟩

[2119] ——, *Perfect factorisations of bipartite graphs and latin squares without proper subrectangles*, Electron. J. Comb. 6 (1999) R9. ⟨145⟩

[2120] ——, *A generalisation of transversals for latin squares*, Electron. J. Comb. 9 (2002) R12. ⟨143, 147⟩

[2121] ——, *Atomic latin squares based on cyclotomic orthomorphisms*, Electron. J. Comb. 12 (2005) R22. ⟨146, 752⟩
[2122] I. M. Wanless and E. C. Ihrig, *Symmetries that latin squares inherit from 1-factorizations*, J. Combin. Des. 13 (2005) 157–172. ⟨146, 755⟩
[2123] I. M. Wanless and B. S. Webb, *The existence of latin squares without orthogonal mates*, Des. Codes Crypt. 40 (2006) 131–135. ⟨189⟩
[2124] A. Wassermann, *Finding simple t-designs with enumeration techniques*, J. Combin. Des. 6 (1998) 79–90. ⟨766⟩
[2125] J. J. Watkins and R. J. Wilson, *A survey of snarks*, in Graph Theory, Combinatorics, and Applications, Y. Alavi, G. Chartrand, O. R. Oellermann, and A. J. Schwenk, eds., Wiley, New York, 1991, 1129–1144. ⟨741⟩
[2126] R. Wei, *Group divisible designs with equal-sized holes*, Ars Combin. 35 (1993) 315–323. ⟨260⟩
[2127] L. M. Weiss and D. L. Kreher, *The bigraphical t-wise balanced designs of index two*, J. Combin. Des. 3 (1995) 233–255. ⟨492⟩
[2128] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976. ⟨848, 851, 852⟩
[2129] P. Wernicke, *Das Problem der* 36 *Offiziere*, Deutsche Math.-Ver. 19 (1910) 264–267. ⟨12⟩
[2130] M. A. Wertheimer, *Designs in Quadrics*, PhD thesis, University of Pennsylvania, 1986. ⟨37, 44, 46, 50⟩
[2131] A. T. White, *Efficient imbeddings of finite projective planes*, Proc. London Math. Soc. (3) 70 (1995) 33–55. ⟨488⟩
[2132] ——, *Graphs of Groups on Surfaces*, North-Holland, Amsterdam, 2001. ⟨488⟩
[2133] ——, *Modelling finite geometries on surfaces*, Discrete Math. 244 (2002) 479–493. ⟨489⟩
[2134] ——, *Modelling biplanes on surfaces*, Europ. J. Combin. 25 (2004) 899–909. ⟨489⟩
[2135] H. S. White, F. N. Cole, and L. D. Cummings, *Complete classification of the triad systems on fifteen elements*, Memoirs Nat. Acad. Sci. U.S.A. 14 (1919) 1–89. 2nd memoir. ⟨15⟩
[2136] A. L. Whiteman, *A family of difference sets*, Illinois J. Math. 6 (1962) 107–121. ⟨116⟩
[2137] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964. ⟨820, 847⟩
[2138] A. Wigderson, *The amazing power of pairwise independence*, in Proc. 26th ACM Symposium on the Theory of Computing, ACM, 1994, 645–647. ⟨391⟩
[2139] H. A. Wilbrink, *Two-graphs and geometries*. unpublished. ⟨879⟩
[2140] H. A. Wilbrink and A. E. Brouwer, *A* $(57, 14, 1)$ *strongly regular graph does not exist*, Indag. Math. 45 (1983) 117–121. ⟨856⟩
[2141] P. Wild, *Generalized Hussain graphs and semibiplanes with* $k \leq 6$, Ars Combin. 14 (1982) 147–167. ⟨123⟩
[2142] J. Williamson, *Hadamard's determinant theorem and the sum of four squares*, Duke Math. J. 11 (1944) 65–81. ⟨14⟩
[2143] R. A. Wilson, P. Walsh, J. Tripp, I. Suleiman, S. Rogers, R. Parker, S. Norton, S. Nickerson, S. Linton, J. Bray, and R. Abbott, *Atlas of finite group representations*, 1999. University of Birmingham, `http://brauer.maths.qmul.ac.uk/Atlas/`, Version 2.0. ⟨820⟩
[2144] R. M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory 4 (1972) 17–47. ⟨35, 40, 42, 43, 45, 46, 47, 49, 50, 51, 52, 55, 397, 401⟩
[2145] ——, *An existence theory for pairwise balanced designs I. Composition theorems and morphisms*, J. Combin. Theory A 13 (1972) 220–245. ⟨20, 236⟩
[2146] ——, *An existence theory for pairwise balanced designs II. The structure of PBD-closed sets and the existence conjectures*, J. Combin. Theory A 13 (1972) 246–273. ⟨20, 247, 248, 249⟩
[2147] ——, *The necessary conditions for t-designs are sufficient for something*, Utilitas Math. 4 (1973) 207–215. ⟨20, 84⟩

[2148] ———, *Nonisomorphic Steiner triple systems*, Math. Zeitschr. 135 (1973/74) 303–313. ⟨37⟩
[2149] ———, *Constructions and uses of pairwise balanced designs*, in Mathematisch Centre Tracts, vol. 55, Mathematisch Centrum, Amsterdam, 1974, 18–41. ⟨20, 254⟩
[2150] ———, *A few more squares*, Congr. Numer. 10 (1974) 675–680. ⟨417⟩
[2151] ———, *An existence theory for pairwise balanced designs III: A proof of the existence conjectures*, J. Combin. Theory A 18 (1975) 71–79. ⟨20, 247, 658⟩
[2152] ———, *Decompositions of complete graphs into subgraphs isomorphic to a given graph*, Congr. Numer. 15 (1976) 647–659. ⟨478⟩
[2153] ———, *Inequalities for t-designs*, J. Combin. Theory A 34 (1983) 313–324. ⟨789⟩
[2154] ———, *The exact bound in the Erdős–Ko–Rado theorem*, Combinatorica 4 (1984) 247–257. ⟨330⟩
[2155] ———, *On the theory of t-designs*, in Enumeration and Design, D. M. Jackson and S. A. Vanstone, eds., Academic Press, Toronto, 1984, 19–49. ⟨329, 330, 785, 789⟩
[2156] ———, *Signed hypergraph designs and diagonal forms for some incidence matrices*, Des. Codes Crypt. 17 (1989) 289–297. ⟨788⟩
[2157] A. Winterhof, *On the non-existence of generalized Hadamard matrices*, J. Stat. Plann. Infer. 84 (2000) 337–342. ⟨305⟩
[2158] E. Witt, *Die 5-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg 12 (1938) 256–264. ⟨107⟩
[2159] ———, *Über Steinersche Systeme*, Abh. Math. Sem. Univ. Hamburg 12 (1938) 265–275. ⟨12, 17, 85, 86, 87, 544⟩
[2160] M. Wojtas, *Five mutually orthogonal latin squares of order* 35, J. Combin. Des. 4 (1996) 153–154. ⟨167⟩
[2161] ———, *Three new constructions of mutually orthogonal latin squares*, J. Combin. Des. 8 (2000) 218–220. ⟨170⟩
[2162] J. K. Wolf, *Born again group testing: Multiaccess communications*, IEEE Trans. Inform. Theory 31 (1985) 185–191. ⟨630, 633⟩
[2163] A. Wolfe, *Block transitive meager squares over GF(q) for prime q*, preprint. ⟨69⟩
[2164] ———, *The resolution of the anti-mitre Steiner triple system conjecture*, J. Combin. Des. 14 (2006) 229–236. ⟨68⟩
[2165] W. W. Wolfe, *Orthogonal Designs—Amicable Orthogonal Designs*, PhD thesis, Queen's University, Kingston, 1975. ⟨283, 295⟩
[2166] D. E. Woolbright and H. L. Fu, *On the existence of rainbows in* 1*-factorizations*, J. Combin. Des. 6 (1998) 1–20. ⟨752⟩
[2167] W. S. B. Woolhouse, *Prize question 1733*, Lady's and Gentleman's Diary (1844). ⟨12⟩
[2168] ———, *On the Rev. T.P. Kirkman's problem respecting certain triadic arrangements of fifteen symbols*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. 22 (1861) 510–515. ⟨13⟩
[2169] N. C. Wormald, *Isomorphic factorizations. VII. Regular graphs and tournaments*, J. Graph Theory 8 (1984) 117–122. ⟨485⟩
[2170] Q. Wu, *On Properties and Constructions of t-Designs, λ-Designs and Perpendicular arrays*, PhD thesis, University of Nebraska, 1975. ⟨660⟩
[2171] S. L. Wu and H. L. Fu, *Cyclic m-cycle systems with* $m \leq 32$ *or* $m = 2q$ *with* q *a prime power*, J. Combin. Des. 14 (2006) 66–81. ⟨382⟩
[2172] T. Xia, M. Xia, and J. R. Seberry, *Regular Hadamard matrix, maximum excess and SBIBD*, Australas. J. Combin. 27 (2003) 263–275. ⟨277, 280⟩
[2173] Q. Xiang, *Recent progress in algebraic design theory*, Finite Fields Appl. 11 (2005) 622–653. ⟨420, 423, 435, 790⟩
[2174] Y. Xu, H. Zhang, and L. Zhu, *Existence of frame SOLS of type* $a^n b^1$, Discrete Math. 250 (2002) 211–230. ⟨214⟩
[2175] S. Yamada and D. K. Lin, *Construction of mixed-level supersaturated designs*, Metrika 56 (2002) 205–214. ⟨453⟩
[2176] C. H. Yang, *On composition of four-symbol δ-codes and Hadamard matrices*, Proc. Amer. Math. Soc. 107 (1989) 763–776. ⟨320, 321⟩

[2177] S. H. Yang, *The isomorphic factorization of complete tripartite graphs $K(m, n, s)$—A proof of F. Harary, R. W. Robinson and N. C. Wormald's conjecture*, Discrete Math. 145 (1995) 239–257. ⟨485⟩
[2178] H. P. Yap, *Some Topics in Graph Theory*, Cambridge Univ. Press, Cambridge, 1986. ⟨479⟩
[2179] F. Yates, *Complex experiments*, Proc. Royal Stat. Soc. B2 (1935) 181–223. ⟨17⟩
[2180] ——, *Incomplete randomised blocks*, Ann. Eugenics 7 (1936) 121–140. ⟨17⟩
[2181] ——, *A new method of arranging variety trials involving a large number of varieties*, J. Agricultural Science 26 (1936) 424–455. ⟨17⟩
[2182] J. X. Yin, *Existence of BIBDs with block size eight and $\lambda = 7$*, J. Combin. Math. Combin. Comput. 16 (1994) 193–198. ⟨72, 245⟩
[2183] ——, *On λ-packings of pairs by quintuples: $\lambda \equiv 0 \pmod 4$*, Ars Combin. 37 (1994) 288–300. ⟨551⟩
[2184] ——, *Some combinatorial constructions for optical orthogonal codes*, Discrete Math. 185 (1998) 201–219. ⟨556⟩
[2185] ——, *Existence of directed GDDs with block size five and index $\lambda \geq 2$*, J. Stat. Plann. Infer. 86 (2000) 619–627. ⟨442⟩
[2186] ——, *A combinatorial construction for perfect deletion-correcting codes*, Des. Codes Crypt. 23 (2001) 99–110. ⟨387⟩
[2187] ——, *Packing designs with equal-sized holes*, J. Stat. Plann. Infer. 94 (2001) 393–403. ⟨554⟩
[2188] ——, *A general construction for optimal cyclic packing designs*, J. Combin. Theory A 97 (2002) 272–284. ⟨556⟩
[2189] ——, *A survey on maximum distance holey packings*, Discrete Appl. Math. 121 (2002) 279–294. ⟨555, 556⟩
[2190] J. X. Yin and A. M. Assaf, *Constructions of optimal packing designs*, J. Combin. Des. 6 (1998) 245–260. ⟨551⟩
[2191] J. X. Yin and K. Chen, *A complete solution to the packing problem with block size six and index five*, Ars Combin. 37 (1994) 257–261. ⟨552⟩
[2192] J. X. Yin, Y. Lu, and J. Wang, *Maximum distance holey packings and related codes*, Science In China A 42 (1999) 1262–1269. ⟨554, 555⟩
[2193] J. X. Yin and Y. Miao, *Almost resolvable BIBDs with block size 5 or 6*, Ars Combin. 138 (1993) 303–314. ⟨125, 127⟩
[2194] J. X. Yin and S. Wu, *Four new BIBDs with block size seven*, Discrete Math. 113 (1993) 281–284. ⟨72, 245⟩
[2195] W. J. Youden, *Use of incomplete block replications in estimating tobacco-mosaic virus*, Contrib. Boyce Thompson Inst. 9 (1937) 41–48. ⟨18, 669⟩
[2196] M. L. Yu, *Almost resolvable P_k-decompositions of complete graphs*, J. Graph Theory 15 (1991) 523–541. ⟨479⟩
[2197] ——, *On tree factorizations of K_n*, J. Graph Theory 17 (1993) 713–725. ⟨480⟩
[2198] A. I. Zenkin and V. K. Leont′ev, *A nonclassical pattern recognition problem*, Zh. Vychisl. Mat. i Mat. Fiz. 24 (1984) 925–931. ⟨386⟩
[2199] H. Zhang, *Specifying latin squares in propositional logic*, in Automated Reasoning and Its Applications, R. Veroff, ed., M.I.T. Press, 1997, ch. 6. ⟨157⟩
[2200] J. Zhang and Y. Chang, *The spectrum of cyclic* BSA$(v, 3, \lambda; \alpha)$ *with $\alpha = 2, 3$*, J. Combin. Des. 13 (2005) 313–335. ⟨616⟩
[2201] X. Zhang and G. Ge, *On the existence of partitionable skew Room frames*, preprint. ⟨263, 588⟩
[2202] ——, *Super-simple resolvable balanced incomplete block designs with block size 4 and index 2*, J. Combin. Des. (to appear). ⟨634⟩
[2203] X. B. Zhang, *Constructions of resolvable Mendelsohn designs*, Ars Combin. 34 (1992) 225–250. ⟨531⟩
[2204] ——, *Construction for indecomposable simple (v, k, λ)-BIBDs*, Discrete Math. 156 (1996) 317–322. ⟨70⟩
[2205] ——, *On the existence of $(v, 4, 1)$-RPMD*, Ars Combin. 42 (1996) 3–31. ⟨532, 666⟩
[2206] ——, *A few more RPMDs with $k = 4$*, Ars Combin. 74 (2005) 187–200. ⟨532⟩

[2207] Y. Zhang and B. Du, *α-resolvable group divisible designs with block size three*, J. Combin. Des. 13 (2005) 139–151. ⟨265⟩

[2208] Y. Zhang, S. Pang, and Y. Wang, *Orthogonal arrays obtained by generalized Hadamard product*, Discrete Math. 238 (2001) 151–170. ⟨220⟩

[2209] K. Zhu and B. Mukherjee, *A review of traffic grooming in WDM optical networks: Architectures and challenges*, Optical Networks Magazine 4 (2003) 55–64. ⟨494⟩

[2210] L. Zhu, *A few more self-orthogonal latin squares with symmetric orthogonal mates*, Congr. Numer. 42 (1984) 313–320. ⟨216⟩

[2211] ———, *Some recent developments on BIBDs and related designs*, Discrete Math. 123 (1993) 189–214. ⟨232, 235, 244, 255, 256, 259, 260⟩

[2212] ———, *Existence of self-orthogonal latin squares* ISOLS$(6m + 2, 2m)$, Ars Combin. 39 (1995) 65–74. ⟨213⟩

[2213] L. Zhu, B. Du, and X. B. Zhang, *A few more RBIBD's with $k = 5$ and $\lambda = 1$*, Discrete Math. 97 (1991) 409–417. ⟨125, 127⟩

[2214] L. Zhu and S. Wu, *Existence of three-fold BIBDs with block size* 7, Appl. Math. J. Chinese Universities 7 (1992) 321–326. ⟨72⟩

[2215] L. Zhu and H. Zhang, *Completing the spectrum of r-orthogonal latin squares*, Discrete Math. 268 (2003) 343–349. ⟨190⟩

[2216] P.-H. Zieschang, *An Algebraic Approach to Association Schemes*, Springer, Berlin, 1996. ⟨330⟩

[2217] B. I. Zil′ber, *The structure of models of uncountably categorical theories*, in Proceedings of the International Congress of Mathematicians, Z. Ciesielski and C. Olech, eds., North-Holland, Amsterdam, 1984, 359–368. ⟨851⟩

[2218] V. A. Zinov′ev and V. K. Leont′ev, *On non-existence of perfect codes over Galois fields*, Problems Control Inform. Theory 2 (1973) 123–132. ⟨701⟩

[2219] K. Zulauf, *Über Tripelsysteme von* 13 *Elementen*, Wintersche Buchdruckerei, Darmstadt, 1897. ⟨15⟩

Index

Mathematics

Handbook of Combinatorial Designs

Continuing in the bestselling, informative tradition of the first edition, the **Handbook of Combinatorial Designs, Second Edition** remains the only resource to contain all of the most important results and tables in the field of combinatorial design. More than 30% longer than the first edition, the handbook covers the constructions, properties, and applications of designs as well as existence results.

New to the Second Edition

- An introductory part that provides a general overview and a historical perspective of combinatorial designs
- Numerous chapters concerning the combinatorics of designs, such as triple systems, group divisible designs, block-transitive designs, factorial designs, lotto designs, and nested designs
- Applications in cryptography, communications, networking, statistics, and testing
- Various codes for nontraditional applications, including superimposed, optical orthogonal, and powerline
- Fully updated tables, including BIBDs, MOLS, PBDs, and Hadamard matrices
- Over 2,200 references in a single bibliographic section

Meeting the need for up-to-date and accessible tabular and reference information, this handbook provides the tools to understand combinatorial design theories and applications that span the entire discipline.

Features

- Presents the latest as well as basic information pertaining to the construction, existence, and uses of combinatorial designs
- Supplies extensive tables and examples of Latin squares, orthogonal arrays, balanced incomplete block designs, t-designs, pairwise balanced designs, and Hadamard matrices
- Includes many applications used in statistics, cryptography, coding theory, graph theory, computer science, information theory, and mathematical finance
- Contains a state-of-the-art description of the computational methods used to construct and classify combinatorial designs

About the Editors

Charles J. Colbourn is professor of computer science at Arizona State University, Tempe, USA.
Jeffrey H. Dinitz is professor of mathematics at the University of Vermont, Burlington, USA.

Chapman & Hall/CRC
Taylor & Francis Group
an informa business
www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

C5068

ISBN 1-58488-506-8

9 781584 885061 90000

www.crcpress.com