Oxford Lecture Series in
Mathematics and its Applications 30

OXFORD LECTURES SERIES IN MATHEMATICS AND ITS APPLICATIONS

Books in the series

1. J.C. Baez (ed.): *Knots and quantum gravity*
2. I. Fonseca and W. Gangbo: *Degree theory in analysis and applications*
3. P.L. Lions: *Mathematical topics in fluid mechanics, Vol. 1: Incompressible models*
4. J.E. Beasley (ed.): *Advances in linear and integer programming*
5. L.W. Beineke and R.J. Wilson (eds): *Graph connections: Relationships between graph theory and other areas of mathematics*
6. I. Anderson: *Combinatorial designs and tournaments*
7. G. David and S.W. Semmes: *Fractured fractals and broken dreams*
8. Oliver Pretzel: *Codes and algebraic curves*
9. M. Karpinski and W. Rytter: *Fast parallel algorithms for graph matching problems*
10. P.L. Lions: *Mathematical topics in fluid mechanics, Vol. 2: Compressible models*
11. W.T. Tutte: *Graph theory as I have known it*
12. Andrea Braides and Anneliese Defranceschi: *Homogenization of multiple integrals*
13. Thierry Cazenave and Alain Haraux: *An introduction to semilinear evolution equations*
14. J.Y. Chemin: *Perfect incompressible fluids*
15. Giuseppe Buttazzo, Mariano Giaquinta and Stefan Hildebrandt: *One-dimensional variational problems: an introduction*
16. Alexander I. Bobenko and Ruedi Seiler: *Discrete integrable geometry and physics*
17. Doina Cioranescu and Patrizia Donato: *An introduction to homogenization*
18. E.J. Janse van Rensburg: *The statistical mechanics of interacting walks, polygons, animals and vesicles*
19. S. Kuksin: *Hamiltonian partial differential equations*
20. Alberto Bressan: *Hyperbolic systems of conservation laws: the one-dimensional Cauchy problem*
21. B. Perthame: *Kinetic formulation of conservation laws*
22. A. Braides: *Gamma-convergence for beginners*
23. Robert Leese and Stephen Hurley: *Methods and Algorithms for Radio Channel Assignment*
24. Charles Semple and Mike Steel: *Phylogenetics*
25. Luigi Ambrosio and Paolo Tilli: *Topics on Analysis in Metric Spaces*
26. Eduard Feireisl: *Dynamics of Viscous Compressible Fluids*
27. Antonìn Novotnỳ and Ivan Straškraba: *Introduction to the Mathematical Theory of Compressible Flow*
28. Pavol Hell and Jarik Nesetril: *Graphs and Homomorphisms*
29. Pavel Etingof and Frederic Latour: *The dynamical Yang-Baxter equation, representation theory, and quantum integrable systems*
30. Jorge Ramirez Alfonsin: *The Diophantine Frobenius Problem*

The Diophantine Frobenius Problem

J.L. Ramírez Alfonsín

Equipe Combinatoire
Université Pierre et Marie Curie, Paris 6
4 Place Jussieu, 75252 Paris Cedex 05

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford OX2 6DP
Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide in

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trade mark of Oxford University Press
in the UK and in certain other countries

Published in the United States
by Oxford University Press Inc., New York

First published 2005

British Library Cataloguing in Publication Data
Data available

Library of Congress Cataloguing in Publication Data
Data available

Typeset by SPI Publisher Services, Pondicherry, India
Printed in Great Britain
on acid-free paper by

Biddles Ltd., King's Lynn. Norfolk

ISBN 0-19-856820-7 978-0-19-856820-9

1 3 5 7 9 10 8 6 4 2

à Sylvie

This page intentionally left blank

Contents

Preface **xi**

Acknowledgements **xv**

1 Algorithmic aspects **1**

1.1 Algorithms for computing $g(a_1, a_2, a_3)$ 3

1.1.1 Rødseth's Algorithm 3

1.1.2 Davison's Algorithm 4

1.1.3 Killingbergtrø's method 6

1.2 General algorithms 8

1.2.1 Scarf and Shallcross' method 8

1.2.2 Heap and Lynn method 11

1.2.3 Greenberg's Algorithm 18

1.2.4 Nijenhuis' Algorithm 19

1.2.5 Wilf's Algorithm 19

1.2.6 Kannan's method 21

1.3 Computational complexity of **FP** 24

1.4 Supplementary notes 28

2 The Frobenius number for small n **31**

2.1 Computing $g(p, q)$ is easy 31

2.2 A Formula for $g(a_1, a_2, a_3)$ 35

2.3 Results when $n = 3$ 36

2.3.1 Hofmeister's formula and its generalization 39

2.3.2 More special cases 40

2.3.3 Johnson integers 42

2.4 $g(a_1, a_2, a_3, a_4)$ 42

2.5 Supplementary notes 43

3 The general problem **45**

3.1 Formulas and upper bounds 45

3.2 Bounds in terms of the $lcm(a_1, \ldots, a_n)$ 57

3.3 Arithmetic and related sequences 59

3.4 Regular bases 61

3.5 Extending basis 62

3.6 Lower bounds 63
3.7 Supplementary notes 68

4 Sylvester denumerant 71
4.1 From partitions to denumerants 71
4.2 Formulas and bounds for $d(m; a_1, \ldots, a_n)$ 73
4.3 Computing denumerants 77
4.3.1 Partial fractions 77
4.3.2 Bell's method 78
4.4 $d(m; p, q)$ 80
4.5 $d(m; a_1, a_2, a_3)$ and $d(m; a_1, a_2, a_3, a_4)$ 81
4.6 Hilbert series 86
4.7 A proof of a formula for $g(a_1, a_2, a_3)$ 89
4.8 Ehrhart polynomial 91
4.9 Variations of the denumerant 95
4.9.1 $d'(m; a_1, \ldots, a_n)$ 96
4.9.2 $d''(m; a_1, \ldots, a_n)$ 98
4.10 Supplemetary notes 100

5 Integers without representation 103
5.1 Sylvester's classical result 103
5.2 Nijenhuis' and Wilf's results 105
5.3 Formulas for $N(a_1, \ldots, a_n)$ 108
5.4 Arithmetic sequences 110
5.5 The sum of integers in $N(p, q)$ 111
5.6 Related games 113
5.6.1 Sylver Coinage 113
5.6.2 The jugs problem 114
5.7 Supplemetary notes 117

6 Generalizations and related problems 119
6.1 Special functions 119
6.2 The modular generalization 124
6.3 The postage stamp problem 127
6.4 $(a_1, \ldots, a_n)$-trees 128
6.5 Vector generalization of **FP** 130
6.6 Supplementary notes 133

7 Numerical semigroups 135
7.1 Gaps and non-gaps 135
7.1.1 Telescopic semigroups 139
7.1.2 Hyperelliptic semigroups 140

7.2 Symmetric semigroups 141
7.2.1 Intersection of semigroups 148
7.2.2 Apéry sets 149
7.3 Related concepts 150
7.3.1 Type sequences 150
7.3.2 Complete intersection 152
7.3.3 The Möbius function 153
7.4 Supplementary notes 154

8 Applications of the Frobenius number 159
8.1 Complexity analysis of the Shell-sort method 159
8.2 Petri Nets 161
8.2.1 P/T systems 161
8.2.2 Weighted circuits systems 163
8.3 Partition of a vector space 165
8.4 Monomial curves 168
8.5 Algebraic geometric codes 171
8.6 Tilings 174
8.7 Applications of denumerants 175
8.7.1 Balls and cells 175
8.7.2 Conjugate power equations 177
8.7.3 Invariant cubature formulas 179
8.8 Other applications 179
8.8.1 Generating random vectors 179
8.8.2 Non-hamiltonian graphs 181
8.9 Supplementary notes 183

Appendix A
Problems and conjectures 185
A.1 Algorithmic questions 185
A.2 $g(a_1, \ldots, a_n)$ 186
A.3 Denumerant 187
A.4 $N(a_1, \ldots, a_n)$ 187
A.5 Gaps 188
A.6 Miscellaneous 189
A.6.1 Erdős' Problems 191

Appendix B 193
B.1 Computational complexity aspects 193
B.2 Graph theory aspects 194
B.3 Modules, resolutions and Hilbert series 194
B.4 Shell-sort method 197

B.5 Bernoulli numbers 198
B.6 Irreducible and primitive matrices 200
B.6.1 Upper bounds of index of primitivity 202
B.6.2 Computation of index of primitivity 203

References 205

Index 241

Preface

During the early part of the last century, Ferdinand Georg Frobenius (1849–1917) raised, in his lectures (according to [57]), the following problem (called the *diophantine Frobenius Problem* **FP**): given relatively prime positive integers $a_1, \ldots, a_n$, find the largest natural number (called the *Frobenius number* and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a non-negative integer combination of $a_1, \ldots, a_n$.

At first glance, **FP** may look deceptively specialized. Nevertheless it crops up again and again in the most unexpected places. It turned out that the knowledge of $g(a_1, \ldots, a_n)$ has been extremely useful to investigate many different problems.

A number of methods, from several areas of mathematics, have been used in the hope of finding a formula giving the Frobenius number and algorithms to calculate it. The main intention of this book is to highlight such 'methods, ideas, viewpoints and applications' for as wide an audience as possible. The results on **FP** are quite scattered in the literature and, at present, there is no complete or accessible source summarizing the progress on it. This book aims to provide a comprehensive exposition of what is known today on **FP**.

Chapter 1 is devoted to the computational aspects of the Frobenius number. After discussing a number of methods to solve **FP** when $n = 3$ (some of these procedures make use of diverse concepts, such as the *division remainder, continued fractions* and *maximal lattice free bodies*) we present a variety of algorithms to compute $g(a_1, \ldots, a_n)$ for general n. The main ideas of these algorithms are based on concepts from *graph theory, index of primitivity* of non-negative matrices (see Appendix B.6) and *mathematical programming.* While the running times of these algorithms are superpolynomial, there does exist a method, due to R. Kannan, that solves **FP** in polynomial time for any *fixed* n. We describe this method, in which the *covering radius* concept is introduced. We finally prove that **FP** is *$\mathcal{NP}$-hard* under Turing reductions.

FP is easy to solve when $n = 2$. Indeed,

$$g(a_1, a_2) = a_1 a_2 - a_1 - a_2. \qquad (1)$$

However, the computation of a (simple) formula when $n = 3$ is much more difficult and has been the subject of numerous research papers over a long period. F. Curtis has proved that the search for such a formula is, in some sense, doomed to failure since the Frobenius number cannot be given by 'closed' formulas of a certain type. Recently, an explicit formula for computing $g(a_1, a_2, a_3)$ has been found. After presenting four different proofs of equality (1), one of which uses the well-known *Pick's theorem*, Chapter 2 presents the result of Curtis, the general formula (whose algebraic proof is given in Chapter 4) and summarizes the known upper bounds for $g(a_1, a_2, a_3)$, as well as exact formulas for particular triples.

Chapter 3 provides a systematic exposition of the known formulas, including upper and lower bounds for $g(a_1, \ldots, a_n)$ for general n and for special sequences (for instance, when $a_1, \ldots, a_n$ forms an *arithmetic* sequence). Results on the change in value of $g(a_1, \ldots, a_n)$, when an additional element a_{n+1} is inserted, are also given.

In 1857, while investigating the *partition number* function, James Joseph Sylvester (1814–1897) [438] defined the function $d(m; a_1, \ldots, a_n)$, called the *denumerant*, as the number of non-negative integer representations of m by $a_1, \ldots, a_n$, that is, the number of solutions of the form

$$m = \sum_{i=1}^{n} x_i a_i$$

with integers $x_i \geq 0$. Chapter 4 is devoted to the study of the denumerant and related functions. After discussing briefly some basic properties of the *partition function* and its relation with denumerants, we analyse the general behaviour of $d(m; a_1, \ldots, a_n)$ and its connection to $g(a_1, \ldots, a_n)$. Two interesting methods for computing denumerants, one based on a decomposition of the *rational fraction* into *partial fractions* and a second due to E.T. Bell, are described. We prove an exact value of $d(m; p, q)$, first found by T. Popoviciu in 1953, and summarize the known results when $n = 2$ and $n = 3$. We shall see how to calculate $g(a_1, \ldots, a_n)$ by using *Hilbert series* via *free resolutions* and use this approache to show an explicit formula for $g(a_1, a_2, a_3)$. We discuss the connection among denumerants, **FP** and *Ehrhart polynomial.* Also, two variants of $d(m; a_1, \ldots, a_n)$ are studied. The first is related to counting the number of lattice points lying in certain polytopes while the second restricts the number of repetitions of the a_is.

Let $N(a_1, \ldots, a_n)$ be the number of integers without non-negative integer representations by $a_1, \ldots, a_n$. In Chapter 5, a thorough presentation of the function $N(a_1, \ldots, a_n)$ is given. In 1882, Sylvester [439], obtained the exact value when $n = 2$,

$$N(a_1, a_2) = \frac{1}{2}(a_1 - 1)(a_2 - 1). \tag{2}$$

Later, in 1884, in the *Educational Times* journal, Sylvester [437] posed (as a recreational problem) the question of finding such a formula. An ingenious solution was given by W.J. Curran Sharp. It remains a mystery why the standard reference to this celebrated formula of Sylvester is the solution given by Curran Sharp rather than its original appearance in [439, page 134]. In this chapter, we reproduce the original page of this famous and much-cited manuscript. We also give two other proofs of equality (2). We then discuss the work of M. Nijenhuis and H.S. Wilf connecting $N(a_1, \ldots, a_n)$ to **FP** as well as to other concepts (such as the *Gorenstein* condition). We continue by discussing some general bounds on $N(a_1, \ldots, a_n)$ and exact formulas for special sequences, for instance the formula given by E.S. Selmer for *almost arithmetic* sequences. A generalization of Sylvester's formula due to Ø.J. Rødseth, where the so-called *Bernoulli* numbers (see Appendix B.5) appeared, is treated. The final section of this chapter is devoted to two 'integer representation' games: the well-known *sylver coinage*, invented by J.C. Conway and the *jugs problem* the roots of which can be traced back at least as far as Tartaglia, an Italian mathematician of the sixteenth century.

Let $g(n, t)$ and $h(n, t)$ be the largest and smallest of the Frobenius numbers when $a_1 < \cdots < a_n = t$ and $t = a_1 < \cdots < a_n$, respectively. Chapter 6 reviews the results on these functions. It also examines an algorithm that solves the *modular change* problem, a generalization of **FP**, due to Z. Skupień, discribes the relation between **FP** and $(a_1, \ldots, a_n)$*-trees*, discusses the *postage stamp* problem as well as a multidimensional generalization of **FP**.

Chapter 7 introduces the concept of *numerical semigroups*. We investigate several properties of the *gaps* and *nongaps* of a semigroup (which are closely related to $N(a_1, \ldots, a_n)$) and point out the importance of the role played by the Frobenius number (also known as *conductor*) in the study of *symmetric* and *pseudo-symmetric* semigroups (and their connection to *monomial curves*). We prove a number of results relating **FP** to *telescopic semigroups*, the famous *Apéry Sets* (used by R. Apéry [13] in the study of *algebroid planar branches*), *type sequences* in semigroups, *complete intersection* semigroups, γ-*hyperelliptic* semigroups (motivated by the study of *Weierstrass* semigroups), the *Möbius* function, and other related concepts.

Chapter 8 presents a number of applications of **FP** to a variety of problems. The complexity analysis of the *Shell-sort* method was not well understood until J. Incerpi and R. Sedgewick nicely observed that **FP** can be used to obtain upper bounds for the running time of this fundamental sorting algorithm. Chapter 8 starts by explaining this application. Then, it is explained how **FP** may be applied to analyse *Petri nets* (a net model for discrete event systems), to study *partitions of vector spaces* (which can be considered as a generalization of partitions of abelian groups), to compute *exact resolutions* via Rødseth's method for finding the Frobenius number when $n = 3$, to investigate *algebraic geometric* codes via the properties of special semigroups and their corresponding conductors and to study *tiling* problems. Chapter 8 also discusses three applications of the denumerant. One in relation to the calculation of the number of possible placements of n different balls into r distinct cells under certain restrictions, another to investigate the solution of some *conjugate* problems and the last one in relation with *invariant cubature* formulas. We also present an application of the *modular change* problem to study *non-hypoHamiltonian* graphs, and of the *vector* generalization to give a new method for generating *random* vectors.

The book concludes with two appendices. In the first one a number of open problems are stated and in the second one some notation, definitions and basic results of various topics are given.

This book attempts to place the reader at the frontier of what is known on **FP**. In the interests of balance, we have chosen not to give a proof of each and every result (particularly of the numerous bounds and formulas stated in Chapters 2 and 3). However, all the main theorems are either proved or treated in some detail. We illustrate with examples most of the methods explained in Chapter 1. We always try to give exact references and appropriate credits for the proofs and results that have been adapted from printed material. References to the literature where the reader may find more complete treatments of the various topics, and some historical comments, are given at the end of each chapter.

Despite many careful readings, errors will unavoidably remain. We welcome corrections and suggestions. Please send these to me at ramirez@math.jussieu.fr. We plan to mantain an updated list of corrections at the following web site pointer

`http://www.ecp6.math.jussieu.fr/pageperso/ramirez/ramirez.html`

The topics in this book are in a state of continual development. We also plan to note new progress on **FP** in the same site.

Acknowledgements

I first started to work on **FP** while doing my D.Phil. supervised by Colin McDiarmid. At that time, Colin introduced me to knapsack-type problems that naturally lead me to consider **FP**. Colin has always encouraged and motivated me in different mathematical (and other) aspects that have certainly impacted in my academic career. In particular, Colin's enthusiasm gave me a first stimulus to write this manuscript. I wish to express my gratitude to Colin not only for his continuous support and generosity but also for a number of insightful mathematical discussions. I thank D. Welsh for many interesting conversations.

I am grateful to the following people either for providing me with several reprints and manuscripts or for their helpful comments and suggestions to early drafts of this manuscript (most of them for both!): K. Aardal, M. Beck, A. Bondy, E. Boros, V.E. Brimkov, P. Chrzastowski-Wachtel, W.-S. Chou, C. Delorme, C. Del Vigna, S. Eliahou, L.G. Fel, R. Freud, J.I. García-García, P.A. García-Sánchez, F. Halter-Koch, Y. Hamidoune, H.G. Killingbergtrø, G. Kiss, T. Komatsu, Z. Lipták, P. Lisoněk, A. López-Ortiz, M. Morales, R.Z. Norman, A.E. Özlük, A. Plagne, C. Pomerance, S. Robins, J.C. Rosales, Ø.J. Rødseth, A. Rycerz, E.S. Selmer, J. Shallit, P.J.-S. Shiue, J. Simpson, B. Stechkin, L. Szekely, C. Tinaglia, H.J.H. Tuenter, B. Vizvári, S. Wagon, N. Yanev and D. Zagier. I thank P. Chrząstowski-Wachtel for giving me a copy of his mailing with P. Erdős.

I would like thank the Computer and Automata Research Institute, (SZTAKI) Budapest (especially J. Breyer), the Forschungsinstitut für Diskrete Mathematik, Universität Bonn (especially M. Lange), the Technische Universität Chemnitz, Chemnitz, the Radcliffe Science, University of Oxford, the Research Institute for Symbolic Computation, Johannes Kepler University, Linz the Mathématiques – Recherche, Jussieu, Paris (especially O. Vigeannel-Larive), and d'Informatique – Recherche, Jussieu, Paris libraries for searching a number of literature sources for me.

The roots of this book come from the unpublished manuscript [344] done while visiting the Forschungsinstitut für Diskrete Mathematik, Universität Bonn. I wish to thank B. Korte and all his team at the Forschungsinstitut für Diskrete Mathematik for warmly hosting me and offering me a number of facilities while preparing [344] and others. I am also grateful to the Alexander von Humboldt Foundation for their financial support and generous hospitality during my stay at Bonn.

I especially want to thank my wife Sylvie for her patience and encouragement that always accompanied me through this (and others) work.

J.L. Ramírez Alfonsín,
Paris, 2005

1

Algorithmic aspects

Let $a_1, \ldots, a_n$ be positive integers with $a_i \geq 2$ and such that their greatest common divisor, denoted by $(a_1, \ldots, a_n)$, is one (the sequence $a_1, \ldots, a_n$ is called the *basis*). We say that s is representable as a non-negative integer combination of $a_1, \ldots, a_n$ if there exist integers $x_i \geq 0$ such that

$$s = \sum_{i=1}^{n} x_i a_i.$$

The existence of a positive integer N such that any integer $s \geq N$ is representable as a non-negative integer combination of $a_1, \ldots, a_n$ is a folk result[1].

Theorem 1.0.1 *If $(a_1, \ldots, a_n) = 1$ then there exists an integer N such that any integer $s \geq N$ is representable as a non-negative integer combination of $a_1, \ldots, a_n$.*

The celebrated *Frobenius problem* (**FP**) is to find the largest natural number that is not representable as a non-negative integer combination of $a_1, \ldots, a_n$. This number is traditionally denoted by $g(a_1, \ldots, a_n)$ and called the *Frobenius number*[2]. **FP** is also known as the *money-changing* problem:

[1] This result has been used in the study on the density of the sum of two sets of integers [358, page 211] and in the theory of probability [141].

[2] Although, F.G. Frobenius never put forward such a problem explicitly written in a manuscript, **FP** has been attributed to him. In the introduction section of [57], A. Brauer stated

> *Frobenius mentioned this problem occasionally in his lectures.*

Two of the main subjects of interest of Frobenius were the cyclicity of non-negative matrices [147, page 553] and the theory of linear forms [146]. It is conceivable that this kind of investigation naturally led Frobenius to consider **FP**.

> *"Given n coins of denominations $a_1, \ldots, a_n$ with $(a_1, \ldots, a_n) = 1$, what is the largest integer amount of money for which change cannot be made with these coins?"*

The Frobenius number is frequently related to the McNugget numbers[†]; see [464]. We give two proofs of Theorem 1.0.1.

First proof of Theorem 1.0.1. Since $(a_1, \ldots, a_n) = 1$ we can write $m_1a_1 + \cdots + m_na_n = 1$ for some integers m_i. Denote by P and $-Q$ the sum of the positive and negative terms in this decomposition, so that P and Q belong to the semigroup[3] W generated by $a_1, \ldots, a_n$ and $P - Q = 1$. Any integer $k \geq 0$ can be written as $ha_1 + k'$ with $h \geq 0$ and $0 \leq k' < a_1$. Then $(a_1-1)Q+k = ha_1+(a_1-1-k')Q+k'P \in W$. Hence all integers greater than or equal to $(a_1-1)Q$ belong to W. That is, any integer $t \geq (a_1 - 1)Q$ can be written as a non-negative integer combination of $a_1, \ldots, a_{n-1}$. □

The above proof implies that $g(a_1, \ldots, a_n) < (a_1 - 1)Q$. We will see in Chapter 3 that this bound can be largely improved. The following proof of Theorem 1.0.1 is by induction on n.

Second proof of Theorem 1.0.1. If $n = 2$ the result follows since $g(a_1, a_2) = a_1a_2 - a_1 - a_2$ (see Theorem 2.1.1). Suppose that $n \geq 3$. If $(a_1, \ldots, a_{n-1}) = 1$, then, by induction, it is not even needed a_n to represent all large integer. Assume that $(a_1, \ldots, a_{n-1}) = d > 1$. Let $a_i = a_i'd$ for each $i = 1, \ldots, n-1$. Since $(d, a_n) = 1$ then equation

$$\sum_{i=1}^{n} a_ix_i = m \tag{1.1}$$

becomes

$$\sum_{i=1}^{n-1} a_i'x_i = \frac{m - a_nb_n}{d} \tag{1.2}$$

where $0 \leq b_n \leq d-1$ is the unique integer such that $a_nb_n \equiv m \bmod d$. By induction, there exists integer $M(a_1', \ldots, a_{n-1}')$ such that eqn (1.2) has non-negative integer solution $x_i = b_i$, $1 \leq i \leq n-1$ whenever $\frac{m-a_nb_n}{d} \geq \frac{m-a_n(d-1)}{d} > M(a_1', \ldots, a_{n-1}')$. So, eqn (1.1) has non-negative

[†] (From [478]) A *McNugget number* is a number which can be obtained by adding together orders of McDonald's® Chicken McNuggets™ (prior to consuming any), which originally came in boxes of 6, 9 and 20. All positive integers are McNugget numbers except 1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 22, 23, 25, 28, 31, 34, 37, and 43. So, the largest non-McNugget number is given by g(6, 9, 20) = 43.

[3] See Chapter 7 for a detailed discussion on semigroups.

integer solution $x_i = b_i$, $1 \le i \le n$ whenever $m > a_n(d-1) + dM(a'_1, \dots, a'_{n-1})$. □

Theorem 1.0.1 can also be proved by using generating functions; see Theorems 4.2.1 and 4.3 and also [305]. We shall see in Section 1.3 that **FP** is a hard problem in general from the computational point of view. We will see in Chapter 6 (Corollary 6.1.1 and eqn (6.5)) that the magnitude of $g(a_1, \dots, a_n)$, with $t_1 \le a_1 < \cdots < a_n \le t_2$, is between $t_1 + \frac{1}{n-1}$ and t_2^2 for any fixed $n \ge 3$. This can explain, in some sense, why **FP** when $n \ge 3$, is so difficult (computing $g(a_1, a_2)$ is easy; see Theorem 2.1.1).

1.1 Algorithms for computing $g(a_1, a_2, a_3)$

FP is a difficult problem from the computational point of view (see Theorem 1.3.1) so there is no hope for a *fast* (*polynomial time*) algorithm that solves **FP**, unless $\mathcal{P} = \mathcal{NP}$. Thus, not-so-fast algorithms as well as algorithms for particular cases have great importance. In this section we overview some well-known algorithms that compute $g(a_1, a_2, a_3)$.

1.1.1 Rødseth's Algorithm

Selmer and Beyer [404] developed an algorithm to compute $g(a_1, a_2, a_3)$; see also [44]. Their method relies on many elementary but tedious manipulations with continued fractions, and is therefore not easy to implement. Rødseth [373] managed to simplify the Selmer–Beyer algorithm by using negative division remainders in the continued fraction algorithm[4]. Rødseth's algorithm works well on average (probably $O(\log a_2)$) but in the worst case can take $O(a_1 + \log a_2)$ operations since it involves the length of a semiregular continued fraction for a_3/a_2, which can be as long as a_2. We describe Rødseth's procedure.

Rødseth's Algorithm

Let s_0 be the unique integer such that $a_2 s_0 \equiv a_3 \bmod a_1$, $0 \le s_0 < a_1$
The continued fraction algorithm is applied to the ratio a_1/s_0:

[4] In an unpublished thesis by Siering [422], closely related results (with quite different proofs) to those presented by Rødseth in [373] were given.

$$\begin{aligned} a_1 &= q_1 s_0 - s_1,\ 0 \le s_1 < s_0,\\ s_0 &= q_2 s_1 - s_2,\ 0 \le s_2 < s_1,\\ s_1 &= q_3 s_2 - s_3,\ 0 \le s_3 < s_2,\\ &\ \vdots\\ s_{m-1} &= q_{m+1} s_m,\\ s_{m+1} &= 0, \end{aligned}$$

where $q_i \ge 2$, $s_i \ge 0$ for all i.
Let $p_{-1} = 0,\ p_0 = 1,\ p_{i+1} = q_{i+1}p_i - p_{i-1}$ and $r_i = (s_i a_2 - p_i a_3)/a_1$. Let v be the unique integer number such that $r_{v+1} \le 0 < r_v$, or equivalently, the unique integer such that

$$\frac{s_{v+1}}{p_{v+1}} \le \frac{a_3}{a_2} < \frac{s_v}{p_v}.$$

Then,

$$g(a_1, a_2, a_3) = -a_1 + a_2(s_v - 1) + a_3(p_{v+1} - 1) - \min\{a_2 s_{v+1}, a_3 p_v\}.$$

Example 1.1.1 Let us compute $g(5, 7, 11)$ by using Rødseth's method. In this case, $s_0 = 3$ and

$$\begin{aligned} 5 &= q_1 3 - s_1,\ 0 \le s_1 < 3,\ q_1 = 2,\ s_1 = 1\\ 3 &= q_2 1 - s_2,\ 0 \le s_2 < 1,\ q_2 = 3,\ s_2 = 0. \end{aligned}$$

Thus, $p_0 = 1,\ p_1 = 2,\ p_3 = 5$ and $\frac{s_1}{p_1} = \frac{1}{2} \le \frac{11}{7} < \frac{3}{1} = \frac{s_0}{p_0}$. Therefore, $g(5, 7, 11) = -5 + 7(2) + 11(1) - \min\{7, 11\} = -5 + 14 + 11 - 7 = 25 - 12 = 13$.

We invite the reader to see Section 8.4 where a nice algebraic application of this method is given.

1.1.2 Davison's Algorithm

Davison [104] proposed an algorithm, based on modifications of Rødseth and Selmer–Beyer algorithms, running in $O(\log a_2)$ operations for all inputs. Let us see how Davison's method works.

Let $G(a_1, \ldots, a_n)$ be the largest integer not representable as a linear combination of $a_1, \ldots, a_n$ in positive integers. Notice that $G(a_1, \ldots, a_n)$

$= g(a_1, \ldots, a_n) + \sum_{i=1}^{n} a_i$. Davison's algorithm actually computes the integer $G(a_1, a_2, a_3)$. Let $d_{12} = (a_1, a_2)$, $d_{13} = (a_1, a_3)$ and $d_{23} = (a_2, a_3)$. By Johnson's result (see Theorem 2.3.1), we have

$$G(a_1, a_2, a_3) = G(a_1/d_{12}d_{13}, a_2/d_{12}d_{23}, a_3/d_{13}d_{23})d_{12}d_{13}d_{23}.$$

Thus, we may assume that a_1, a_2 and a_3 are pairwise relatively prime.

Davison's Algorithm

Let $1 < a < b < c$ be pairwise relatively prime non-negative integers.

(1) Solve $bs \equiv c \bmod a$ with $0 < s < a$

If $bs < c$ **then** c is dependent on a and b and

$$g(a, b, c) = G(a, b, c) - a - b - c = ab + c - a - b - c = ab - a - b \text{ and STOP.}$$

(2) Use the Euclidean algorithm on the pair (s, a)

$$\begin{aligned} a &= a_1 s + r_1, \\ s &= a_2 r_1 + r_2, \\ r_1 &= a_3 r_2 + r_4, \\ &\vdots \\ r_{m-2} &= a_m r_{m-1} + r_m, \end{aligned}$$

where $s := r_0 > r_1 > r_2 > \cdots r_{m-1} = 1 > r_m = 0$.

(3) Let $q_{i+1} = a_{i+1}q_i + q_{i-1}$ for $i = 2, \ldots, m$ with $q_0 = 1$ and $q_1 = a_1$ and find k so that $r_{2k}/q_{2k} < c/b < r_{2k-2}/q_{2k-2}$ (note that $k \geq 1$ since $bs > c$).

(4) Set $\Phi(t) = \frac{r_{2k-2} - t r_{2k-1}}{q_{2k-2} - t q_{2k-1}}$ and use binary search to find the value t^* that satisfies $\Phi(t^*) < c/b < \Phi(t^* - 1)$ where $1 \leq t^* \leq a_{2k}$ (this is possible since the function Φ strictly decreases on the interval $[0, a_{2k}]$).

(5) Set $x' = r_{2k-2} - (t^* - 1)r_{2k-1}$, $y' = q_{2k-2} - (t^* - 1)q_{2k-1}$ and $x'' = r_{2k-2} - t^* r_{2k-1}$, $y'' = q_{2k-2} - t^* q_{2k-1}$. Then, $g(a, b, c) = G(a, b, c) - a - b - c = \max\{bx' + cq_{2k-1}, cy'' br_{2k-1}\} - a - b - c$ and STOP.

Notice that the number of elementary operations required in steps **1,2,3** and **4** (resp. in step **5**) is $O(\log a)$ (resp. $O(1)$). Also note the number of elementary operations needed, to assume that integers a, b and c are pairwise relatively primes, is $O(\log b)$. Thus, Davison's algorithm runs in $O(\log b)$ operations for all inputs.

Example 1.1.2 Let us compute $g(5, 7, 11)$ by using Davison's method.

(1) Let $s = 3$ be the unique integer $1 \leq s < 5$ such that $7s \equiv 11 \bmod 5$.

(2) The Euclidean algorithm gives: $a_1 = 1, a_2 = 1, a_3 = 2$, $r_0 = s = 3, r_1 = 2, r_2 = 1$ and $r_3 = 0$.

(3) $q_0 = 1, q_1 = a_1 = 1, q_2 = 2$ and $q_3 = 5$. Thus, with $k = 1$ we have $\frac{1}{2} < \frac{11}{7} < 3$.

(4) Trivially, $t^* = 1$ (since $1 \leq t^* \leq a_2 = 1$).

(5) $x' = 3, x'' = 1, y' = 1$ and $y'' = 2$. Thus, $g(5, 7, 11) = G(5, 7, 11) - 23 = \max\{32, 36\} - 23 = 13$.

1.1.3 Killingbergtrø's method

Killingbergtrø [236] has proposed a new approach to study **FP** when $n = 4$. This method is based on constructing a *cube-figure* from which information for **FP** is obtained. Killingbergtrø presented such a method by means of an arbitrary chosen case (when $a_1 = 103, a_2 = 133, a_3 = 165$ and $a_4 = 228$) and argued that it can be applied for any $n \geq 3$.

Let us consider Killingbergtrø's method for three arbitrary integers a_1, a_2 and a_3. The main idea is to construct a figure made out of a special set of unit squares in the positive quadrant.

Killingbergtrø's Algorithm

Let L_1 (resp. L_2 and L_3) be the least integer such that $L_1 a_1$ (resp. $L_2 a_2$ and $L_3 a_3$) is representable by a non-negative integer combination of $\{a_2, a_3\}$ (resp. representable by $\{a_1, a_3\}$ and by $\{a_1, a_2\}$.)

Suppose that, $a_1 L_1 = (a_2, a_3) \cdot (p_1, p_2)$, for some positive integers p_1, p_2 and denote by (x, y)-square the unit square with vertices $x, x + 1, y$ and $y + 1$.

Let $C = \{$all unit squares in the positive quadrant $\}$, $C_1 = \{(x, y)$-squares with $x > p_1$ and $y > p_2\}$, $C_2 = \{(x, y)$-squares with $x > L_2\}$ and $C_3 = \{(x, y)$-squares with $y > L_3\}$.

Let $\mathcal{R}[a_1, a_2, a_3] := C \setminus \{C_1 \cup C_2 \cup C_3\}$; see Fig. 1.1. $\mathcal{R}[a_1, a_2, a_3]$ is called a *cube-figure*.

Let BLC be the set of all integers points $c = (c_1, c_2)$ such that c is the bottom-left corner of a square belonging to $\mathcal{R}[a_1, a_2, a_3]$. Then,

$$g(a_1, a_2, a_3) = \max\{c_1a_2 + c_2a_3 | (c_1, c_2) \in BLC\} - a_1.$$

The proof for the correctness of Killingbergtrø's method is based on the following remark.

Remark 1.1.3 *(a) The area of* $\mathcal{R}[a_1, a_2, a_3]$ *is equal to* a_1 *and (b)* $\{c_1a_2 + c_2a_3 \bmod a_1 | (c_1, c_2) \in BLC\} = \{0, \ldots, a_1 - 1\}$.

Example 1.1.4 Let $a_1 = 5, a_2 = 7$ and $a_3 = 11$. Then, $5(5) = 2(7) + 1(11)$, $3(7) = 2(5) + 1(11)$ and $2(11) = 3(5) + 1(7)$. So, $(p_1, p_2) = (2, 1)$, $L_2 = 3$ and $L_3 = 2$, (the cube-figure $\mathcal{R}[5, 7, 11]$ is showed in Fig. 1.2).

Thus, the set of bottom-left corners in $\mathcal{R}[5, 7, 11]$ is $\{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0)\}$ and $g(5, 7, 11) = (1, 1) \cdot (7, 11) - 5 = 18 - 5 = 13$.

Example 1.1.5 We give the example, for $n = 4$, given in [236] and that Killingbergtrø was based on for presenting the remainder figure

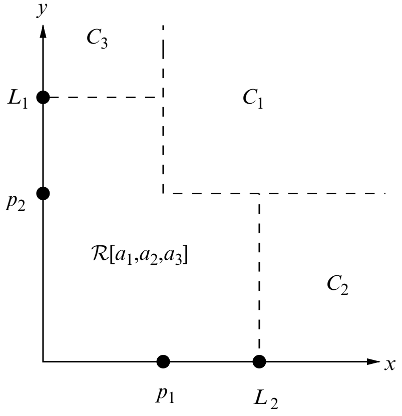

Figure 1.1: $\mathcal{R}[a_1, a_2, a_3]$.

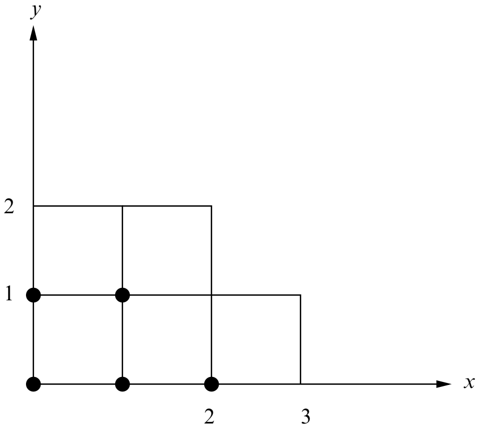

Figure 1.2: $\mathcal{R}[5,7,11]$ where bottom-left corners are bolded.

approach. Let $a_1 = 103, a_2 = 133, a_3 = 165$ and $a_4 = 228$. In this case, the cube-figure, $\mathcal{R}$', is formed by cubes, see Fig. 1.3. Notice that the volume of $\mathcal{R}$' is equal to 103. The set of corners (nearest vertex to the origin) of the cubes with three visible faces (these cubes are shaded in Fig. 1.3) is given by $\{(1,4,3),(3,1,3),(3,0,5),(6,4,0),(6,1,2),(8,0,2)\}$. Among all these, corner $(3,0,5)$ gives the greatest number in the dot product $(3,0,5)\cdot(133,165,228)$. Thus, $g(103,133,165,228) = (3,0,5)\cdot(133,165,228) - 103 = 1539 - 103 = 1436$.

We notice that the complexity of Killingbergtrø's method depends very much on how efficiently one can find the integers L_i. In Theorem 2.2.3 integers L_is are used for giving an explicit formula for $g(a_1,a_2,a_3)$ and in Claim 8.4.3 their value are calculated.

1.2 General algorithms

In this section, we shall present different methods that solve **FP** for any $n \geq 4$.

1.2.1 Scarf and Shallcross' method

Scarf and Shallcross [386] related **FP** to an area concerning maximal closed sets containing no interior lattice points. A body represented by $\{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\}$ where A is a matrix, is a *maximal lattice free body* if it contains no lattice points in its interior and if any strictly larger body

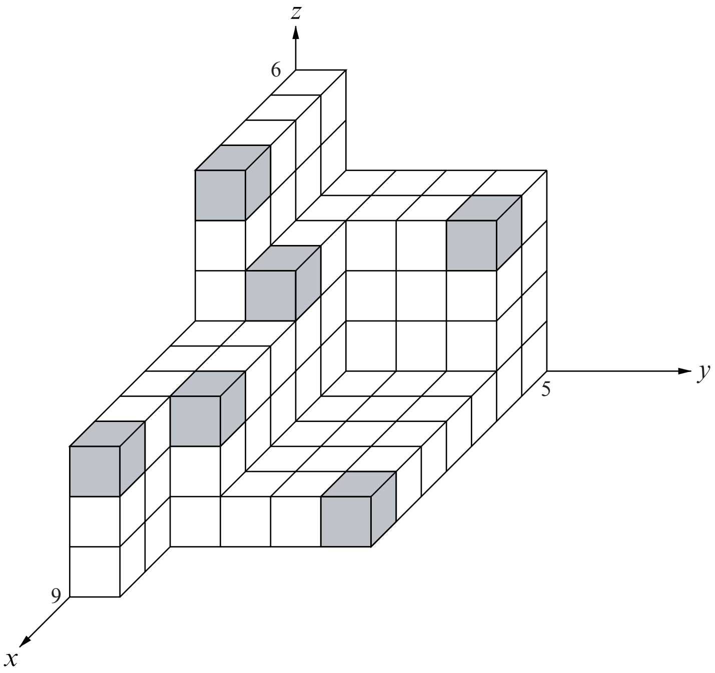

Figure 1.3: Cube-figure $\mathcal{R}$'.

obtained by relaxing some of the inequalities does contain an interior lattice point. Scarf and Shallcross proved that if they can maximize a linear function over the set of **b**s yielding maximal lattice free bodies for a matrix A of size $(n \times n - 1)$ then they can solve **FP**.

Scarf and Shallcross' Algorithm

Let $\mathbf{a} = (a_1, \ldots, a_n)$ and let A be a matrix of size $(n \times n - 1)$, whose columns generate the $(n-1)$-dimensional lattice of $\mathbf{h}$ satisfying $\mathbf{a} \cdot \mathbf{h} = 0$ (the set of solutions $\mathbf{h}$ lie on a hyperplane)

Note that in this case the bodies $\{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\}$ will be simplices that are non-empty if $\mathbf{a} \cdot \mathbf{b} \geq 0$.

$$g(a_1, \ldots, a_n) = \max\{\mathbf{a} \cdot \mathbf{b} | \mathbf{b} \text{ is integral and } \{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\} \text{ contains no lattice points}\}.$$

Proof for the exactness of Scarf and Shallcross' Method. Observe that if $\mathbf{b}$ is an integer vector such that $\{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\}$ contains no lattice points, then $f = \mathbf{a} \cdot \mathbf{b}$ cannot be written as $\mathbf{a} \cdot \mathbf{h}$ with $\mathbf{h}$ non-negative vector. Otherwise, $0 = \mathbf{a} \cdot (\mathbf{b} - \mathbf{h})$ so that $\mathbf{b} - \mathbf{h}$ is in the $(n-1)$-dimensional lattice generated by the columns of A. Thus, $\mathbf{b} - \mathbf{h} = A\alpha$ for some integrals α and therefore the set $\{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\}$ contains a lattice point, which is a contradiction.

Coversely, if $\mathbf{b}$ is an integral vector such that $\{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\}$ contains a lattice point α, then $f = \mathbf{a} \cdot \mathbf{b} = \mathbf{a} \cdot (\mathbf{b} - A\alpha)$ with $\mathbf{b} - A\alpha$ a non-negative integer vector. Finally, since $(a_1, \ldots, a_n) = 1$ every integer f can be written as $\mathbf{a} \cdot \mathbf{b}$ for some integral $\mathbf{b}$. Hence, by the above observation, $g(a_1, \ldots, a_n)$ is the maximal value of $\mathbf{a} \cdot \mathbf{b}$ for those integrals $\mathbf{b}$ such that $\{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\}$ is free of lattice points. □

Example 1.2.1 Let $a_1 = 3$ and $a_2 = 5$. Since $(3, 5) = 1$ then the set of vectors $\mathbf{h} = (h_1, h_2)$ satisfying that $(3, 5) \cdot (h_1, h_2) = 0$ is given by $(\pm 5r, \mp 3r)$ where $r = 0, 1, 2, \ldots$. The 1-dimensional lattice generated by vector $\mathbf{h}$ is illustrated in Fig. 1.4.

Now, the one column matrix $A = \begin{pmatrix} -5 \\ 3 \end{pmatrix}$ generates the integer lattice of $\mathbf{h}$. So, we want to find integral $\mathbf{b} = (b_1, b_2)$ such that

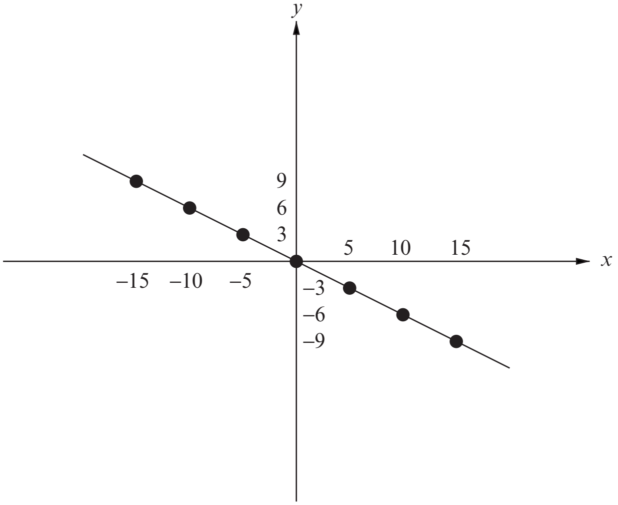

Figure 1.4: Lattice generated by the set of solutions of $(3, 5) \cdot (h_1, h_2) = 0$.

$$\begin{pmatrix} -5 \\ 3 \end{pmatrix} \mathbf{x} \leq \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \tag{1.3}$$

is free of lattice points and $(3,5) \cdot (b_1, b_2)$ is maximal. From, eqn (1.3) we have that $-\frac{b_1}{5} \leq x \leq \frac{b_2}{3}$ and thus $0 < -b_1 < 5$ and $0 < b_2 < 3$ since the corresponding simplex must not have lattices points. From this, $(3,5) \cdot (b_1, b_2)$ is maximal when $(b_1, b_2) = (-1, 2)$, obtaining that $g(3,5) = (3,5) \cdot (-1,2) = -3 + 10 = 7$.

Scarf and Shallcross used the above approach to obtain an algorithm for $g(a_1, a_2, a_3)$. Their method used the existence of a particular transformation so that the matrix A has a certain sign pattern and thus identifying the maximal lattice free bodies associated with A.

1.2.2 Heap and Lynn method

A matrix $B = (b_{i,j})$, $1 \leq i, j \leq m$, is called *non-negative* (resp. *positive*) if $b_{i,j} \geq 0$ (resp. if $b_{i,j} > 0$). A positive matrix B is denoted by $B > 0$. A $(n \times n)$ matrix B is called *reducible* if there exists an $(n \times n)$ permutation matrix P such that

$$PBP^T = \begin{bmatrix} B_{1,1} & B_{1,2} \\ 0 & B_{2,2} \end{bmatrix},$$

where $B_{1,1}$ is an $(r \times r)$ submatrix and $B_{2,2}$ is an $(n-r) \times (n-r)$ submatrix. If no such permutation matrix exists, then B is called *irreducible*[5]; see Appendix B.6 where some motivations for the study of such matrices are explained.

An irreducible, non-negative matrix B is *primitive* if $B^t > 0$ for some integer $t \geq 1$ (and hence, it can be shown, for all integers greater than t). The least integer $\gamma(B)$ such that $B^{\gamma(B)} > 0$ is called the *index of primitivity* of B.

Heap and Lynn [188] used graph-theoretic techniques to show that **FP** is equivalent to computing the index of primitivity of a matrix B of order $a_n + a_{n-1} - 1$; thereby providing a feasible algorithm for the computation of $g(a_1, \ldots, a_n)$. Let us look at this in more detail.

Let $B = (b_{ij})$ be a real $(m \times m)$ matrix. We define a directed graph[6] $G(B)$, of B, as the graph having vertex set $\{1, \ldots, m\}$ and

[5] The concepts of irreducible and reducible non-negative matrices have great importance in the theory of *Markov chains*; see [233, 298].

[6] This kind of directed graphs have been used extensively in analysing the matrix properties of matrix equations defined from elliptic (and parabolic) partial differential equations; see for instance [465, Chapter 6].

directed edge from i to j if and only if $b_{ij} \neq 0$; see Appendix B.2 for graph-theory definitions. There is a strong connection[7] between *strongly connectedness* of $G(B)$ and $\gamma(B)$ that Heap and Lynn [187] used to establish the following two lemmas.

Lemma 1.2.2 *[187] Let B be a primitive matrix and let $0 < a_1 < \cdots < a_k$ be the distinct lengths of all* elementary *circuits of $G(B)$. Then, $(a_1, \ldots, a_n) = 1$ and the length L, of any circuit of $G(B)$ can be expressed in the form $L = \sum_{i=1}^{n} x_i a_i$ with $x_i \geq 0$ for all i.*

The proof of this lemma is given in Appendix B.6 (*cf.* Lemma B.6.5).

Lemma 1.2.3 *[187] Let B be a primitive matrix and let $a_1 < \cdots < a_n$ be the distinct lengths of the elementary circuits of $G(B)$. Then,*

$$g(a_1, \ldots, a_n) \leq \gamma(B) - 1.$$

Proof. Since the diagonal elements of $B^{\gamma(B)+m}$ are positive for all $m \geq 0$ then by Lemma B.6.3, there are circuits in $G(B)$ of length $\gamma(B) + m$. The result follows by using Lemma 1.2.2 and the definition of $g(a_1, \ldots, a_n)$. □

Given integers $1 \leq a_1 < \cdots < a_n$, Heap and Lynn [188] defined the *Frobenius (directed) graph*, $G(B) = G(a_1, \ldots, a_n)$, obtained from matrix $B = (b_{i,j})$, $1 \leq i, j \leq s = a_n + a_{n-1} - 1$, where

$$b_{i,j} = \begin{cases} 1 & \text{if } j = i+1 \text{ with } i = 1, \ldots, s-1 \text{ and } i \neq a_{n-1}, \\ 1 & \text{if } j = 1 \text{ with } i = s \text{ or } a_t,\ t = 1, \ldots, n-1, \\ 1 & \text{if } i = 1 \text{ and } j = a_{n-1} + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the elementary circuits of $G(a_1, \ldots, a_n)$ have lengths $a_1, \ldots, a_n$; see Fig. 1.5. By using the same technique as in Lemma 1.2.3 and a heavy analysis of the Frobenius graph, Heap and Lynn [188] obtained the following result (see also [122] where the same idea has been exploited).

Theorem 1.2.4 *[188] Let B be the matrix defined as above. Then,*

$$g(a_1, \ldots, a_n) = \gamma(B) - 2a_n + 1.$$

The above theorem may yield to an algorithm that finds the Frobenius number. Clearly, the complexity of such an algorithm depends on

[7] See Appendix B.6 for a detailed explanation of this relation.

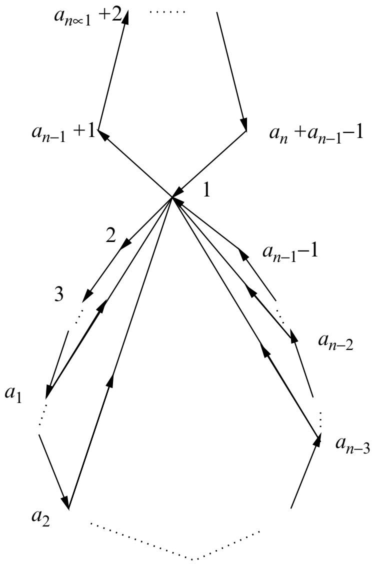

Figure 1.5: The Frobenius graph $G(a_1, \ldots, a_n)$.

how efficiently one is able to compute the index of primitivity of a matrix[8].

Example 1.2.5 Let $a_1 = 3$ and $a_2 = 5$. We calculate $\gamma(B)$ below and obtaining $g(3, 5) = 16 - 2(5) + 1 = 7$.

$$B = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

[8] See Appendix B.6.2 where a procedure to calculate the primitivity index of a matrix is explained.

$$B^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$B^4 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$B^8 = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$B^{12} = \begin{pmatrix} 2 & 3 & 1 & 3 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 2 & 0 & 1 \\ 3 & 1 & 1 & 1 & 1 & 2 & 0 \\ 2 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 2 & 0 & 2 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 & 1 \\ 3 & 1 & 1 & 1 & 1 & 2 & 0 \end{pmatrix}$$

$$B^{14} = \begin{pmatrix} 3 & 3 & 2 & 3 & 2 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 & 0 & 1 \\ 3 & 1 & 1 & 1 & 1 & 2 & 0 \\ 1 & 2 & 1 & 2 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 1 & 1 \end{pmatrix}$$

obtaining

$$B^{15} = \begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 2 & 3 \\ 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 3 & 1 & 3 & 1 & 3 & 1 \\ 3 & 1 & 2 & 1 & 2 & 2 & 0 \\ 1 & 3 & 1 & 3 & 1 & 1 & 2 \\ 3 & 1 & 2 & 1 & 2 & 1 & 1 \\ 4 & 3 & 1 & 3 & 1 & 3 & 1 \end{pmatrix}$$

$$B^{16} = \begin{pmatrix} 6 & 3 & 3 & 3 & 3 & 3 & 2 \\ 2 & 3 & 1 & 3 & 1 & 1 & 1 \\ 2 & 4 & 3 & 4 & 3 & 1 & 3 \\ 2 & 3 & 1 & 3 & 1 & 2 & 2 \\ 3 & 1 & 3 & 1 & 3 & 1 & 1 \\ 4 & 3 & 1 & 3 & 1 & 2 & 1 \\ 2 & 4 & 3 & 4 & 3 & 1 & 3 \end{pmatrix}.$$

Notice that $G(B^k)$ is the directed graph obtained by considering all paths of $G(B)$ of length exactly $k \geq 1$. Thus, $\gamma(B)$ is the smallest integer such that there is a directed edge for each pair of vertices in $G(B^{\gamma(B)})$; see Lemma B.6.3. So, $G(B^{\gamma(B)})$ is the diagraph where every pair of vertices is joined by two edges (one in each direction). Figure. 1.6 illustrates $G(B) = G(3,5)$ and $G(B^2)$.

Heap and Lynn [189] reduced the computation time of their algorithm by defining another directed graph called the *Frobenius minimal graph* (denoted by $G(\bar{B})$), obtained, from matrix $\bar{B} = (\bar{b}_{i,j})$ (which is

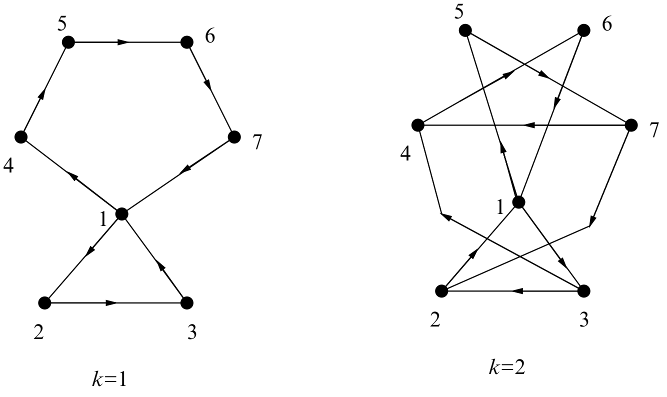

Figure 1.6: $G(B)$ and $G(B^2)$.

only of order a_n) defined as follows

$$\bar{b}_{i,j} = \begin{cases} 1 & \text{if } j = i+1,\ i = 1, \ldots, a_n - 1, \\ 1 & \text{if } i - j = a_s - 1 \text{ for some } 1 \le s \le n, \\ 0 & \text{otherwise.} \end{cases}$$

Example 1.2.6 Let $a_1 = 3, a_2 = 5$ and $a_3 = 8$. Then, matrix $\bar{B}$ has the form

$$\bar{B} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Figure 1.7 illustrates the corresponding minimal Frobenius graph $G(\bar{B})$.

Theorem 1.2.7 *[189] Let $\bar{B}$ be the matrix defined as above. Then,*

$$g(a_1, \ldots, a_n) = \gamma(\bar{B}) - a_n.$$

The proof of Theorem 1.2.7 is based in the following easy Lemma and Corollary.

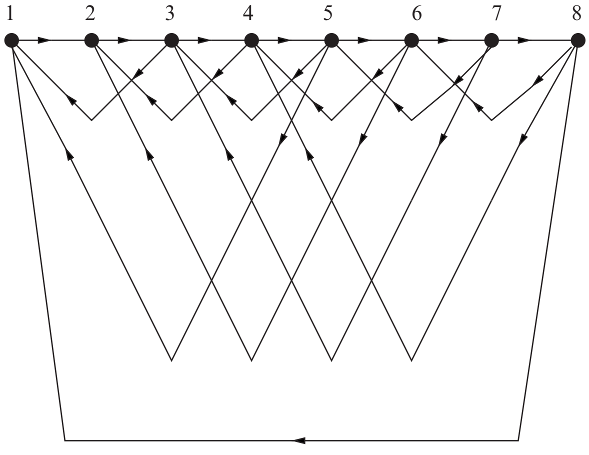

Figure 1.7: The minimal Frobenius graph when $a_1 = 3, a_2 = 5$ and $a_3 = 8$.

Lemma 1.2.8 *[189]*

(a) There exists a unique path from vertex i to vertex j, $i < j$ in $G(\bar{B})$.

(b) There are only elementary circuits of length a_i in $G(\bar{B})$.

(c) Each vertex in $G(\bar{B})$ lies on an elementary circuit of length a_i, $i = 1, \ldots, n$.

Corollary 1.2.9 *[189] $\bar{B}$ is primitive.*

Proof. Since $G(\bar{B})$ is strongly connected (there is an elementary circuit of length a_i) then $\bar{B}$ is irreducible. The result follows from Lemmas 1.2.8 and 1.2.2. □

Proof of Theorem 1.2.7. We first show that

$$g(a_1, \ldots, a_n) + a_n \leq \gamma(\bar{B}). \tag{1.4}$$

Notice that any path from vertex 1 to vertex a_n must consist of an elementary path of length $a_n - 1$ by Lemma 1.2.8 (a) plus a number of circuits, that is, its length is necessarily of the form

$$L = a_n - 1 + \sum_{i=1}^{n} x_i a_i,$$

where $x_i \geq 0$. Hence, there does not exist a path from vertex 1 to vertex a_n of length $g(a_1, \ldots, a_n) + a_n - 1$. And, eqn (1.4) follows from Lemma 1.2.2. Now, we shall show that

$$g(a_1, \ldots, a_n) + a_n \geq \gamma(\bar{B}). \tag{1.5}$$

To this end, we notice that any two vertices i and j of $G(\bar{B})$ can be connected by a path of length at most $a_n - 1$, since there exists an elementary circuit of length a_n that contains all the vertices of the graph. Since vertex i lies on elementary circuits of all lengths a_s, $1 \leq s \leq n$, there is a path connecting vertex i to vertex j of length

$$a_n - 1 - \delta + \sum_{i=1}^{n} x_i a_i$$

for all $a_i \geq 0$ and some $\delta \geq 0$. Given $\mu \geq 0$, we may choose the $\{a_i\}$ such that $\sum_{i=1}^{n} x_i a_i = g(a_1, \ldots, a_n) + 1 + \delta + \mu$, and hence there exist paths connecting an arbitrary vertex i to an arbitrary vertex j of lengths

$$a_n + g(a_1, \ldots, a_n) + \mu$$

for all $\mu \geq 0$. Thus, eqn (1.5) follows from Lemma 1.2.2 by taking $\mu = 0$.

□

1.2.3 Greenberg's Algorithm

Greenberg [171] gave an algorithm, to compute $g(a_1, \ldots, a_n)$, by using mathematical programming ideas. Greenberg's algorithm is based in the following result.

Theorem 1.2.10 *Let $a_1, \ldots, a_n$ and L be positive integers and let*

$$E(L) = \min\left\{\sum_{j=1}^{n} x_j a_j | \sum_{j=2}^{n} x_j a_j \equiv L \bmod a_1,\ x_j \geq 0\right\}.$$

Then, there exist integers $x_j \geq 0$ such that $\sum_{j=1}^{n} x_j a_j = L$ if and only if $L \geq E(L)$. Moreover, there are no non-negative integers x_i such that $\sum_{j=1}^{n} x_j a_j = E(L) - sa_1$ for each $s \in \{1, 2, \ldots, (E(L) - L)/a_1\}$ and any $L \in \{1, \ldots, a_1 - 1\}$ and these are the only equations in the form $\sum_{j=1}^{n} x_j a_j = L$ without solutions in non-negative integers x_i for each $L \in \{1, \ldots, a_1 - 1\}$.

The proof of Theorem 1.2.10 easily follows from Lemma 3.1.6. Note that L and $E(L)$ are in the same residue class modulo a_1. Furthermore, if $E(L)$ is known, with solution $x_1 = 0$, $x_j = x'_j$ for $j \geq 2$ and $L \geq E(L)$ then $\sum_{j=1}^{n} x_j a_j = L$ with $x_1 = (E(L) - L)/a_1$ and $x_j = x'_j$ for $j \geq 2$. With the above theorem, the complete characterization of all solutions and non-solutions to $\sum_{j=1}^{n} x_j a_j = L$ is obtained from the function $E(L)$ and thus

$$g(a_1, \ldots, a_n) = \max\{E(L) | L = 1, \ldots, a_1 - 1\} - a_1.$$

Example 1.2.11 Let $a_1 = 5, a_2 = 7$ and $a_7 = 9$. We compute $E(j) = \min\{5x_1 + 7x_2 + 9x_3 | 7x_2 + 9x_3 \equiv j \bmod 5,\ x_1, x_2, x_3 \geq 0\}$ for each $j = 1, \ldots, 4$. We have that $E(1) = 16$ (with $x_1 = 0, x_2 = x_3 = 1$), $E(2) = 7$ (with $x_1 = x_3 = 0, x_2 = 1$), $E(3) = 18$ (with $x_1 = x_2 = 0, x_3 = 2$) and $E(4) = 9$ (with $x_1 = 0 = x_2 = 0, x_3 = 1$). Thus, $g(5, 7, 9) = \max\{16, 7, 18, 9\} - 5 = 13$.

1.2.4 Nijenhuis' Algorithm

Nijenhuis [309] provided an algorithm to compute $g(a_1, \ldots, a_n)$ by constructing, in a graph with weighted edges, a path of minimal weight from one vertex to all others.

Nijenhuis' Algorithm

Let D be the directed graph (with multiple edges and loops) defined as follows: the vertices of D are $\{v_0, \ldots, v_{a_1-1}\}$ and for each $0 \leq p \leq a_1 - 1$ there is a directed edge from vertex v_p to vertex v_{p+a_i} for all $1 \leq i \leq n$ where $p + a_i$ is computed modulo a_1, the *weight* of this edge is a_i.

Let w_p be the minimum of all directed weighted paths from v_0 to v_p (the weight of a directed path is just the sum of the weights of its edges). Then,

$$g(a_1, \ldots, a_n) = \max_{1 \leq p \leq a_1 - 1} \{w_p\} - a_1.$$

It turns out that w_p is exactly the smallest element of the set of integers representable as a non-negative linear combination of $a_1, \ldots, a_n$ congruent to p modulo a_1. Thus, the correctness of Nijenhuis' algorithm follows by using Theorem 3.1.6. Nijenhuis' algorithm runs in time of order $O(na_{\min} \log a_{\min})$ where $a_{\min} = \min\limits_{i=1,\ldots,n} \{a_i\}$.

Example 1.2.12 Let $a_1 = 5$, $a_2 = 7$ and $a_3 = 8$. The corresponding directed graph is shown in Fig. 1.8. We obtain that $w_0 = 5$, $w_1 = 16$, $w_2 = 7$, $w_3 = 8$ and $w_4 = 14$. Thus, $g(5, 7, 8) = \max\{w_0, w_1, w_2, w_3, w_4\} - a_1 = 16 - 5 = 11$.

1.2.5 Wilf's Algorithm

Wilf [480] gave an algorithm to compute $g(a_1, \ldots, a_n)$ in $O(na_n^2)$ operations; see also [206]. Wilf's procedure is as follows.

Wilf's Algorithm

Form a circle of a_n lights, labelled by $l_0, l_1, \ldots, l_{a_n-1}$ (initially light l_0 is on and the others off).

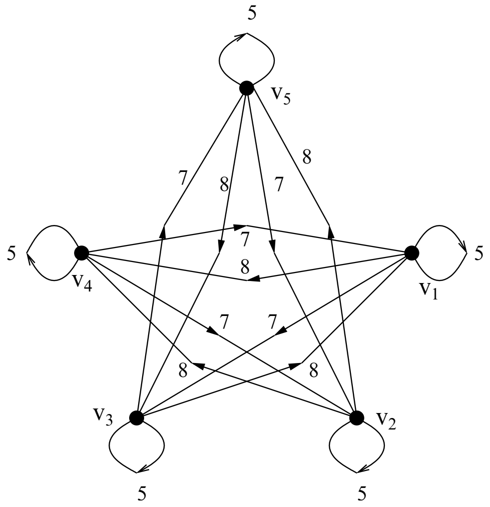

Figure 1.8: Nijenhuis' directed graph when $a_1 = 5, a_2 = 7$ and $a_3 = 8$.

Sweep around the circle starting from l_0 (clockwise) and as we encounter each light we will turn it on if any of the n lights that are situated at distance $a_1, \ldots, a_n$ back (*i.e.* in counterclockwise sense) from the present one is on, we leave it on if it was already on, otherwise we leave it off. The process halts as soon as any a_1 consecutive lights are on.

Let $s(l_{a_i})$ be the number of times light l_{a_i} is visited during the procedure and let l_r be the last visited off light just before ending the process. Then,

$$g(a_1, \ldots, a_n) = r + (s(l_r) - 1)a_n.$$

The proof for the correctness of Wilf's algorithm follows from Brauer and Shockley's result (*cf.*, Theorem 3.1.6).

Example 1.2.13 Let $a_1 = 5, a_2 = 6$ and $a_3 = 7$. In Fig. 1.9 the procedure is represented where the arrow marks the encountered light during the sweeping and the full (resp. empty) circles represents the on (resp. off) lights. So, l_2 is the last visited off light and thus $g(5, 6, 7) = 2 + (s(l_2) - 1)7 = 2 + (2 - 1)7 = 9$.

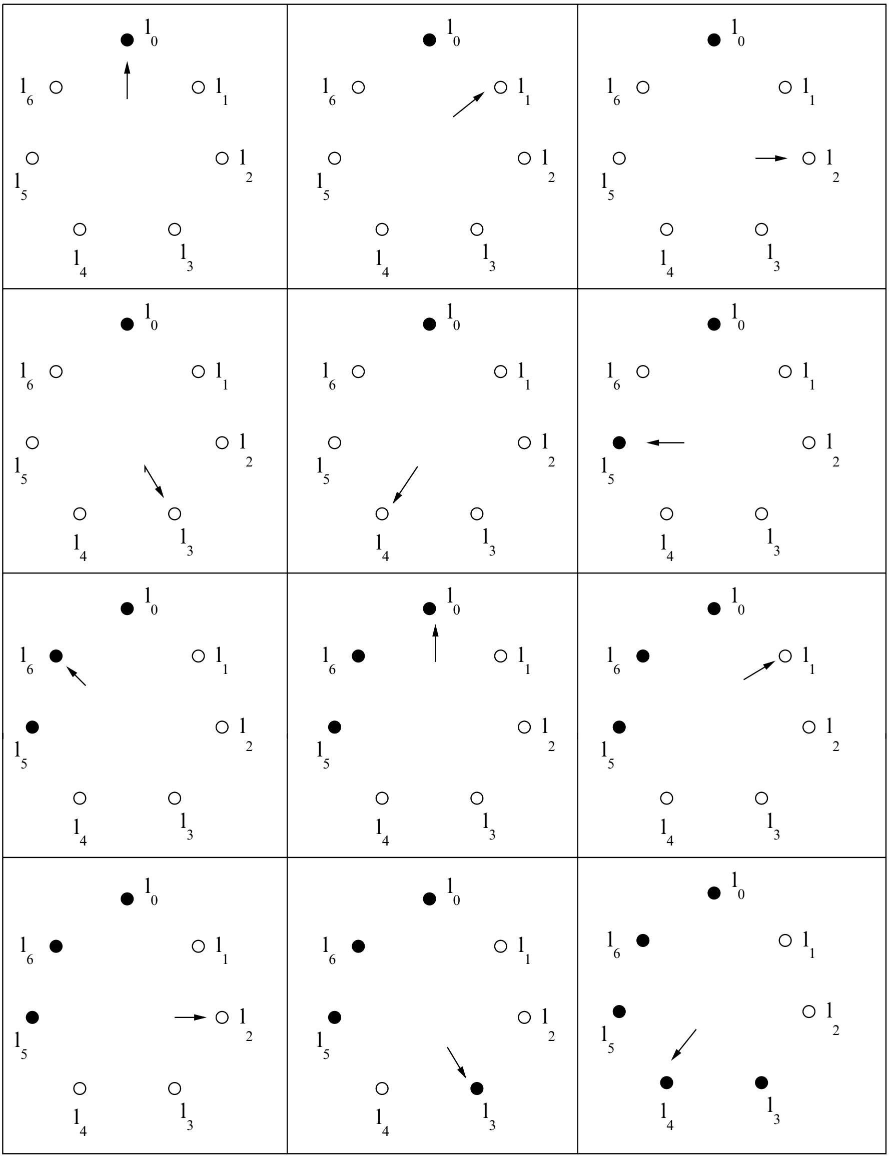

Figure 1.9: Circle of 7 lights.

1.2.6 Kannan's method

Kannan [228] gave a polynomial time algorithm for **FP** for any fixed n; see also [229]. Kannan has done this by first proving a beautiful exact relation between **FP** and a geometric concept called the *covering* *radius.* We recall that for a closed bounded convex set P of non-zero volume in $\mathbb{R}^n$ and a lattice L of dimension n also in $\mathbb{R}^n$, the least positive real t so that $tP+L$ equals $\mathbb{R}^n$ is called the *covering radius* of P with respect to L (denoted by $\mu(P,L)$). That is, the covering radius of a polytope P with respect to a lattice L is the least amount t by that we must 'blow up' P and one copy of P placed at each lattice point so that all the space is covered.

Theorem 1.2.14 *[228] Let* $L = \{(x_1,\ldots,x_{n-1}) | x_i$ *integers and* $\sum_{i=1}^{n-1} a_i x_i \equiv 0 \bmod a_n\}$ *and* $S = \{(x_1,\ldots,x_{n-1}) | x_i \geq 0$ *reals and* $\sum_{i=1}^{n-1} a_i x_i \leq 1\}$*. Then,*

$$\mu(S,L) = g(a_1,\ldots,a_n) + a_1 + \cdots + a_n,$$

where $\mu(S,L)$ *is the covering radius of* S *with respect to* L*.*

In [228], Kannan then developed a polynomial time algorithm for finding the covering radius of any polytope in a fixed number of dimensions yielding to a polynomial time algorithm for finding $g(a_1,\ldots,a_n)$ for any fixed n. Unfortunately, Kannan's algorithm is doubly exponential on n and is likely not to be useful in practice.

Proof of Theorem 1.2.14. Let us first show that $\mu(S,L) \leq g(a_1,\ldots, a_n) + a_1 + \cdots + a_n$. Suppose that $y \in \mathbb{Z}^{n-1}$ and $\sum_{i=1}^{n-1} a_i y_i \equiv l \bmod a_n$. Let t_l be the smallest positive integer congruent to l modulo a_n, that is representable as a non-negative integer combination of $a_1,\ldots,a_{n-1}$. So, there exist integers $x_1,\ldots,x_n \geq 0$ such that $\sum_{i=1}^{n-1} a_i x_i = t_l = l + a_n x_n$; thus with $x' = (x_1,\ldots,x_{n-1})$, we have $(y-x') \in L$ and $(y-x') + t_l S$ contains $y - x' + x' = y$. Since this is true for any $y \in \mathbb{Z}^{n-1}$ and $t_l \leq g(a_1,\ldots,a_n) + a_n$ then $\mathbb{Z}^{n-1} \subseteq (g(a_1,\ldots,a_n)+a_n)S + L$. Further, it is clear that $\mathbb{R}^{n-1} \subseteq \mathbb{Z}^{n-1} + (a_1 + \cdots + a_n)S$. To see the latter, note that for $z \in \mathbb{R}^{n-1}$, we have $\lfloor z \rfloor = (\lfloor z_1 \rfloor, \ldots, \lfloor z_{n-1} \rfloor) \in \mathbb{Z}^{n-1}$ and $(z - \lfloor z \rfloor) \in (a_1 + \cdots + a_{n-1})S$. Hence,

$$\mathbb{R}^{n-1} \subseteq \mathbb{Z}^{n-1} + (a_1 + \cdots + a_{n-1})S \subseteq (g(a_1,\ldots,a_n) + a_1 + \cdots + a_{n-1})S + L.$$

We now show that $\mu(S,L) \geq g(a_1,\ldots,a_n) + a_1 + \cdots + a_n$. To this end, we first show, by contradiction, that $g(a_1,\ldots,a_n) + a_n$ is the smallest positive real t such that $tS + L$ contains $\mathbb{Z}^{n-1}$. So, suppose that it is not true, then for some $t' < g(a_1,\ldots,a_n) + a_n$, $t'S + L$ contains $\mathbb{Z}^{n-1}$. Then for any $l \in \{1,\ldots,a_n - 1\}$ pick a $y \in \mathbb{Z}^{n-1}$ such that $\sum_{i=1}^{n-1} a_i y_i \equiv l \bmod a_n$. Hence, y is in $t'S + x$ for some x in L, so $(y - x)$ is in $t'S$. But $\sum_{i=1}^{n-1} a_i(y_i - x_i) \equiv l \bmod a_n$ and $y_i - x_i \geq 0$ for all i implying that $t_l \leq t'$. Since this is true for any l then, by Theorem

3.1.6, we have that $g(a_1,\ldots,a_n) \le t' - a_n$ but $t' - a_n < g(a_1,\ldots,a_n)$ yielding a contradiction. Thus,

$$g(a_1,\ldots,a_n) + a_n = \min\{t | t > 0, \text{ real and } \mathbb{Z}^{n-1} \subseteq tS + L\}. \quad (1.6)$$

From eqn (1.6), we see that there exists $y \in \mathbb{Z}^{n-1}$ such that for any $x \in L$ with $y_i - x_i \ge 0$ for all i we have that $\sum_{i=1}^{n-1} a_i(y_i - x_i) \ge g(a_1,\ldots,a_n) + a_n$. Now, let ϵ be any real number with $0 < \epsilon < 1$ and consider the point $p = (p_1,\ldots,p_{n-1})$ defined by $p_i = y_i + (1-\epsilon)$ for all i. Suppose that q is any point of L such that $p_i \ge q_i$ for all i. Then, q_i are all integers, so we must have $q_i \le y_i$ for all i. So,

$$\begin{aligned}\sum_{i=1}^{n-1} a_i(p_i - q_i) &= (1-\epsilon)\sum_{i=1}^{n-1} a_i + \sum_{i=1}^{n-1} a_i(y_i - q_i)\\ &\ge (1-\epsilon)\sum_{i=1}^{n-1} a_i + g(a_1,\ldots,a_n) + a_n.\end{aligned}$$

Since this argument holds for any $\epsilon \in (0,1)$, we have $\mu \ge g(a_1,\ldots, a_n) + a_1 + \cdots + a_n$ and the result follows. □

In [346], we investigated Kannan's relation and found a max-min formula for $\mu(S, L)$. We explain this approach as it may lead to a more constructive proof for Theorem 1.2.14 that yields to a method for computing $g(a_1,\ldots,a_n)$. We write $\mu(\mathbf{x}) = \mu S(\mathbf{x})$ to denote a μ-dilated copy of S placed at point $\mathbf{x} = (x_1,\ldots,x_{n-1}) \in L$. We say that $\mu(\mathbf{x})$ *absorbs* point $\mathbf{x}'$ if $\mathbf{x}'$ lies in $\mu(\mathbf{x})$ where $x_i < x'_i$ for all i. In other words, point $\mathbf{x}'$ is *absorbed* by $\mu(\mathbf{x})$ if $\mathbf{x}'$ lies either in the interior or on the skewed facet of simplex $\mu(\mathbf{x})$.

Proposition 1.2.15 *The $(n-1)$-dimensional space is covered by μ-dilated copies of S placed at each point in L if and only if each point $\mathbf{x} \in \mathbb{Z}^{n-1}$ is absorbed by $\mu(\mathbf{x}')$ for some $\mathbf{x}' \in L$ with $x'_i < x_i$, $1 \le i \le n-1$.*

Proof. Assume that $\mathbb{R}^{n-1}$ is covered by μ-dilated copies of S and suppose that there is a point $\mathbf{x} \in \mathbb{Z}^{n-1}$, that is, $\mathbf{x}$ is not absorbed by any $\mu(\mathbf{x}')$ with $x'_i < x_i$ with $1 \le i \le n-1$. Then, one could find $0 < \epsilon < 1$ such that $(x_1 - \epsilon,\ldots,x_{n-1} - \epsilon)$ is not covered by any of the μ-dilated copies of S, which is a contradiction since the space is covered.

Now, for the converse, let $\mathbf{x} \in \mathbb{R}^{n-1}$. We shall show that $\mathbf{x}$ is covered by $\mu(\mathbf{x}')$ for some $\mathbf{x}' \in L$ with $x'_i < x_i$, $1 \le i \le n-1$. This is true if $\mathbf{x} \in \mathbb{Z}^{n-1}$ by hypothesis, so we assume that $x_k \notin \mathbb{Z}$ for some $1 \le$

$k \leq n-1$. Let x_i' be the smallest integers such that $x_i \leq x_i'$ for each $i = 1, \ldots, n-1$. Since $\mathbf{x}' \in \mathbb{Z}^{n-1}$ then it is absorbed by some $\mu(\bar{\mathbf{x}})$ with $\bar{x}_i < x_i'$, $1 \leq i \leq n-1$. But, by construction of $\mathbf{x}'$ and definition of absorption we have that $\bar{x}_i < x_i$. Thus, $\mathbf{x}$ is also absorbed by $\mu(\bar{\mathbf{x}})$. □

We have the following corollary of Proposition 1.2.15.

Corollary 1.2.16 *Let $\mu^*_{\mathbf{x}}$ be the smallest positive integer such that the point $\mathbf{x} \in \mathbb{Z}^{n-1}$ is absorbed by $\mu^*_{\mathbf{x}}(\mathbf{x}')$ for some $\mathbf{x}' \in L$ with $x_i' < x_i$, $1 \leq i \leq n-1$. Then,*

$$\mu(S, L) = \max_{\mathbf{x} \in \mathbb{Z}^{n-1}} \{\mu^*_{\mathbf{x}}\}.$$

Example 1.2.17 Let a and b positive integers such that $(a, b) = 1$. Then L (resp. S) is the set of points (resp. the segment) lying in the positive side of the real line as shown in Fig. 1.10. It is clear that the minimum integer t such that tS covers the interval $[0, b]$ is ab. Thus, $g(a, b) = \mu(S, L) - a - b = ab - a - b$ (yielding to an easy proof of Theorem 2.1.1).

Example 1.2.18 Let $a_1 = 3$, $a_2 = 4$ and $a_3 = 5$. The corresponding lattice L and simplex S are shown in Fig. 1.11(a). It is clear that $g(3, 4, 5) = 2$; and thus $\mu(L, S) = 14$. Figure 1.11(b) shows that $(14)S$ covers the plane while Fig. 1.11(c) shows that $(13)S$ does not.

A relation between **FP** and the covering radius was also studied by Scarf and Shallcross [386] in terms of maximal lattice free simplices.

1.3 Computational complexity of FP

In this section we show that **FP** is a difficult problem from the computational point of view.

Theorem 1.3.1 *[342]* **FP** *is $\mathcal{NP}$-hard under* Turing reductions.

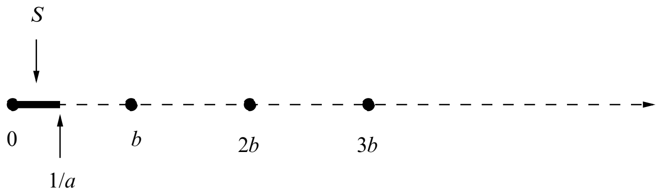

Figure 1.10: Covering radius in the one-dimensional case.

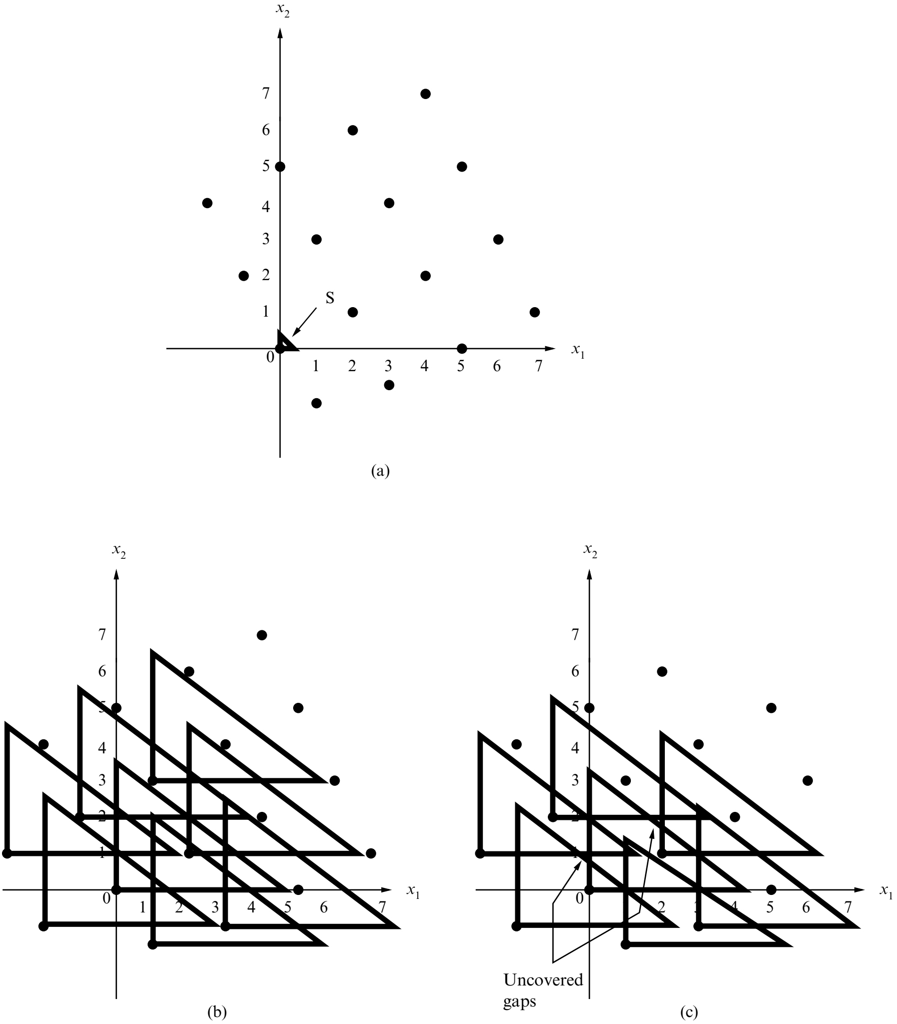

Figure 1.11: (a) L and S for $a_1 = 3$, $a_2 = 4$ and $a_3 = 5$, (b) translations of $(14)S$ and (c) translations of $(13)S$.

Theorem 1.3.1 is proved by giving a *Turing reduction* (see Appendix B.1 for computational complexity details) from the *Integer Knapsack* problem [9] (**IKP**) that is known to be an $\mathcal{NP}$-complete problem [322, page 376]; see also [3] and [283].

IKP Input: Positive integers $a_1, \dots, a_n$ and t.

[9] This is actually a particular case of the general *Knapsack* problem that is fully explained in Chapter 3.

Question: Do there exist integers $x_i \geq 0$, with $1 \leq i \leq n$ such that $\sum_{i=1}^{n} x_i a_i = t$?

In [342], it is proved that the following procedure that uses a hypothetical subroutine that solves **FP**, solves **IKP** in polynomial time. We assume that $r = (a_1, \ldots, a_n) = 1$, otherwise consider **IKP** with input $a'_i = \frac{a_i}{r}$, $i = 1, \ldots, n$ and $t' = \frac{t}{r}$.

```
Procedure A

Find $g(a_1, \ldots, a_n)$
If $t > g(a_1, \ldots, a_n)$ Then IKP is answered affirmatively
Else
      If $t = g(a_1, \ldots a_n)$ Then
         IKP is answered negatively
      Else
         Find $g(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1})$ where $\bar{a}_i = 2a_i$, $i = 1, \ldots, n$ and
         $\bar{a}_{n+1} = 2g(a_1, \ldots, a_n)+1$ (note that $(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}) = 1$)

         Find $g(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}, \bar{a}_{n+2})$ where
         $\bar{a}_{n+2} = g(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}) - 2t$

         IKP is answered affirmatively if and only if
         $g(\bar{a}_1, \ldots, \bar{a}_{n+2}) < g(\bar{a}_1, \ldots, \bar{a}_{n+1})$
```

In order to prove Theorem 1.3.1, we need the following Proposition.

Proposition 1.3.2 *Let b_i for each $i = 1, \ldots, n$ and $\bar{b}_i$ for each $i = 1, \ldots, n$ be the integers as defined in Procedure A. Then,*

$$g(\bar{b}_1, \ldots, \bar{b}_{n+1}) = 4g(b_1, \ldots, b_n) + 1.$$

Proof. Let g be an integer such that $g > 4g(b_1, \ldots, b_n) + 1$. Let $g' = g - \ell \bar{b}_{n+1}$ where $\ell \equiv g \ (mod\ 2)$. If $\ell = 0$ then

$$g' = g > 4g(b_1, \ldots, b_n) + 1 > 2g(b_1, \ldots, b_n).$$

Otherwise, if $\ell = 1$ then $g' = g - \bar{b}_{n+1} > 4g(b_1, \ldots, b_n) + 1 - (2g(b_1, \ldots, b_n) + 1) = 2g(b_1, \ldots, b_n)$.

Hence, $g' > 2g(b_1, \ldots, b_n)$ and since $g' \equiv 0 \ (mod\ 2)$ then g' is representable as a non-negative integer combination of $\bar{b}_1, \ldots, \bar{b}_n$. Therefore, g is also representable as a non-negative integer combination of $\bar{b}_1, \ldots, \bar{b}_{n+1}$.

We prove now by contradiction that $4g(b_1, \ldots, b_n) + 1$ is not representable as a non-negative integer combination of $\bar{b}_1, \ldots, \bar{b}_{n+1}$.

Suppose there exist integers $x_i \geq 0$, $1 \leq i \leq n+1$, such that $\sum_{i=1}^{n+1} x_i\bar{b}_i = 4g(b_1, \ldots, b_n) + 1$. Since $4g(b_1, \ldots, b_n) + 1 \not\equiv 0 \ (mod\ 2)$ then $x_{n+1} \geq 1$.

On the other hand, if $x_{n+1} \geq 2$ then $x_{n+1}\bar{b}_{n+1} > 4g(b_1, \ldots, b_n) + 1$ so $x_{n+1} \leq 1$. Therefore $x_{n+1} = 1$, thus

$$\sum_{i=1}^{n} x_i\bar{b}_i + \bar{b}_{n+1} = 4g(b_1, \ldots, b_n) + 1,$$

and

$$\sum_{i=1}^{n} x_i\bar{b}_i = 2g(b_1, \ldots, b_n),$$

then

$$\sum_{i=1}^{n} x_i b_i = g(b_1, \ldots, b_n), \text{ which is impossible.}$$

Hence, $4g(b_1, \ldots, b_n) + 1$ is the largest natural number that is not representable as a non-negative integer combination of $\bar{b}_1, \ldots, \bar{b}_{n+1}$. □

We may prove now Theorem 1.3.1.

Proof of Theorem 1.3.1. Let $t < g(b_1, \ldots, b_n)$. We claim that there exist integers $x_i \geq 0$, with $1 \leq i \leq n$, such that $\sum_{i=1}^{n} x_i b_i = t$ if and only if $g(\bar{b}_1, \ldots, \bar{b}_{n+2}) < g(\bar{b}_1, \ldots, \bar{b}_{n+1})$.

Assume that there exist integers $x_i \geq 0$, $1 \leq i \leq n$, such that $\sum_{i=1}^{n} x_i b_i = t$. So, $\sum_{i=1}^{n} x_i\bar{b}_i = 2t$ and since $\bar{b}_{n+2} = g(\bar{b}_1, \ldots, \bar{b}_{n+1}) - 2t$ then

$$g(\bar{b}_1, \ldots, \bar{b}_{n+1}) = \sum_{i=1}^{n+2} x_i\bar{b}_i.$$

Hence, $g(\bar{b}_1, \ldots, \bar{b}_{n+2}) < g(\bar{b}_1, \ldots, \bar{b}_{n+1})$.

Conversely, assume $g(\bar{b}_1, \ldots, \bar{b}_{n+2}) < g(\bar{b}_1, \ldots, \bar{b}_{n+1})$. By Proposition 1.3.2 we have, $g(\bar{b}_1, \ldots, \bar{b}_{n+1}) = 4g(b_1, \ldots, b_n) + 1 = \sum_{i=1}^{n+2} x_i\bar{b}_i$ for some integers $x_i \geq 0$, with $1 \leq i \leq n+2$.

Since $g(\bar{b}_1, \ldots, \bar{b}_{n+1})$ is not representable as a non-negative integer combination of $\bar{b}_1, \ldots, \bar{b}_{n+1}$ then $x_{n+2} \geq 1$. On the other hand, from

$$x_{n+2}\bar{b}_{n+2} = x_{n+2}\left(g(\bar{b}_1, \ldots, \bar{b}_{n+1}) - 2t\right),$$

and

$$2t < 2g(b_1, \ldots, b_n) < \frac{4g(b_1, \ldots, b_n) + 1}{2},$$

we have

$$\begin{aligned}x_{n+2}\bar{b}_{n+2} &> x_{n+2}\left(4g(b_1,\ldots,b_n)+1-\left(\frac{4g(b_1,\ldots,b_n)+1}{2}\right)\right)\\ &= x_{n+2}\left(\frac{4g(b_1,\ldots,b_n)+1}{2}\right).\end{aligned}$$

Thus, if $x_{n+2} \geq 2$ then $x_{n+2}\bar{b}_{n+2} > 4g(b_1,\ldots,b_n)+1$ so $x_{n+2} \leq 1$. Therefore $x_{n+2} = 1$, so

$$4g(b_1,\ldots,b_n)+1 = \sum_{i=1}^{n+1} x_i\bar{b}_i + \bar{b}_{n+2},$$

and

$$4g(b_1,\ldots,b_n)+1 = \sum_{i=1}^{n+1} x_i\bar{b}_i + g(\bar{b}_1,\ldots,\bar{b}_{n+1}) - 2t,$$

then

$$2t = \sum_{i=1}^{n+1} x_i\bar{b}_i.$$

Finally, $\bar{b}_{n+1} = 2g(b_1,\ldots,b_n)+1 > 2t$ leads to $x_{n+1} = 0$. Therefore,

$$2t = \sum_{i=1}^{n} x_i\bar{b}_i \text{ and } t = \sum_{i=1}^{n} x_ib_i.$$

□

Example 1.3.3 Let $a_1 = 5, a_2 = 11$ and $a_3 = 13$ (a) if $t = 24$ then t is representable by $5, 11$ and 13 since $t > g(5,11,13) = 19$ (say, $t = 11 + 13$) (b) if $t = 17$ then let $\bar{a}_1 = 10, \bar{a}_2 = 22, \bar{a}_3 = 26, \bar{a}_4 = 2g(5,8,22)+1 = 39$ and $\bar{a}_5 = g(10,22,26,39) - 2t = 77 - 34 = 43$. Thus $g(10,22,26,39) = 77 = g(10,22,26,39,43)$ and so 17 is not representable by $5, 11$ and 13.

1.4 Supplementary notes

In [280], Lovász described a relationship between **FP** and the study of maximal lattice point free convex bodies. Lovász formulated a conjecture whose affirmative answer would imply a polynomial time algorithm for **FP** for a fixed number of integers. Scarf and Shallcross [386] also related **FP** with the covering radius. In [28], Barvinok and Wood gave a polynomial time algorithm to compute the generating function of the projection of the set of integer points in a rational d-dimensional polytope for any fixed d implying, in particular, a polynomial time algorithm[10] that computes $g(a_1,\ldots,a_n)$ for any fixed n.

Lewin [274] has proposed a simple algorithm for finding $g(a_1,\ldots,a_n)$ given that $a_1,\ldots,a_n$ form an *almost arithmetic* sequence (*i.e.*, all but one of the basis elements form an arithmetic sequence) under certain conditions; see also [374]. Lewin [271], Hann-Shuei [183] and Chen [90] proposed an algorithm to calculate $g(a_1,\ldots,a_n)$ but no complexity analysis was given. Shevchenko [420] investigated the relation of **FP** and the *group minimization* problem and their algorithmic complexity. Zhu [490] studied the smallest integer b^* such that for every $b^* \geq b$ the knapsack problem of size b is equivalent to the group knapsack problem. The latter can be regarded as a generalization of **FP**. An extension of Greenberg's algorithm is also provided in [490].

Tinaglia [451] gave a procedure that converts the computation of $g(a_1,a_2,a_3)$ to that of $g(a_1,r,s)$ when $a_1 \leq a_2 \leq a_3$, $a_2 = pa_1 + r$, and $a_3 = qa_1 + s$, with integers $p,q \geq 1$ and $r,s \geq 0$. An algorithm to solve **FP** for $n = 3$ was also proposed by Greenberg [172]. An experimental analysis and comparison of Wilf, Nijenhuis and Greenberg algorithms can be found in [204]. Brimkov [65, 66] gave a polynomial time algorithm to find a non-negative integer solution of linear diophantine equations and Owens [320] proposed a geometric method to calculte the Frobenius problem closely related to Killingbergtrø' approach.

In [223], I.D. Kan introduced a new specific partial order on the set of integers $a_1,\ldots,a_n$ and proved some new results on **FP** yielding to an algorithm to calculate $g(a_1,\ldots,a_n)$ in some cases. The algorithm is based on a rather involved analysis of the problem and it is claimed to require at most $O(\ln a_1)$ operations. Kan [226] also calculated and estimated $g(a_1,\ldots,a_n)$ when $a_1,\ldots,a_n$ is an *almost chain sequence* (the sequence $a_1,\ldots,a_n$ is called an *almost chain* if there exists an integer $1 < j < n$ such that $a_2,\ldots,a_j$ and $a_{j+1},\ldots,a_n$ are *chains sequences*[11] with $a_2 \equiv a_{j+1} \equiv 0 \bmod a_1$, and $(a_1,a_2,a_{j+1}) = 1$).

In [51], Böcker and Lipták have introduced a simple algorithm to compute the residue table of a_1 yielding a method to compute $g(a_1,\ldots,a_n)$ in time $O(na_1)$, improving the complexity of Nijenhuis'

[10] In a personal communication, A. Barvinok communicated to me that this algorithm is probably very slow and cannot be easily implemented.

[11] We say that $a_{-m}, a_{-m+1},\ldots,a_{-1},a_0,a_1,\ldots,a,n$ with $m,n \geq 1$, $(a_0,a_1) = 1$ is a *chain sequence* if

$$l_j = \tfrac{a_{j-1}+a_{j+1}}{a_j} \text{ for each } j = -m+1,\ldots,0,1,\ldots,n-1 \text{ are naturals.}$$

algorithm who actually claimed that the running time of his method could be improved to time of order $O(a_{\min}(n+\log a_{\min}))$. In [37], Beihoffer *et al.* use additional symmetry properties of a Nijenhuis' graph to design two algorithms for computing $g(a_1,\ldots,a_n)$ and conjectured that their average-case complexity is $O(\sqrt{n}a_1)$.

We finally mention that Beukers has created software to compute the Frobenius number of four variables, which one can found in the following web site pointer

`http://www.math.ruu.nl/people/beukers/frobenius/`

2

The Frobenius number for small n

2.1 Computing $g(p, q)$ is easy

FP is easy to solve when $n = 2$.

Theorem 2.1.1 [1] *[437] Let p, q be non-negative relatively prime integers. Then,*

$$g(p, q) = pq - p - q.$$

We may present four different proofs of Theorem 2.1.1. The first, due to Nijenhuis and Wilf [310], and the second one are arithmetical proofs, the third one uses the well-known *Pick's theorem* and the fourth one uses power series.

First proof of Theorem 2.1.1. Since $(p, q) = 1$ then any integer p is representable as $p = xp + yq$ with $x, y \in \mathbb{Z}$. Note that p can be represented in many different ways but the representation becomes unique if we ask for $0 \leq x < q$. In this case, p is representable if $y \geq 0$ and it is not representable if $y < 0$. Thus, the largest non-representable value is when $x = q - 1$ and $y = -1$. So,

$$g(p, q) = (q - 1)p + (-1)q = pq - p - q.$$

□

[1] The origin of this famous result is unclear. It is usually attributed to Sylvester because of his works in [437,439]. Although Theorem 2.1.1 is not stated in these papers, they contain Theorem 5.1.1 from which it is conceivable that Sylvester knew Theorem 2.1.1 as they are strongly related.

Second proof of Theorem 2.1.1. Let $T = p\mathbb{N}+q\mathbb{N} = \{xp+yq | x, y \in \mathbb{N}\}$. Suppose that $pq-p-q = r_1p+r_2q$ with $r_1, r_2 \in \mathbb{N}$. So, $p(q-r_1-1) = q(r_2+1)$ and since $(p, q) = 1$ then $q - r_1 - 1 = sq \geq q$, which is impossible. Thus, $pq - p - q \notin T$.

Now, let $c = pq - p - q$, we may show that $c + i \in T$ for any integer $i \geq 1$. By Bézout's theorem, there always exist positive integers r_1 and r_2, $0 \leq r_1 < q$ such that $pr_1 + qr_2 = 1$ (and thus $pir_1 + qir_2 = i$) then

$$c + i = (q - 1 + ir_1)p + (ir_2 - 1)q. \tag{2.1}$$

We may write eqn (2.1) as $c + i = v_1p + v_2q$ with $0 \leq v_2 < p$. Now, since $-i = c - v_1p - v_2q = (-v_1 - 1)p + (p - 1 - v_2)q$ does not belong to T and as $p - 1 - v_2 \geq 0$ then we must have $-v_1 - 1 < 0$ implying that $v_1 > -1$ and thus $v_1 \geq 0$. So $c + i \in T$. □

In 1899, Pick [327] found an elegant formula for computing the area of simple lattice polytopes. A polygon is *simple* if its boundary is a simple closed curve and a *lattice polygon* is a polygon where its vertices are integer coordinates.

Theorem 2.1.2 *(***Pick's Theorem***) [327] Let S be a simplest lattice polygon. Then,*

$$A(S) = I(S) + \frac{B(S)}{2} - 1,$$

where $A(S)$ denotes the area of S, $I(S)$ and $B(S)$ are the number of lattice points in the interior of S, and in the boundary of S, respectively.

Pick's theorem is one of the gems of elementary mathematics; see [463] for a short proof of Pick's theorem.

Third proof of Theorem 2.1.1. Let P be the lattice polygon with vertices $A = (q-1, -1)$, $B = (-1, p-1)$, $C = (q, 0)$ and $D = (0, p)$. Notice that there are no other lattice points on the boundary of P and that the set of lattice points inside P, denoted by $I(P)$, are all in the first quadrant; see Fig. 2.1.

The equation of the line connecting points A and B (respectively points C and D) is given by $px + qy = pq - p - q$ (respectively is given by $px + qy = pq$). Let T_1 and T_2 be the triangles formed by points $(q, 0), (0, p), (-1, p-1)$ and $(-1, p-1), (q-1, -1), (q, 0)$, respectively. Since

$$A(T_1) = \frac{1}{2}\begin{vmatrix} q & 0 & 1 \\ 0 & p & 1 \\ -1 & p-1 & 1 \end{vmatrix} = \frac{1}{2}(q+p)$$

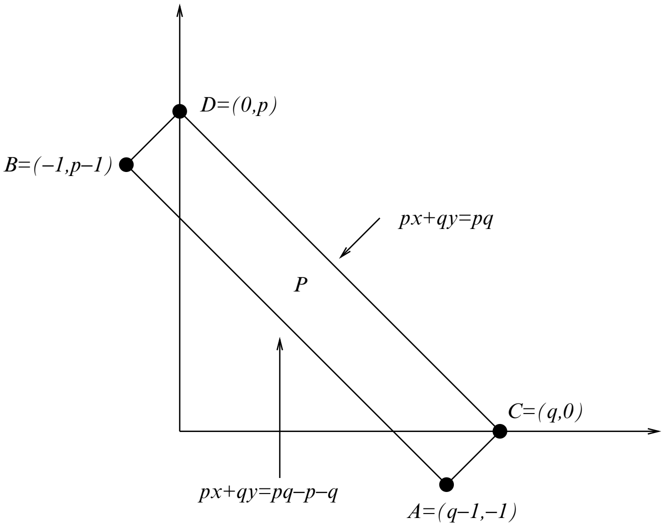

Figure 2.1: Polygon P.

$$= \frac{1}{2}\begin{vmatrix} -1 & p-1 & 1 \\ q-1 & -1 & 1 \\ q & 0 & 1 \end{vmatrix} = A(T_2),$$

then $A(P) = A(T_1) + A(T_2) = p + q$ and, by Pick's theorem, we have that $I(P) = p + q - 1$. We claim that line $px + qy = pq - p - q + i$ contains exactly one point in $I(P)$ for each $i = 1, \ldots, p+q-1$. Suppose that there exists $1 \leq j \leq p+q-1$ such that line $px+qy = pq-p-q+j$ contains two points of $I(P)$, that is, $px_1+qy_1 = pq-p-q+j = px_2+qy_2$ for some $0 \leq x_1, x_2 < q$, $x_1 \neq x_2$ and $0 \leq y_1, y_2 < q$, $y_1 \neq y_2$. Then, $(x_1 - x_2)p = (y_2 - y_1)q$ and since $(p, q) = 1$ then $(x_1 - x_2) = sq \geq q$, which is impossible. So, each line $px + qy = pq - p - q + i$ contains at most one point of $I(P)$. Moreover, each line $px+qy = pq-p-q+i$ has at least one point of $I(P)$, if not, then there exists $1 \leq j \leq p + q - 1$ such that $px_1+qy_1 = pq-p-q+j$ do not contain point from $I(P)$ and then each of the $p+q-1$ points of $I(P)$ belongs to at least one of the $p+q-2$ lines $px_1+qy_1 = pq-p-q+i$, $1 \leq i \neq j \leq p+q-1$. So, by the pigeon-hole principle, there would exist a line $px + qy = pq - p - q + j$ for some $1 \leq j \leq p + q - 1$ containing two points of $I(P)$, which is a contradiction.

Since all lines $px + qy = n \geq pq$ clearly have at least one lattice point in the first quadrant then $pq-p-q$ is the largest value for which $px + qy = pq - p - q$ has no solution on the non-negative integers. □

A geometrical proof of Theorem 2.1.1 follows from Theorem 1.2.14 (*cf.* Example 1.2.17).

Fourth proof of Theorem 2.1.1. Let $r(n)$ be the number of representations of n in the form $px+qy$ with $x, y \geq 0$. By Theorem 4.1.2, we have that

$$R(x) = \sum_{i=1}^{\infty} r(i)x^i = \frac{1}{(1-x^p)(1-x^q)}.$$

Let

$$Q(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)} = \frac{f(x)}{h(x)}.$$

We claim that $Q(x)$ is a polynomial of degree $pq-p-q+1$ with leading coefficient 1. Indeed, let ζ be any complex number such that both $\zeta^p = 1$ and $\zeta^q = 1$. Since $(p, q) = 1$ then there exist integers a, b such that $\zeta^1 = \zeta^{as+bq} = (\zeta^p)^a(\zeta^q)^b = 1$. So, no linear factor (except for $(x-1)$) appears twice in the denominator of $Q(x)$ and therefore, every linear factor in the denominator cancels against a linear factor in the numerator. Now, by L'Hopital's rule we have that

$$Q(1) = \lim_{x\to 1}\frac{f(x)}{h(x)} = \lim_{x\to 1}\frac{f'(x)}{h'(x)} = \lim_{x\to 1}\frac{f''(x)}{h''(x)} = \frac{2pq}{2pq} = 1.$$

Therefore, one is a root of $Q(x)-1$ and $\frac{Q(x)-1}{x-1}$ is also a polynomial of degree $pq-p-q$ with leading coefficient 1. But,

$$\begin{aligned}\frac{Q(x)-1}{x-1} &= (x^{pq}-1)R(x) + \frac{1}{1-x} = x^{pq}R(x) - R(x) + \sum_{i=0}^{\infty} x^i\\ &= \sum_{i=0}^{\infty} r(i)x^{pq+i} + \sum_{i=0}^{\infty}(1-r(i))x^i\\ &= \sum_{i=0}^{\infty}(r(i-pq)+1-r(i))x^i + \sum_{i=0}^{pq-1}(1-r(i))x^i.\end{aligned}$$

Since the rational function $\frac{Q(x)-1}{x-1}$ is of degree $pq-p-q$ with leading coefficient 1 then the power series coefficient of the $(pq-p-q)-th$ term is 1 (and thus $1-r(pq-p-q) = 1$ implying that $r(pq-p-q) = 0$) and the coefficient of the $k-th$ term is zero for each $k > pq-p-q$ (and thus $1-r(k) = 0$ implying that $r(k) = 1$ for each $pq-p-q < k \leq pq-1$). □

A proof of Theorem 2.1.1 can also be obtained from the very useful result in terms of congruences due to Brauer and Shockley [59] (*cf.* Lemma 3.1.6).

2.2 A Formula for $g(a_1, a_2, a_3)$

Contrary to the case $n = 2$, the computation of a formula for $g(a_1, a_2, a_3)$ turned out to be much more difficult. As we have seen in Chapter 1, various polynomial time algorithms to compute $g(a_1, a_2, a_3)$ are known but none lead to an explicit formula. Curtis showed that, in some sense, a search for a simple formula when $n = 3$ is impossible. Indeed, Curtis [100] proved that in the case $n = 3$, and consequently in all cases $n \geq 3$, the Frobenius number cannot be given by closed formulas of a certain type.

Theorem 2.2.1 *[100] Let $A = \{(a_1, a_2, a_3) \in \mathbb{N}^3 |\ a_1 < a_2 < a_3,\ a_1$ and a_2 are prime, and $a_1, a_2 \not| a_3\}$. Then there is no non-zero polynomial $H \in C[X_1, X_2, X_3, Y]$ such that $H(a_1, a_2, a_3, g(a_1, a_2, a_3)) = 0$ for all $(a_1, a_2, a_3) \in A$.*

The following corollary shows that $g(a_1, a_2, a_3)$ cannot be determined by any set of 'closed' formulas that could be reduced to a finite set of polynomials when restricted to set A (defined in Theorem 2.2.1).

Corollary 2.2.2 *[100] There is no finite set of polynomials $\{h_1, \ldots, h_n\}$ such that for each choice of a_1, a_2, a_3 there is some i such that $h_i(a_1, a_2, a_3) = g(a_1, a_2, a_3)$.*

Proof. $H = \prod_{i=1}^{n}(h_i(X_1, X_2, X_3) - Y)$ would vanish on A. □

An explicit general formula for computing $g(a_1, a_2, a_3)$ can be found. Let L_1, L_2 and L_3 be the smallest positive integers such that there exist integers $x_{ij} \geq 0$, $1 \leq i, j \leq 3$, $i \neq j$ with

$$\begin{aligned} L_1 a_1 &= x_{12} a_2 + x_{13} a_3, \\ L_2 a_2 &= x_{21} a_1 + x_{23} a_3, \\ L_3 a_3 &= x_{31} a_1 + x_{32} a_2. \end{aligned} \tag{2.2}$$

Theorem 2.2.3 *[109, 347] Let a_1, a_2, a_3 be pairwise relatively prime positive integers and $\{i, j, k\} = \{1, 2, 3\}$. Then,*

$$g(a_1, a_2, a_3) = \begin{cases} \max\{L_i a_i + x_{jk} a_k, L_j a_j + x_{ik} a_k\} - \sum\limits_{n=1}^{3} a_n & \text{if } x_{ij} > 0 \\ & \text{for all } i, j, \\ L_j a_j + L_i a_i - \sum\limits_{n=1}^{3} a_n & \text{if } x_{ij} = 0. \end{cases}$$

The formula of Theorem 2.2.3 can be deduced from the degree of Hilbert series of certain graded ring. This algebraic proof is given in

Chapter 4 (Section 4.7) where a more general setting is discussed. In Section 8.4, we describe a polynomial time method to calculate L_1, L_2 and L_3 that depends on the values s_i, p_i and r_i defined in Rødseth's method (see Section 1.1.1).

We notice that the following closely related formula was given by Johnson [219, Theorem 4],

$$g(a_1,a_2,a_3) = L_i a_i + \max_{j,k\neq i}\{x_{jk}a_k, x_{kj}a_j\} - \sum_{n=1}^{3} a_n.$$

However, Johnson's formula assumes that $L_i > 1$ for all i and $x_{ij} > 0$ for all $i \neq j$. Thus, it may not give the Frobenius number for certain triples (for instance, if $a_1 = 4, a_2 = 9$ and $a_3 = 25$ then $x_{13} = x_{23} = 0$ and $L_3 = 1$). The formula of Theorem 2.2.3 does not have these constraints and is valid for any given triple; see also [457].

2.3 Results when $n = 3$

Johnson [219] showed that a common factor $(a_1, a_2) = d$ can be removed in order to compute $g(a_1, a_2, a_3)$.

Theorem 2.3.1 *[219] If a_1, a_2, a_3 are relatively prime and $(a_1, a_2) = d$ then*

$$g(a_1,a_2,a_3) = dg(\frac{a_1}{d}, \frac{a_2}{d}, a_3) + (d-1)a_3.$$

It is clear from Theorem 2.3.1 that if $a_3 \geq g(\frac{a_1}{d}, \frac{a_2}{d})$ then $g(a_1, a_2, a_3) = d(a_1a_2 - a_1 - a_2) + (d-1)a_3$. Oiu and Niu [311] generalized the latter in the following way.

Theorem 2.3.2 *[311] Let $(a_1, a_3) = d$, $a_1 = a'_1 d$ and $a_2 = a'_2 d$ such that there exist integers $x_1, x_2 \geq 0$ with $a_3 = x_1a'_1 + x_2a'_2$. Then,*

$$g(a_1,a_2,a_3) = \frac{a_1a_2}{d} - a_1 - a_2 + (d-1)a_3.$$

Brauer and Shockley [59] generalized Johnson's result for any integer $n \geq 1$ (*cf.* Lemma 3.1.7). In fact, the methods obtained by Brauer and Shockley in [59] (*cf.* Lemma 3.1.6) give the exact value for some special cases when $n = 3$; see also [213]. For instance, if a_1, a_2, a_3 are relatively prime and $a_1|(a_2 + a_3)$ then

$$g(a_1,a_2,a_3) = -a_1 + \max_{i=2,3}\left\{a_i \left\lfloor \frac{a_1a_{5-i}}{a_2+a_3} \right\rfloor\right\}. \tag{2.3}$$

Kan generalized equality (2.3) (see Theorem 3.1.21). Among other particular results, Roberts [356] obtained the following one.

Theorem 2.3.3 *[356] (a) If $(a_3 - a_1, a_2 - a_1) = 1$ then*

$$g(a_1, a_2, a_3) \le a_1 \left(a_3 - a_2 - 2 + \left\lfloor \frac{a_1}{a_3 - a_1} \right\rfloor\right) + (a_2 - a_1 - 1)(a_3 - a_1 - 1) + a_1 + a_2 + a_3.$$

(b) If $a, j > 2$ are integers then

$$g(a, a+1, a+j) = \begin{cases} \left\lfloor \dfrac{a+1}{j} \right\rfloor a + (j-3)a & \text{if } a \equiv -1 \bmod j \text{ and } a \ge j^2 - 5j + 3, \\ \left\lfloor \dfrac{a+1}{j} \right\rfloor (a+j) + (j-3)a & \text{if } a \equiv -1 \bmod j \text{ and } a \ge j^2 - 4j + 2. \end{cases}$$

(c) $0 < a < b$ and m are integers such that $(a, b) = 1$, $m \ge 2$ then

$$g(m, m+a, m+b) \le m \left(b - 2 + \left\lfloor \frac{m}{b} \right\rfloor\right) + (a-1)(b-1).$$

Goldberg [159] studied $g(a_1, a_2, a_3)$ in some very special cases.

Theorem 2.3.4 *[159] Let $1 < a < b$ be integers with $(a, b) = d$ and $(d, m) = 1$ with $md^2 > b(b-a-2d)$ and $dm = ax_0 + by_0$, $0 \le x_0 < b/d$, $y_0 \ge 0$. Then,*

$$g(m, m+a, m+b) = \begin{cases} \left(\dfrac{a}{d} + x_0 + y_0 + d - 3\right) n + b\left(\dfrac{a}{d} - 1\right) - a & \text{if } dx_0 \ge b - a, \\ \left(\dfrac{b}{d} + y_0 + d - 3\right) n + b(\frac{a}{d} - 1) - a(x_0 + 1) & \text{otherwise.} \end{cases}$$

This result solves **FP** for the relatively prime numbers $1 < a_1 < a_2 < a_3$ if these numbers are not very different (that is, if a_1 is large enough compared to $a_3 - a_1$). Byrnes [79] gave the following partial result and observed that his method can be applied in many other cases when $n = 3$.

Theorem 2.3.5 *[79] Let* $a_1 < a_2 < a_3$*, with* $a_2 \equiv 1 \bmod a_1$*. Then,*

$$g(a_1, a_2, a_3) = \begin{cases} a_1a_2 - (a_1 + a_2) & \text{if } a_3 \leq ja_2, \\ a_3\left(\frac{a_1-m}{j}\right) + (m-1)a_2 - a_1 & \text{if } (j-m)a_2 < a_3 \leq ja_2, \\ a_3\left(\frac{a_1-m-j}{j}\right) + (j-1)a_2 - a_1 & \text{if } a_2\left(\frac{j}{a_1-m+j}\right)(j-m) \leq a_3 \\ & < (j-m)a_2, \end{cases}$$

where j *and* m *are such that* $a_3 \equiv j \bmod a_1$*,* $0 \leq j < a_1$ *and (if* $j \neq 0$*)* $a_1 \equiv m \bmod j$*,* $1 \leq m \leq j$*.*

The sequence $a_1, \ldots, a_n$ is called *independent* if none of the basis elements has a representation by the others. Selmer [392] found a quite general formula for independent triples.

Theorem 2.3.6 *[392] If* a_1, a_2 *and* a_3 *are independent and pairwise relatively prime then*

$$g(a_1, a_2, a_3) \leq \max\{(s-1)a_2 + (q-1)a_3, (r-1)a_2 + qa_3\} - a_1,$$

where s *is determined by* $a_3 \equiv sa_2 \bmod a_1$*,* $1 < s < a_1$ *and* q *and* r *are determined by* $a_1 = qs + r$*,* $0 < r < s$*. Moreover, if* $a_2 \geq t(q+1)$ *where* $a_3 = sa_2 - ta_1$*,* $t > 0$ *then*

$$g(a_1, a_2, a_3) = \max\{(s-1)a_2 + (q-1)a_3, (r-1)a_2 + qa_3\} - a_1.$$

The latter can be considered as a particular case of a rather complicated general result given by Hofmeister [198] (*cf.* Theorem 2.3.11).

In [346], we studied Kannan's approach to **FP** via the covering radius (see Section 1.2, Corollary 1.2.16 and Proposition 3.1.8) and found two upper bounds close related to those given in Theorem 2.3.6.

Theorem 2.3.7 *[346] Let* $0 < w_1 < a_3$ *and* $0 < w_2 < a_3$ *be the unique integers such that* $a_1w_1 \equiv a_2 \bmod a_3$ *and* $a_2w_2 \equiv -a_1 \bmod a_3$*, respectively, and let* r_1 *and* r_2 *be the largest positive integers such that* $-a_3 + r_1w_1 < 0$ *and* $a_3 - w_2r_2 > 0$*, respectively.*

(a) $g(a_1, a_2, a_3) \leq \max\{a_1(a_3 - r_1w_1) + a_2(r_1 + 1), a_1w_1 + a_2r_1\}$
$-a_1 - a_2 - a_3.$

(b) $g(a_1, a_2, a_3) \leq \max\{a_1 + a_2(a_3 + (1 - r_2)w_2), a_1r_2 + a_2w_2\} - a_1 - a_2 - a_3.$

The upper bounds given in Theorem 2.3.7 might not be close to each other, however, there are cases in which one of them (or both) give a value very close to $g(a_1, a_2, a_3)$. This is illustrated in Examples 2.3.8 and 2.3.9.

Example 2.3.8 Let $a_1 = 4, a_2 = 7$ and $a_3 = 9$. We have that $w_1 = 4, w_2 = 2, r_1 = 2$ and $r_2 = 4$. Then,

$$g(4,7,9) \leq \begin{Bmatrix} \text{(by Theorem 2.3.7 (a)) } \max\{25, 30\} - 20 \\ \text{(by Theorem 2.3.7 (b)) } \max\{18, 30\} - 20 \end{Bmatrix}$$
$$= 10 = g(4,7,9).$$

Example 2.3.9 Let $a_1 = 5, a_2 = 14$ and $a_3 = 31$. We have that $w_1 = 11, w_2 = 2, r_1 = 2$ and $r_2 = 15$. Then,

$$g(5,14,31) \leq \begin{cases} \text{(by Theorem 2.3.7 (a)) } \max\{87, 83\} - 50 = 37 \\ \qquad = g(5,14,31) \\ \text{(by Theorem 2.3.7 (b)) } \max\{47, 103\} - 50 = 87. \end{cases}$$

In [31], Beck *et al.* used their results on denumerants (see Section 4.1) to obtain the following upper bound.

Theorem 2.3.10 *[31] Let a_1, a_2, a_3 be positive integers with $(a_1, a_2, a_3) = 1$. Then,*

$$g(a_1, a_2, a_3) \leq a_1 a_2 a_3 \sqrt{\frac{1}{4}\left(\frac{1}{a_1 a_2} + \frac{1}{a_2 a_3} + \frac{1}{a_1 a_3}\right)} - \frac{1}{2}(a_1 - a_2 - a_3).$$

2.3.1 Hofmeister's formula and its generalization

Hofmeister [198] generalized Theorem 2.3.3.

Theorem 2.3.11 *[198] Let a_1, a_2, a_3 be positive integers pairwise relatively prime with $a_i \geq 4$ and $a_1 < a_2, a_3$. Let j, k, m be positive integers defined by $a_3 \equiv j a_2 \bmod a_1,\ a_1 = kj + m$. Then,*

$$g(a_1, a_2, a_3) = -a_1 + \begin{cases} (m-1)a_2 + k a_3 & \text{if } (j-m)a_2 \leq a_3, \\ (j-1)a_2 + (k-1)a_3 & \text{if } (j-m)a_2 > a_3 \geq \\ & a_2\left(\frac{j-m}{k+1}\right). \end{cases}$$

Note that the above theorem does not consider the case $a_3 < a_2\left(\frac{j-m}{k+1}\right)$. Hujter and Vizvári [213] extended Hofmeister's formula.

Theorem 2.3.12 *[213] Let a_1, a_2, a_3 be positive integers pairwise relatively prime with $a_i \geq 7$ and $a_1 < a_2, a_3$. Let j, k, l be positive integers as in Theorem 2.3.11 and let r be an integer such that $0 \leq r \leq j-m$, $m-1 \equiv r \bmod (j-m)$.*

a) If $j \geq 2m$ and $a_2\left(\frac{j-2m}{k+1}\right) \leq a_3 < a_2\left(\frac{j-m}{k+1}\right)$ then

$$g(a_1, a_2, a_3) = -a_1 + (m-1)a_2 + 2ka_3,$$

and b) if $j < 2m$ and $a_2\left(\frac{j-m-r-1}{k+1}\right) \leq a_3 < a_2\left(\frac{j-m}{k+1}\right)$ then

$$g(a_1, a_2, a_3) = -a_1 + ra_2 + \left(2k + \left\lfloor \frac{m-1}{j-m} \right\rfloor (k+1)\right) a_3.$$

2.3.2 More special cases

Vitek [467] has shown that

Theorem 2.3.13 *[467] If a_1, a_2, a_3 are independent (i.e. none of the a_i is representable by the other two) then*

$$g(a_1, a_2, a_3) \leq a_1 \left\lfloor \frac{a_3}{2} - 1 \right\rfloor.$$

Vitek exhibited some cases to show that the bound in Theorem 2.3.13 is sharp. Davison [104] gave a new shorter proof of Vitek's upper bound. Kan *et al.* [224] gave an identity connecting $g(a_1, a_2, a_3)$ with $g(s, s+1, s+p)$ for particular integers s and p (answering a conjecture posed by Stechkin and Baranov [435, Problem 2.25, page 99]).

Theorem 2.3.14 *[224] Let $a_1 < a_2 < a_3$ be positive integers and let $d = (a_1, a_2)$. Then,*

$$g(a_1, a_2, a_3) = \frac{a_1 a_2 (g(s, s+1, s+p) + 2s + 1)}{ds(s+1)} + (d-1)a_3 - (a_1 + a_2),$$

where $s = \frac{a_2}{d}v - 1$, $p = s(\frac{a_3 dv}{a_1} - 1)$ and $v \in \mathbb{N}$ satisfies the condition $a_2 v \equiv d \bmod a_1$ with $vd < a_1$.

Kan *et al.* [224] gave[2] an exact formula for $g(s, s+1, s+p)$ when $2 \leq p \leq 5$, $s > p(p-4) + 1$ and also an upper bound for general p.

[2] The results of [224] appeared in the section 'short communications' of the journal, and no proofs were given.

Hujter [210] has proved the following equality in order to give a lower bound for the general problem (*cf.* Theorem 3.6.2). If $q > 2$ is an arbitrary integer then

$$g(q^2, q^2 + 1, q^2 + q) = 2q^3 - 2q^2 - 1. \tag{2.4}$$

Djawadi [116] gave an exact formula for $g(a, a-2, a+k)$ with $k \geq 5$, k-odd and $a \geq k$.

Beck *et al.* [34] have studied **FP** when $n = 3$ and, based on empirical data, they conjectured that

$$g(a_1, a_2, a_3) \leq C\sqrt{a_1 a_2 a_3}^{p} - a_1 - a_2 - a_3 \text{ where } p < \tfrac{4}{3} \text{ and } C \text{ is a constant.} \tag{2.5}$$

They also conjectured that, in fact:

$$g(a_1, a_2, a_3) \leq \sqrt{a_1 a_2 a_3}^{5/4} - a_1 - a_2 - a_3. \tag{2.6}$$

They checked by computer that this upper bound is verified in more than three thousand randomly chosen *admissible* triplet (a triple is called admissable if they are *independent*, they do not form an *almost arithmetic sequence* and they are pairwise coprime). In [140], Fel disproved both conjectures by giving the following two counterexamples. Let $a_1 = 10\,001 = 73 \times 137, a_2 = 10\,003 = 7 \times 1429$ and $a_3 = 20\,003 = 83 \times 241$ (it can be checked that this is an admissable triple). In this case, $g(10\,001, 10\,003, 20\,003) = 50\,014\,999$ while the conjectured bound in eqn (2.6) reads

$$\begin{aligned} &g(10\,001, 10\,003, 20\,003) \\ &\quad \leq \sqrt{10\,001 \cdot 10\,003 \cdot 20\,003}^{5/4} - (10\,001 + 10\,003 + 20\,003) \\ &\quad = 48\,745\,742.422. \end{aligned}$$

For the conjectured bound in eqn (2.5), Fel considered the triple $a_1 = 2l + 1, a_2 = a_1 + 2 = 2l + 3$ and $a_3 = 2a_1 + 1 = 4l + 3$ with $l >> 1$ and where a_1 is a prime number. Again, it can be checked that this is an admissable triple. Here, $g(2l + 1, 2l + 3, 4l + 3) = 2l^2 + 3l - 1$. Now, in order to disproved conjecture 2.5 it is showed that that there is not always a constant C and value $p < 4/3$ such that

$$\delta_l(C, p) = \frac{C\sqrt{(2l + 1)(2l + 3)(4l + 3)}^{p} - (2l + 1 + 2l + 3 + 4l + 3)}{g(2l + 1, 2l + 3, 4l + 3)} \geq 1$$

for all $l > 1$. Independently, Schlage-Puchta [387] has also disproved the conjectured bound in eqn (2.6).

2.3.3 Johnson integers

In [219], Johnson gave a symmetric expression for the best upper bound for $g(a_1, a_2, a_3)$ and insights into the general problem. Based on Johnson's work, Tinaglia investigated $g(a_1, \ldots, a_n)$ by defining the *Johnson integers* as follows. For each $j = 1, \ldots, n$ the *j–th Johnson integer* A_j, associated with the integers $a_1, \ldots, a_j, \ldots, a_n$, is defined by

$$\begin{aligned} A_j = \min\{&X_j \in \mathbb{Z} | X_j \geq 1 \text{ such that there exist } X_1, \ldots, X_{j-1}, \\ &X_{j+1}, \ldots, X_n \text{ with } a_1X_1 + \cdots + a_{j-1}X_{j-1}, a_{j+1}X_{j+1} \\ &+ \cdots + a_nX_n = a_jX_j\}. \end{aligned}$$

That is, A_j is the smallest integer such that a_jA_j is a linear combination of $a_1, \cdots, a_{j-1}, a_{j+1}, \ldots, a_n$. In such a case each solution $X_1, \ldots, -A_j, \ldots, X_n$ of the equation $\sum_{i=1}^{n} a_ix_i = 0$ with integers $X_i \geq 0$, $i = 1, \ldots, j-1, j+1, \ldots, n$, is a *Johnson solution* associated with A_j. Note that there are always at least n Johnson solutions.

Let $\bar{d}(m)$ be the number of solutions of $\sum_{i=1}^{n} a_ix_i = m$ with $x_i < A_i$. In [449], Tinaglia gave a specification of what happens to the solution of $a_1x_1 + a_2x_2 + a_3x_3 = m$, with $x_i \geq 0$, when $m < g(a_1, a_2, a_3)$, by analysing $\bar{d}(m)$ and $d(m; a_1, a_2, a_3)$ (the number of different representations of m as $a_1x_1 + a_2x_2 + a_3x_3 = m$ with $x_i \geq 0$; see Chapter 5).

2.4 $g(a_1, a_2, a_3, a_4)$

If $g(a_1, a_2, a_3)$ is difficult to compute the cases $n \geq 4$ seem even harder. By using graph-theoretical methods, Dulmage and Mendelsohn [122] obtained some interesting formulas.

Theorem 2.4.1 *[122] Let a be a non-negative integer. Then,*

a) $g(a, a+1, a+2, a+4) = (a+1)\lfloor \frac{a}{4} \rfloor + \lfloor \frac{a+1}{4} \rfloor + 2\lfloor \frac{a+2}{4} \rfloor - 1,$

b) $g(a, a+1, a+2, a+5) = a\lfloor \frac{a+1}{5} \rfloor + \lfloor \frac{a}{5} \rfloor + \lfloor \frac{a+1}{5} \rfloor + \lfloor \frac{(a+2)}{5} \rfloor + 2\lfloor \frac{a+3}{5} \rfloor - 1$ *and*

c) $g(a, a+1, a+2, a+6) = a\lfloor \frac{a}{6} \rfloor + 2\lfloor \frac{a}{6} \rfloor + 2\lfloor \frac{a+1}{6} \rfloor + 5\lfloor \frac{a+2}{6} \rfloor + \lfloor \frac{a+3}{6} \rfloor + \lfloor \frac{a+4}{6} \rfloor + \lfloor \frac{a+5}{6} \rfloor - 1.$

In fact, the formula in part (a) of Theorem 2.4.1 follows easily from Theorem 3.3.5; see also [392] and [423]. Vitek [467] has proved that

$$g(a_1, a_2, a_3, a_4) \leq \left\lfloor \frac{(a_4-2)(a_4-3)}{3} \right\rfloor - 1. \tag{2.7}$$

We finally mention the following two formulas due to Kan [225] obtained as a Corollary of Theorem 3.1.21. Let $\{\alpha\}$ denote the fractional

part of $\alpha \in \mathbb{R}$, that is $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$. Let a, b be positive integers such that $a > b \geq 2$.
(a) If $a + 1 \geq (b-1)\lfloor \frac{a}{b} \rfloor$ then

$$g(a, a+1, a+2, a+b, a+2b) = (a+b)\left\lfloor \frac{a-1}{b} \right\rfloor + ab - 2a - 1$$
$$- \min\left\{ -b + (ab+b)\left\{ -\frac{a}{b} \right\} + a\left\lfloor \frac{a-1}{2b} \right\rfloor + a\left\lfloor \frac{b\{(a-1)/b\}}{2} \right\rfloor, a\left\lfloor \frac{b+1}{2} \right\rfloor + a\left\lfloor \frac{a-1-b}{2b} \right\rfloor \right\}.$$

(b) If $2a + 3 \geq (2b-3)\lfloor \dfrac{a}{b} \rfloor$ then

$$g(a, a+1, 2a+3, a+b) = (a+b)\left\lfloor \frac{a-1}{b} \right\rfloor + ab - 2a - 1$$
$$- \min\left\{ -b + (ab+b)\left\{ -\frac{a}{b} \right\} + a\left\lfloor \frac{b\{(a-1)/b\}}{3} \right\rfloor, a\left\lfloor \frac{b+2}{3} \right\rfloor \right\}.$$

2.5 Supplementary notes

A proof of Theorem 2.1.1 using Brauer and Shockley's result (Lemma 3.1.6) is given by Ontkush [318]; see also [275]. In [447] Tinaglia has determined $g(a_1, \ldots, a_4)$ when one of the Johnson integers is less than 5 and in [446] Tinaglia obtained a complete solution for $g(a_1, a_2, a_3)$ by using continued fractions and found a simple formula for $g(a_1, a_2, a_3)$ in special cases. Morikawa [302] has also investigated the Frobenius number when $n = 3$. In [486], Yuan gave an intrisic formula for $g(a_1, a_2, a_3)$ and in [89] Chen proposed some upper bounds when $n = 3$; see also the work by Kang and Liu [227], by Ke [232] and by Grant [169].

In [148], Fröberg used the algebraic concept, called *socle*, to calculate $g(a_1, a_2, a_3)$ when the semigroup $S = \langle a_1, a_2, a_3 \rangle$ is non-symmetric. Fröberg obtained essentially the same formula as that of Theorem 2.2.3 in the case when $x_{ij} > 0$ for all i, j. In the case when $x_{ij} = 0$ (that is, when S is symmetric), Herzog [191] managed to give a method to compute $g(a_1, a_2, a_3)$ but no explicit formula, similar to Theorem 2.2.3, is obtained.

Byrnes [80] studied $g(a_1, \ldots, a_n)$ and examined the situation when $a_k \equiv k - 1 \bmod a_1$, $2 \leq k \leq n$ obtaining an explicit solution for $n = 5$ in such cases. Investigations for a simple formula for $g(a_1, a_2, a_3)$ in special cases has been done by by Chen and Liu [91]. In fact, Chen and Liu's result is a special case (when $n = 3$) of a result by W. Lu and Wu; see eqn (3.8). In [253], Kraft rediscovered some results due to Johnson [219] by considering an algebraic point of view. In [368], Rosales *et al.* proved that for any given positive integer n there always exist integers a, b, c such that $g(a, b, c) = n$; see also [367] for a related result.

3

The general problem

3.1 Formulas and upper bounds

In his lectures in Berlin in 1935, Schur proved[1]

Theorem 3.1.1 *Let* $(a_1, \ldots, a_n) = 1$*. Then,*

$$g(a_1, \ldots, a_n) \leq (a_1 - 1)(a_n - 1) - 1.$$

Smoryński [430] presented a new proof for Schur's result by using Skolem's method [425] of *quantifier elimination*[2]. Brauer [57] improved Schur's result[3].

Theorem 3.1.2 *[57] Let* $d_i = (a_1, \ldots, a_i)$ *and let* $T(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_{i+1} d_i / d_{i+1}$*. Then,*

$$g(a_1, \ldots, a_n) \leq T(a_1, \ldots, a_n) - \sum_{i=1}^{n} a_i.$$

Rødseth [379] found the following easy proof of Theorem 3.1.2.

Proof of Theorem 3.1.2. Notice that

$$g\left(\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}, \frac{a_{i+1}}{d_{i+1}}\right) \leq g\left(\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}\right), \tag{3.1}$$

[1] According to Brauer's introduction in [57].

[2] Classical elimination theory consists in reducing questions of the solvability of certain types of equations or systems of equations to calculable conditions on the coefficients of the equations. Smoryński puts forward this application of Skolem's work as a useful pedagogic example for courses in logic and elementary number theory.

[3] Reference [57] was intended to be published originally as a joint paper of Brauer and Schur. But because of the circumstances, Brauer met Schur's wishes and published alone.

where equality holds if $\frac{a_{i+1}}{d_{i+1}}$ is dependent on $\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}$. Since,

$$\frac{d_i}{d_{i+1}} = \left(\frac{a_1}{d_{i+1}}, \ldots, \frac{a_i}{d_{i+1}}\right)$$

then repeated applications of Theorem 3.1.7 and eqn (3.1) give the desired inequality. □

Brauer gave sufficient and necessary conditions for $T(a_1, a_2, a_3)$ (defined in Theorem 3.1.2) to be the smallest best possible bound. In particular, Brauer showed the following result.

Theorem 3.1.3 *[57] Let b_1 and b_2 be relatively prime numbers. Then, there exists exactly $(b_1 - 1)(b_2 - 1)/2$ positive integers b_3 for which $T(a_1, a_2, a_3)$ is not the best bound.*

For instance, $T(m, m+2, m+1)$ is the smallest possible bound if m is an even integer, and it is not the best bound if $m > 1$ is odd.

In a continuation of [57], Brauer and Seelbinder [58] proved the following two theorems; see also [59].

Theorem 3.1.4 *[58] The bound obtained in Theorem 3.1.2 is the best possible if and only if each of the integers $\frac{a_j}{d_j}$, $j = 2, \ldots, n$, is representable in the form*

$$\frac{a_j}{d_j} = \sum_{i=1}^{n-1} y_{ji} \left(\frac{a_i}{d_{j-1}}\right) \quad \textit{with } y_{ji} \geq 0.$$

Nijenhuis and Wilf [310] gave another different proof of Theorem 3.1.4. Their simpler proof is based on the observation that if x and y are positive integers with $x + y = g(a_1, \ldots, a_n)$, then at most one of x and y can have a representation by $a_1, \ldots, a_n$ (see the proof of Theorem 5.2.5).

Theorem 3.1.5 *[58] If in Theorem 3.1.2, $g(a_1, \ldots, a_n) < T(a_1, \ldots, a_n) - \sum_{i=1}^{n} a_i$ then*

$$g(a_1, \ldots, a_n) \leq T(a_1, \ldots, a_n) - \sum_{i=1}^{n} a_i - \min\{a_1, \ldots, a_n\}.$$

The following two lemmas, due to Brauer and Shockley [59], are very helpful.

Lemma 3.1.6 *[59]*

$$g(a_1, \ldots, a_n) = \max_{l \in \{1,2,\ldots,a_n-1\}} \{t_l\} - a_n,$$

where t_l is the smallest positive integer congruent to l modulo a_n, that is expressible as a non-negative integer combination of $a_1, \ldots, a_{n-1}$.

Proof. The proof is rather simple. Let L be a positive integer. If $L \equiv 0 \bmod a_n$ then L is a non-negative integer combination of a_n. If $L \equiv l \bmod a_n$ then L is a non-negative integer combination of $a_1, \ldots, a_n$ if and only if $L \geq t_l$. □

Lemma 3.1.7 *[59] Let $d = (a_1, \ldots, a_{n-1})$. Then,*

$$g(a_1, \ldots, a_n) = dg\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) + (d-1)a_n.$$

Proof. Let $G = G(a_1, \ldots, a_n) = g(a_1, \ldots, a_n) + \sum_{i=1}^{n} a_i$, that is, G is the largest integer not representable as a linear combination of $a_1, \ldots, a_n$ in positive integers. Then, equality $g(a_1, \ldots, a_n) = dg(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n) + (d-1)a_n$ holds if and only if

$$G(a_1, \ldots, a_n) \sum_{i=1}^{n} a_i = dG\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) - d\sum_{i=1}^{n-1} \frac{a_i}{d} - da_n + (d-1)a_n$$

holds, or equivalently, if and only if

$$\begin{aligned} G(a_1, \ldots, a_n) &= dG\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) + a_n - da_n + (d-1)a_n \\ &= dG\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) \end{aligned}$$

holds. Notice that $G(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_i x_i$ with $x_i > 0$ (this follows from the fact that we can write $a_n + G(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_i x_i + a_n x_n$ with $x_i > 0$ and thus $G(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_i x_i + a_n(x_n - 1)$ that contradicts the definition of G unless $x_n = 1$).

Let $a_i = da'_i$, $i = 1, \ldots, n-1$. Hence,

$$G = \sum_{i=1}^{n-1} a_i x_i = d\sum_{i=1}^{n-1} a'_i x_i \text{ and } G \text{ is divisible by } d, \text{ say } G = dG'. \quad (3.2)$$

It is clear that G' cannot be expressed as a linear combination of $a'_1, \ldots, a'_{n-1}, a_n$ in positive integers (otherwise $G' = y_n a_n + \sum_{i=1}^{n-1} a'_i y_i$ with $y_i > 0$ and $G = G'd = y_1 da_1 + \sum_{i=1}^{n-1} a_i y_i$, which is a contradiction).

Now, if $h > G'$ then h can be expressed as a linear combination of $a'_1, \ldots, a'_{n-1}, a_n$ with positive coefficients. For, since $hd > G'd = G$ then $hd = \sum_{i=1}^{n} a_i z_i = z_n a_n + d\sum_{i=1}^{n-1} a'_i z_i$ with $z_i > 0$. Hence, d must divide z_n, say $z_1 = dz'_1$, and $h = z'_n a_n + \sum_{i=1}^{n-1} a'_i z_i$. Thus,

$G' = G(a'_1, \ldots, a'_{n-1}, a_n)$ and by eqn (3.2) we have $G(a_1, \ldots, a_n) = dG(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n)$. □

An algebraic proof of Lemma 3.1.7 was given by Delorme [107, Proposition 1.3]. Notice that Lemma 3.1.7 can also be obtained from Lemma 3.1.6 from which it can be deduced that if a_n is representable as a linear combination of the other a_is with non-negative integers then

$$g(a_1, \ldots, a_n) = g(a_1, \ldots, a_{n-1}). \tag{3.3}$$

Notice that eqn (3.3) and Lemma 3.1.7 reduce the problem to compute $g(a_1, \ldots, a_n)$ to the case where each $(n-1)$-subset of $a_1, \ldots, a_n$ is relatively prime and no a_j is a linear combination of the other a_is with non-negative integers (generalizing Johnson's result given in Theorem 2.3.1).

The following proposition is one of the basic lattice properties investigated in [346] in relation to the covering radius

Proposition 3.1.8 *Let $\mathbf{x}, \mathbf{x}' \in \mathbb{Z}^{n-1}$ be such that $x_i < x'_i$ for each $i = 1, \ldots, n-1$. If $\mu(\mathbf{x})$ absorbs point $\mathbf{x}'$ then $\mu \geq \sum_{i=1}^{n-1} a_i(x'_i - x_i)$.*

As an easy application of the above Proposition and Corollary 1.2.16, we obtain that if $(a_j, a_n) = 1$ for each $j = 1, \ldots, n-1$ then

$$g(a_1, \ldots, a_n) \leq \sum_{i=1}^{n-1} (a_i - 1)v_i, \tag{3.4}$$

where $v_j a_j \equiv -\sum_{i=1\ i\neq j}^{n-1} \bmod a_n$.

The latter comes from the fact that the point $\mathbf{v} = (v_1, \ldots, v_{n-1})$ can be absorbed by a simplex placed at the origin and thus $\mu^*_{\mathbf{v}} \leq \sum_{i=1}^{n-1} a_i v_i$. It can be checked that translations of $\mu_{\mathbf{0}}(\mathbf{v})$ cover the $\mathbb{R}^{n-1}$. This is shown in Fig. 3.1 for the case $n = 3$.

Wilf's algorithm (see Section 1.2) provides the following easy upper bound.

Theorem 3.1.9 *[480]*

$$g(a_1, \ldots, a_n) \leq a_n^2.$$

Proof. After each full sweep of the algorithm at least one more light must be on (otherwise $g(a_1, \ldots, a_n)$ will be infinite, which is a contradiction by Theorem 1.0.1). □

In a personal communication [480], Koren mentioned to Wilf that in fact it can be proved that every sweep interval of length a_1 produces a new light on.

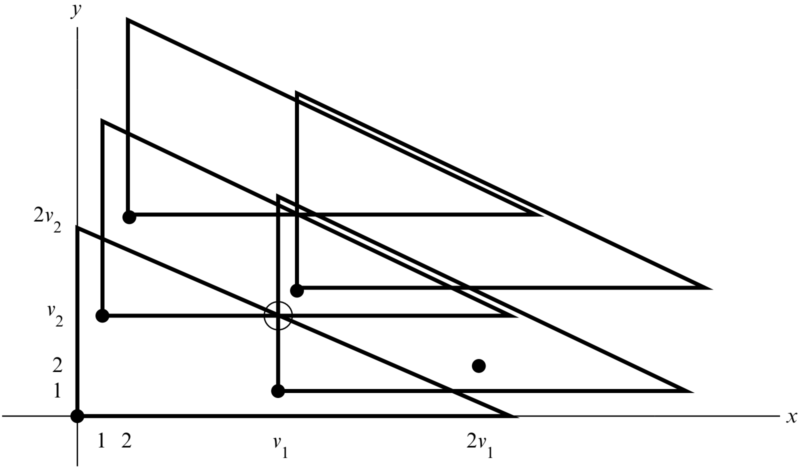

Figure 3.1: Copies of the simplex $\mu_{\mathbf{0}}(\mathbf{v})$ covering $\mathbb{R}^2$.

In [31], Beck *et al.* used their results on denumerants (see Section 4.1) to show the following upper bound.

Theorem 3.1.10 *[31] Let $a_1 \leq \cdots \leq a_n$ with $(a_1, \ldots, a_n) = 1$. Then,*

$$g(a_1, \ldots, a_n) \leq \frac{1}{2}\left(\sqrt{a_1a_2a_3(a_1 + a_2 + a_3)} - a_1 - a_2 - a_3\right).$$

Proof. It can be easily verified that

$$g(a_1, \ldots, a_n) \leq g(a_1, a_2, a_3).$$

The result follows by combining this and Theorem 2.3.10. □

Selmer [392] has remarked that if each element of the basis is independent (*i.e.* has no representation by the other elements in the basis) then $n \leq \min a_i$, the verification of this is immediate. Assume $\min a_i = a_1$ and $n \geq a_1 + 1$, so the number of elements $a_1, \ldots, a_n$ is at least a_1. Then, there is either an $i \geq 2$ such that $a_i \equiv 0 \bmod a_1$, or $i, j \geq 2$ with $a_i \equiv a_j \bmod a_1$ leading in both cases to a dependence between basis elements. Selmer used this easy argument to get the following upper bound.

Theorem 3.1.11 *[392] Let $a_1, \ldots, a_n$ be positive integers with $(a_1, \ldots, a_n) = 1$. Then,*

$$g(a_1, \ldots, a_n) \leq 2a_n \left\lfloor \frac{a_1}{n} \right\rfloor - a_1.$$

This bound is *sometimes* smaller than the following bound[4] given by Erdős and Graham [131], the elegant proof of which is presented here[5].

Theorem 3.1.12 *[131] Let $a_1, \ldots, a_n$ be positive integers with $(a_1, \ldots, a_n) = 1$. Then,*

$$g(a_1, \ldots, a_n) \leq 2a_{n-1} \left\lfloor \frac{a_n}{n} \right\rfloor - a_n.$$

Proof. Let $A = \{0, a_1, \ldots, a_{n-1}\}$ be the set of residues modulo a_n and let

$$\mathcal{C} = \underbrace{A + \cdots + A}_{m} = \{b_1 + \cdots + b_m \mid b_k \in A\} \bmod a_n,$$

where $m = \lfloor \frac{a_n}{n} \rfloor$. By a strong theorem of Kenser [245] there exists a (minimal) divisor g' of a_n such that

$$\mathcal{C} = \underbrace{A^{(g')} + \cdots + A^{(g')}}_{m} \operatorname{mod} a_n,$$

where

$$A^{(g')} = \{a + rg' \mid 0 \leq r < a_n/g', a \in A\} \bmod a_n,$$

and such that

$$\frac{|\mathcal{C}|}{a_n} \geq \frac{mn}{a_n} - \frac{m-1}{g'}. \tag{3.5}$$

Assume that $\mathcal{C}$ does not contain a complete system of residues modulo a_n. Since $(a_1, \ldots, a_n) = 1$ then $A^{(g')}$ must consist of more than one congruence class modulo g'. By the theorem of Kneser and the minimality of g', it follows that $\mathcal{C}$ must contain at least $m+1$ distinct residue classes modulo g'. Thus,

$$\frac{|\mathcal{C}|}{a_n} \geq \frac{m+1}{g'}. \tag{3.6}$$

Note that $a_n \geq n$ and $m = \lfloor \frac{a_n}{n} \rfloor$ imply

$$m + 1 > \frac{1}{2} \left(\frac{m-1}{\frac{mn}{a_n} - \frac{1}{2}} \right). \tag{3.7}$$

Suppose now that $|\mathcal{C}| \leq \frac{1}{2} a_n$. By eqns (3.5) and (3.7) we have

$$\frac{mn}{a_n} - \frac{m-1}{g'} \leq \frac{1}{2}, \qquad g' \leq \frac{m-1}{\frac{mn}{m} - \frac{1}{2}} < 2(a_n + 1).$$

[4] This upper bound has been used to the study of the *partition of vector space* problem; see Section 8.3.

[5] Reproduced from [131] with kind permission of *Acta Arithmetica*.

Hence, by eqn (3.6),

$$\frac{|\mathcal{C}|}{a_n} \geq \frac{m+1}{g'} > \frac{m+1}{2(m+1)} = \frac{1}{2},$$

which is a contradiction. We may therefore assume that $|\mathcal{C}| > \frac{1}{2}a_n$. But in this case it is easily seen that $\mathcal{C}+\mathcal{C}$ contains a complete residue system modulo a_n. It follows that the least possible integer not representable in the form

$$x_1b_1 + \cdots + x_{2m}b_{2m} + xa_n,$$

with $x_i \geq 0$, $x \geq 0$ and $b_i \in A$ is given by

$$2m \cdot \max_{a \in A} a - a_n = 2a_{n-1}\left\lfloor \frac{a_n}{n} \right\rfloor - a_n.$$

□

Erdős and Graham showed that the upper bound of Theorem 3.1.12 is asymptotically sharp. Moreover, in the case $n = 2$ and a_2 is odd we have $g(a_1, a_2) \leq 2a_1\lfloor \frac{a_2}{2} \rfloor - a_2 = a_1a_2 - a_1 - a_2$, which is best possible (*cf.* Theorem 2.1.1). Rødseth [379] gave another proof of Theorem 3.1.12 (using additive number theory) and improved it when n is odd.

Theorem 3.1.13 *[379] Let n be an odd integer. Then,*

$$g(a_1, \ldots, a_n) \leq 2a_n\left\lfloor \frac{a_1+2}{n+1} \right\rfloor - a_1.$$

Vitek [466] has proved inductively the following bound for independent sequences.

Theorem 3.1.14 *[466] Let $a_1 < \cdots < a_n$ be an independent sequence with $n \geq 2$. Then,*

$$g(a_1, \ldots, a_n) < \left\lfloor \frac{a_1}{2} \right\rfloor (a_n - n).$$

Proof. By induction on n. For $n = 2$ the result reduces to Theorem 2.3.13. We suppose that it is true for $n = k - 1$ and prove it for $n = k$. Let $(a_1, \ldots, a_{k-1}) = d$, then clearly $(d, a_k) = 1$ and $(a_1/d, \ldots, a_{k-1}/d) = 1$ so by the induction hypothesis we have

$$g\left(\frac{a_1}{d}, \ldots, \frac{a_{k-1}}{d}\right) < \left\lfloor \frac{a_1}{2d} \right\rfloor \left(\frac{a_{k-1}}{d} - k + 1\right).$$

All multiples of d starting with $\lfloor \frac{a_1}{2d} \rfloor \left(\frac{a_{k-1}}{d} - k + 1\right) d$ are representable as a non-negative linear combination of $a_1, \ldots, a_{k-1}$. On the other hand, all numbers from $g(d, a_k)+1 = (d-1)(a_k-1)$ onwards are representable in the form $\alpha a_k + hd$ with $0 \le \alpha < d$, $h \ge 0$. It follows that

$$\begin{aligned} g(a_1, \dots, a_k) &< \left\lfloor \frac{a_1}{2d} \right\rfloor \left(\frac{a_{k-1}}{d} - k + 1 \right) d + (d-1)(a_k - 1) \\ &\le \left\lfloor \frac{a_1}{2} \right\rfloor \left(\frac{a_{k-1}}{d} - k + 1 \right) + (d-1)(a_k - 1). \end{aligned}$$

Since the set is independent then $1 \le d \le \lfloor \frac{a_1}{2} \rfloor$ (in fact $d \le \lfloor \frac{a_1}{k} \rfloor$). Therefore, if $d = 1$ we have that

$$g(a_1, \dots, a_k) < \left\lfloor \frac{a_1}{2} \right\rfloor (a_{k-1} - k + 1) \le \left\lfloor \frac{a_1}{2} \right\rfloor (a_k - k),$$

and if $d = \lfloor \frac{a_1}{2} \rfloor$ then

$$\begin{aligned} g(a_1, \dots, a_k) &< a_{k-1} - \left\lfloor \frac{a_1}{2} \right\rfloor k + \left\lfloor \frac{a_1}{2} \right\rfloor + \left\lfloor \frac{a_1}{2} \right\rfloor a_k - \left\lfloor \frac{a_1}{2} \right\rfloor - a_k + 1 \\ &\le a_{k-1} + \left\lfloor \frac{a_1}{2} \right\rfloor (a_k - k) - a_k + 1 \\ &\le \left\lfloor \frac{a_1}{2} \right\rfloor (a_k - k). \end{aligned}$$

Then, $g(a_1, \dots, a_k) < \lfloor \frac{a_1}{2} \rfloor (a_k - k)$ for any $1 \le d \le \lfloor \frac{a_1}{2} \rfloor$. □

Shen [419] generalized Vitek's bound by showing that

$$g(a_1, \dots, a_n) \le \left(\frac{a_1 - n - 1 - l}{\lceil \frac{1}{2}(n+1) \rceil + 1} \right) a_n - a_1 - l - 2,$$

where l is the least non-negative integer such that $\left\lceil \frac{1}{2}(n+1) \right\rceil$ divides $a_1 - s - 1 + l$. Vitek used Theorem 3.1.14 to prove the following two theorems.

Theorem 3.1.15 *[466] Let $a_1 < \cdots < a_n$ and let i be the first index such that $a_i \ne \lambda a_1$ for any non-negative integer λ. If there is an a_j such that $a_j \ne \mu a_1 + \nu a_i$ for any pair of non-negative integers μ and ν then*

$$g(a_1, \dots, a_n) < \left\lfloor \frac{a_1}{2} \right\rfloor (a_n - 2)\,,$$

otherwise

$$g(a_1, \dots, a_n) = a_1 a_i - a_1 - a_i.$$

Proof. The existence of such a_j implies the existence of a maximal independent subset $\{a_1, a_{v_1}, \ldots, a_{v_t}\} \subseteq \{a_1, a_1, \ldots, a_n\}$, $t \geq 2$ where $(a_1, a_{v_1}, \ldots, a_{v_t}) = 1$. Then, by Theorem 3.1.14, we have

$$g(a_1, \ldots, a_n) = g(a_1, a_{v_1}, \ldots, a_{v_t}) < \left\lfloor \frac{a_1}{2} \right\rfloor (a_{v_t} - t) \leq \left\lfloor \frac{a_1}{2} \right\rfloor (a_n - 2)\,.$$

□

Theorem 3.1.16 *[466] Let $a_1 < \ldots < a_n$ be positive integers such that $(a_1, \ldots, a_n) = 1$. Then,*

$$g(a_1, \ldots, a_n) < \left\lfloor \frac{(a_2 - 1)(a_n - 2)}{2} \right\rfloor.$$

Proof. Let a_i and a_j be defined as in Theorem 3.1.15. If there exists such a_j, then

$$\begin{aligned} g(a_1, \ldots, a_n) &< \left\lfloor \frac{a_1}{2} \right\rfloor (a_n - 2) \leq \left\lfloor \frac{1}{2}(a_2 - 1) \right\rfloor (a_n - 2) \\ &\leq \frac{(a_2 - 1)(a_n - 2)}{2}. \end{aligned}$$

Otherwise, we have for $i = 1$,

$$g(a_1, \ldots, a_n) = a_1 a_2 - a_1 - a_2 < \left(\frac{a_n}{2} - 1\right)(a_2 - 1) = \frac{(a_2 - 1)(a_n - 2)}{2}.$$

For $i > 1$ we have, by definition of a_i, that $a_2 = \lambda a_1$, $\lambda \geq 2$. Then,

$$\begin{aligned} g(a_1, \ldots, a_n) &< (a_1 - 1)(a_i - 1) = (a_2/\lambda - 1)(a_i - 1) \\ &\leq \left(\frac{a_1}{2} - 1\right)(a_n - 1) < \frac{(a_2 - 1)(a_n - 2)}{2}. \end{aligned}$$

□

Notice that for $n = 3$ Theorem 3.1.16 is Lewin's bound given in Theorem 6.1.2 and for $n > 3$ it is stronger.

In [469], Vizvári analysed the accuracy of some of the above upper bounds by considering the so-called *Knapsack* problem[6]. Vizvári [469]

[6] The *Knapsack* problem is a classical model in operation research literature. Suppose there are n objects, the $i{-}th$ having a positive integer 'weight' a_i and 'utility' u_i. It is desired to find the most valuable subset of objects, subject to the restriction that their total weight does not exceed b, the 'capacity' of a knapsack. The knapsack problem has the following formulation as an integer programming.

$$\begin{array}{ll} \text{Maximize} & \sum_{i=1}^{n} u_i x_i \\ \text{subject to} & \sum_{i=1}^{n} a_i x_i \leq b, \end{array}$$

where $x_i = 1$ if object i is chosen and 0 otherwise.

noted that the problem class where the known upper bounds behave arbitrarily bad had the property that $a_1+1=a_2$. Vizvári then applied this approach to obtain new upper bounds for this special class.

Theorem 3.1.17 *[469] If $a_1+1=a_2$ and $2a_1 \geq a_n$ then*

$$g(a_1,\ldots,a_n) \leq \sum_{j=2}^{n} a_j \left(\frac{a_{j+1}-a_j}{a_j-a_1}\right) - a_1 \text{ where } a_{n+1}=2a_1.$$

The following two results are special cases of Theorem 3.1.17 by remarking that if $a_1,\ldots,a_n$ are arbitrary positive integers but $a_1+1=a_2<a_3<\cdots<a_n<2a_1$ then the numbers $q_1,\ldots,q_{n-1}$ can be chosen so $q_j=\frac{a_{j+2}-a_1}{a_{j+1}-a_1}$, $j=1,\ldots,n-1$ where $a_{n+1}=2a_1$.

Theorem 3.1.18 *[469] Let $q_1,\ldots,q_{n-1}$ be arbitrary rational numbers and suppose that $a_1=q_1\cdots q_{n-1}$, $a_2=a_1+1$, $a_3=a_1+q_1$, $a_4=a_1+q_1q_2,\ldots,a_n=a_1+q_1\cdots q_{n-2}$ are integers. Then,*

$$g(a_1,\ldots,a_n) \leq (q_1+q_2+\cdots+q_{n-1}-n-1)a_1-1.$$

Hujter [209] showed that if the numbers $q_1,\ldots,q_{n-1}$, in Theorem 3.1.18, are integers then equality holds.

Theorem 3.1.19 *[207,209] For an arbitrary positive integer q, we have that*

$$g(q^{n-1},q^{n-1}+1,q^{n-1}+q,\ldots,q^{n-1}+q^{n-2})=(n-1)(q-1)q^{n-1}-1.$$

Boros [55] showed that the assumption $2a_1 \geq a_n$ of Theorem 3.1.17 is not essential.

Theorem 3.1.20 *[55] Let $a_1,d_2,\ldots,d_n,h_2,\ldots,h_n$ be positive integers satisfying $0<d_2\leq d_3\leq\ldots\leq d_n$, $\frac{h_2}{d_2}\geq\frac{h_3}{d_3}\geq\ldots\geq\frac{h_n}{d_n}$ and $d_2=(d_2,\ldots,d_n)$ with $(a_1,d_2)=1$. If k denotes the greatest index for which $d_k<a_1d_2$ and $a_j=ha_1+d_j$, $j=2,\ldots,n$ then*

$$g(a_1,\ldots,a_n) \leq a_1d_2-a_1-d_2+a_1\left(h_2\left(\frac{d_3}{d_2}-1\right)+\cdots\right.$$
$$\left.+h_{k-1}\left(\frac{d_k}{d_{k-1}}-1\right)+h_k\left(\frac{a_1d_2}{d_k}-1\right)\right).$$

Let us briefly describe the simple idea used by Boros in order to prove the above theorem (as well as Theorem 3.6.9). Define the function

$$v(r)=\min\{-x_1+x_2+\cdots+x_n | r=a_1x_1+(a_2-a_1)x_2+\cdots+(a_n-a_1)x_n\},$$

where $r, x_1, \ldots, x_n$ are non-negative integers. It is clear that the greatest integer r with $v(r) > 0$ is $g(a_1, \ldots, a_n)$. Thus, if $u(r)$ (resp. $l(r)$) is an upper bound (resp. lower bound) for $v(r)$ then the greatest r for which $u(r) > 0$ (resp. $l(r) > 0$) is an upper bound (resp. lower bound) for $g(a_1, \ldots, a_n)$. Then, Boros used methods and results from the theory of *subadditive* theory[7] to obtain upper and lower bounds for $v(r)$.

As remarked by Kan [225], Rødseth algorithm (see Section 1.1.1) is based on certain special sequences (sequences where each term, other than the first and last one, is the divisor of the sum of its neighbours). In [225], Kan investigated this approach to obtain new formulas for $g(a_1, \ldots, a_n)$. Recall that $a_{-m}, a_{-m+1}, \ldots, a_{-1}, a_0, a_1, \ldots, a_n$ with $m, n \geq 1$, $(a_0, a_1) = 1$ is a *chain sequence* if

$$l_j = \frac{a_{j-1} + a_{j+1}}{a_j} \text{ for each } j = -m+1, \ldots, 0, 1, \ldots, n-1 \text{ are naturals.}$$

Let $\varepsilon, \varepsilon_1, \varepsilon_2$ be the numbers defined by

$$\varepsilon = \cfrac{1}{l_1 - \cfrac{1}{l_2 - \cfrac{1}{\ddots - \cfrac{1}{l_n}}}} \qquad \varepsilon_1 = \cfrac{1}{l_{-1} - \cfrac{1}{l_{-2} - \cfrac{1}{\ddots - \cfrac{1}{l_{-m+1}}}}} \text{ and } \varepsilon_2 = -\varepsilon_1.$$

For the cases $n = 1$ and $m = 1$ it is assumed that $\varepsilon = \varepsilon_1 = 0$.

Theorem 3.1.21 *[225] (a) If* $a_0 = \min\{a_0, \ldots, a_n\}$ *then*

$$g(a_1, \ldots, a_n) = a_0 a_1 - a_0 - a_1 - a_0 \varepsilon (a_0 - 1).$$

(b) If $a_0 = \min\{a_{-m}, a_{-m+1}, \ldots a_0, \ldots, a_n\}$ *then*

$$g(a_{-m}, \ldots, a_n) = -a_0 + \max\left\{ a_1 \left\lfloor \frac{a_0\varepsilon_2 - a_1}{\varepsilon_2 - \varepsilon} \right\rfloor - a_0 \left\lfloor \varepsilon \left\lfloor \frac{a_0\varepsilon_2 - a_1}{\varepsilon_2 - \varepsilon} \right\rfloor \right\rfloor, \right.$$
$$\left. -a_1 \left\lfloor \frac{a_1\varepsilon - a_0}{\varepsilon_2 - \varepsilon} \right\rfloor - a_0 \left\lfloor -\varepsilon_2 \left\lfloor \frac{a_1 - \varepsilon a_0}{\varepsilon_2 - \varepsilon} \right\rfloor \right\rfloor \right\}.$$

Notice that Theorem 3.1.21 (a) generalizes Theorem 5.1.1 and Theorem 2.3 is a particular case of Theorem 3.1.21 (b).

[7] A function $f : V \rightarrow \mathbb{R} \cup \{+\infty\}$ is said to be *subadditive* on the *monoid* $(V, +)$ if $g(x + y) \leq g(x) + g(y)$ for every $x, y \in V$. Recall that a set V of elements (integers, vectors, etc.) is said to be *monoid* $(V, +)$ if it is closed under the addition.

Lu and Wu [282] found a formula for the following set of special sequences. Let $t_i = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ and $a'_i = a_i/(t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n)$. Then,

$$g(a_1, \ldots, a_n) = \left(\sum_{i=1}^{n} a'_i + g(a'_1, a'_2, \ldots, a'_n) \right) t_1 \cdots t_n - \sum_{i=1}^{n} a_i. \tag{3.8}$$

Note that $g(a'_1, a'_2, \ldots, a'_n) = -1$ when some $a'_i = 1$ (this special case was also rediscoverd by Niu in [312]).

Krawczyk and Paz [255] presented a polynomial time algorithm for the computation of a bound for the Frobenius number.

Theorem 3.1.22 *[255] Let α_i, $1 \le i \le n$ be the minimal integer α such that there exists non-negative integers x_i such that*

$$\sum_{\substack{j=1 \\ j \neq i}}^{n} x_j a_j = \alpha a_i - 1, \tag{3.9}$$

and let $B = \sum_{i=1}^{n} (\alpha_i - 1) a_i$. Then,

$$\frac{B}{n} - 1 \le g(a_1, \ldots, a_n) \le B - 1.$$

Proof. We first prove that $B \le n(g(a_1, \ldots, a_n) + 1)$. To this end, we show that $(\alpha_i - 1)a_i \le g(a_1, \ldots, a_n) + 1$ for any $1 \le i \le n$. Suppose it is not true, that is, $(\alpha_i - 1)a_i > g(a_1, \ldots, a_n) + 1$ then, by the definition of $g(a_1, \ldots, a_n)$, the equation $a_1 x_1 + \cdots + a_n x_n = (\alpha_i - 1)a_i - 1$ has a solution over the non-negative integers, implying that the equation

$$a_1 x_1 + \cdots + a_{i-1} x_{i-1} + a_{i+1} x_{i+1} + \cdots + a_n x_n = (\alpha_i - 1 - x_i) a_i - 1$$

leads to a contradiction with the minimality of α_i. Hence,

$$B = \sum_{i=1}^{n} (\alpha_i - 1) a_i \le \sum_{i=1}^{n} (g(a_1, \ldots, a_n) + 1) = n(g(a_1, \ldots, a_n) + 1).$$

Now, to prove the upper bound we show that for any $m \ge B - 1$ there exist non-negative intgers x_i such that $a_1 x_1 + \cdots + a_n x_n = m$. To this end, we show that if for any $m > B - 1$ a solution exists, then a solution also exists for $m - 1$. Let $\beta_1, \ldots, \beta_n$ be a solution for such a m, that is,

$$a_1 \beta_1 + \cdots + a_n \beta_n = m, \tag{3.10}$$

where β_i are non-negative integers. As $m > B - 1$, there exists some index i, $1 \leq i \leq n$ such that $\beta_i > \alpha_i - 1$. On the other hand, by the definition of α_j, there exist non-negative integers α_i' such that

$$\alpha_1' a_1 + \cdots + \alpha_{i-1}' a_{i-1} - \alpha_i a_i + \alpha_{i+1}' a_{i+1} + \cdots + \alpha_n' a_n = -1. \quad (3.11)$$

Combining eqns (3.10) and (3.11) we get that

$$\begin{gathered}(\beta_1 + \alpha_1')a_1 + c \ldots + (\beta_{i-1} + \alpha_{i-1})a_{i-1} + (\beta_i - \alpha_i)a_i \\ +(\beta_{i+1} + \alpha_{i+1}')a_{i+1} \cdots + (\beta_n + \alpha_n')a_n = m - 1,\end{gathered}$$

where $\beta_i - \alpha_i \geq 0$ since $\beta_i > \alpha_i - 1$. Thus, $m - 1$ is representable by $a_1, \dots, a_n$ as desired. □

Theorem 3.1.23 *[255] The bound B given in Theorem 3.1.22 can be computed in polynomial time for every fixed value n.*

Proof. Finding a minimal α_i in eqn (3.9) is an integer linear problem (minimize $\sum_{j=1\ j\neq i}^{n} x_j a_j$ such that $\sum_{j=1\ j\neq i}^{n} x_j a_j = \alpha a_i - 1$). Thus, in order to find the values α_i we have to solve n such problems but this can be done by using Lenstra's polynomial algorithm for the integer linear programming [264]. □

Up to the Krawczyk and Paz paper, no bound that for fixed n is of the same order of magnitude as $g(a_1, \dots, a_n)$ and computable in polynomial time, was known.

3.2 Bounds in terms of the $lcm(a_1, \dots, a_n)$

Motivated by the investigation of the theory of *concurrency*, Chrząstowski-Wachtel [92] encoutered **FP** and obtained the following upper bound. We denote by $[a_1, \dots, a_n]$ the least common multiple of integers $a_1, \dots, a_n$.

Theorem 3.2.1 *[92] Let $a_1, \dots, a_n$ be positive integers with* $(a_1, \dots, a_n) = 1$. *Then,*

$$g(a_1, \dots, a_n) \leq (n-1)[a_1, \dots, a_n].$$

Proof. The result follows from Theorem 3.1.2 by observing that

$$T(a_1, \dots, a_n) = \sum_{i=1}^{n-1} a_{i+1} d_i / d_{i+1} \leq (n-1)[a_1, \dots, a_n] - \sum_{i=1}^{n} a_i,$$

with $d_i = (a_1, \dots, a_i)$ since each of the first $n-1$ components of T is at most $[a_1, \dots, a_n]$. □

Raczunas and Chrząstowski-Wachtel [337] continued related investigations and found a reduction formula for $g(a_1, \dots, a_n)$ in terms of $[a_1, \dots, a_n]$ for what they called *flat* and *strongly flat systems*. The sequence $a_1, \dots, a_n$ is called *flat* (resp. *strongly flat*) if and only if there exists i such that $a_i = \prod_{j=1}^{n} q_j/q_i$ (resp. if and only if $a_i = \prod_{j=1}^{n} q_j/q_i$ for all i) where $q_j = (a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n)$.

Theorem 3.2.2 *[337] (a) The sequence $a_1, \dots, a_n$ is flat if and only if*

$$g(a_1, \dots, a_n) = \sum_{i=1}^{n} (q_i - 1)a_i - \prod_{i=1}^{n} a_i.$$

(b) The sequence $a_1, \dots, a_n$ is strongly flat if and only if

$$g(a_1, \dots, a_n) = (n-1)[a_1, \dots, a_n] - \sum_{i=1}^{n} a_i.$$

Notice that Theorem 3.2.2 (a) and (b) characterize those sequences for which equality is reached in the inequalities given in Theorem 3.1.2 and Theorem 3.2.1, respectively. Also note that Theorem 3.2.2 (b) is a generalization of Theorem 2.1.1 since all systems for $n = 2$ are strongly flat.

In [67–69], Brimkov and Bârneva found the following upper bound in terms of the least common multiple of a_i and a_j with $i \neq j$

$$g(a_1, \dots, a_n) \leq \min_{j=1,\dots,n} \left\{ \sum_{i \neq j} [a_i, a_j] - \sum_{i \neq j} a_i \right\}.$$

Herzog [191] used the following lemma to investigate *complete intersection* semigroups; see Section 7.3.2.

Lemma 3.2.3 *[191] Let $d_i = (a_1, \dots, a_i)$ with $d_n = 1$ and assume that $[d_i, a_{i+1}]$ is representable by $a_1, \dots, a_i$ for each $i = 1, \dots, n-1$. Then,*

$$g(a_1, \dots, a_n) = \sum_{i=1}^{n-1} [d_i, a_{i+1}] - \sum_{i=1}^{n} a_i.$$

Moreover, z is representable by $a_1, \dots, a_n$ if and only if $g(a_1, \dots, a_n) - z$ is not for all $z \in \mathbb{Z}$ (that is, the semigroup generated by $a_1, \dots, a_n$ is symmetric*; see Section 7.2).*

Proof. Let $c_i = d_{i-1}/d_i$, $1 < i \leq n$. Then, $[d_i, a_{i+1}] = \frac{d_i a_{i+1}}{(d_i, a_{i+1})} = \frac{d_i a_{i+1}}{d_{i+1}} = c_{i+1} a_{i+1}$. Since $d_{j+k} | a_j$ and $d_{j+k} | d_k$ for all $k \geq 0$ then $c_i | a_j$

for all $i > j$. So, if $z = \sum_{i=1}^{n} x_i a_i$ then $0 \le x_i < c_i$, $2 \le i \le n$. We claim that z is representable by $a_1, \ldots, a_n$ if and only if $x_1 \ge 0$. Clearly, if z is representable then $x_1 \ge 0$. Conversely, by contradiction, suppose that $x_1 < 0$ then $\sum_{i=2}^{n} x_i a_i = x_1 a_1$ with $x_1 \ne 0$ and $|x_i| < c_i$, $2 \le i \le n$. Let $k > 0$ be the greatest integer such that $x_k \ne 0$ (there exists such k since $x_1 < 0$). Since c_i divides a_j for all $i > j$ then $x_k a_k = x_1 a_1 - \sum_{i=2}^{k-1} x_i a_i \equiv 0 \bmod c_k$ and then

$$x_k \frac{a_k}{\prod\limits_{i>k} c_i} \equiv 0 \bmod c_k,$$

and as $\left(\frac{a_k}{\prod_{i>k} c_i}, c_k\right) = \left(\frac{a_k}{d_k}, \frac{d_{k-1}}{d_k}\right) = 1$, we find that $x_k \equiv 0 \bmod c_k$, which is a contradiction since $|x_k| < c_k$. Now,

$$\begin{aligned}\sum_{i=1}^{n-1}[d_i, a_{i+1}] - \sum_{i=1}^{n} a_i - z &= \sum_{i=1}^{n-1} c_{i+1}a_{i+1} - \sum_{i=1}^{n} a_i - z \\ &= \sum_{i=2}^{n} c_i a_i - \sum_{i=2}^{n} a_i - a_1 - \sum_{i=2}^{n} x_i a_i - x_1 a_1 \\ &= (-1 - x_1)a_1 + \sum_{i=2}^{n}(c_i - x_i - 1)a_i.\end{aligned}$$

Hence, $\sum_{i=1}^{n-1}[d_i, a_{i+1}] - \sum_{i=1}^{n} a_i - z$ is representable if and only if $-1 - x_1 \ge 0$, that is, if and only if $x_1 < 0$ or equivalently, by the above claim, $\sum_{i=1}^{n-1}[d_i, a_{i+1}] - \sum_{i=1}^{n} a_i - z$ is representable if and only if z is not representable by $a_1, \ldots, a_n$. □

Note that Lemma 3.2.3 also generalizes Theorem 5.1.1.

3.3 Arithmetic and related sequences

Brauer [57] found the Frobenius number for k consecutive positive integers $m, m+1, \ldots, m+k-1$.

Theorem 3.3.1 *[57] Let a be a positive integer. Then,*

$$g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1\right) a - 1.$$

The sequence $a_1, \ldots, a_n$ is called *arithmetic* if $a_{i+1} = a_i + d$ for each $i = 1, \ldots, n-1$ with d a positive integer. Roberts [355] generalized the above theorem for general arithmetic sequences.

Theorem 3.3.2 *[355] Let a, d and s be positive integers with $(a, d) = 1$. Then,*

$$g(a, a+d, \dots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1) - 1.$$

Note that Theorem 3.3.2 contains Theorem 3.3.1 when $s = k - 1$ and $d = 1$. Roberts' proof is elementary but very involved. We present here a much simpler proof of Theorem 3.3.2 due to Bateman [29].

Proof of Theorem 3.3.2. Let $y_i = \sum_{j=i}^{s} x_j$ for $i = 0, \dots, s$. It is clear that a positive integer L has a representation by $\sum_{i=0}^{s}(a + id)x_i$ if and only if $L = ay_0 + d(y_1 + \cdots + y_s)$ with $y_0 \geq \cdots \geq y_s \geq 0$.

Now, for a given y_0, the integers representable in the form $y_1 + \cdots + y_s$ with $y_0 \geq \cdots \geq y_s$ are precisely the integers z such that $0 \leq z \leq sy_0$. Thus,

L has a representation by $a, a+d, \dots, a+sd$ if and only if $L = ay + dz$ with $0 \leq z \leq sy$.

Observation 3.3.3 *Let $R = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1)$ and suppose that $r \geq R$. Since $(a, d) = 1$ then there exists an integer z such that $dz \equiv r \bmod a$ and $0 \leq z \leq a - 1$. Hence, $r - dz = ay$ where y is an integer. Further,*

$$\begin{aligned} ay = r - dz &\geq r - d(a-1) \geq R - d(a-1) \\ &= \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a - (a-1) > \left\lfloor \frac{a-2}{s} \right\rfloor a. \end{aligned}$$

Thus, $y > \lfloor \frac{a-2}{s} \rfloor$; that is, $y \geq \lfloor \frac{a-2}{s} \rfloor + 1$. Since $s\left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) > a - 2$, then

$$sy \geq s\left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) \geq a - 1 \geq z.$$

Therefore, $r = ay + dz$ with $0 \leq z \leq sy$ and thus, by Observation 3.3.3, r has a representation by $a, a+d, \dots, a+sd$. Finally, let $r = R - 1$ and suppose that y and z are integers such that $r = ay + dz$ with $z \geq 0$. Since

$$\begin{aligned} R - 1 &= \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1) - 1 \\ &= \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + d(a-1) - a, \end{aligned}$$

then $z \equiv a - 1 \bmod a$. Hence, $z \geq a - 1$ and $y \leq \lfloor \frac{a-2}{s} \rfloor$. Hence,

$$sy \leq s\left\lfloor \frac{a-2}{s} \right\rfloor \leq a - 2 < a - 1 \leq z.$$

Therefore r cannot be of the form $r = ay + dz$ with $0 \le z \le sy$ and, again, by Observation 3.3.3, r does not have a representation by $a, a + d, \ldots, a + sd$. □

Zheng [489] also found a new proof for Theorem 3.3.2; see [271,357, 374,455] as well. Selmer [392] generalized Robert's result.

Theorem 3.3.4 *[374, 392] Let a, h, d and k be positive integers with $(a, d) = 1$. Then,*

$$g(a, ha + d, ha + 2d, \ldots, ha + kd) = ha \left\lfloor \frac{a-2}{k} \right\rfloor + a(h-1) + d(a-1).$$

In [374], Rødseth also found the above formula and studied the almost arithmetic sequences, obtaining the following result; see also [423].

Theorem 3.3.5 *[374] Let a, h, d, k be positive integers with $(a, d) = 1$. Let $c = a + Kd$, $k \le K$ and put $a = \alpha K + \beta$, $0 \le \beta < K$. If $\beta = 0$ or $\alpha + d \ge \left\lfloor \frac{K-\beta-1}{k} \right\rfloor$ then*

$$g(a, a + d, \ldots, a + kd, c) = c\alpha - d + \max\left\{ a \left\lfloor \frac{\beta-2}{2} \right\rfloor + d\beta, a \left\lfloor \frac{K-2}{2} \right\rfloor - a \right\}.$$

Note that the formulas given by Dulmage and Mendelsohn [122] in Theorem 2.4.1 easily follow from Rødseth's formula. Hofmeister [198] gave a formula for $g(a, a+d, a+dt, \ldots, a+t^{n-2}d)$ provided that a, d, t are positive integers $a, t > 1$, $(a, d) = 1$ and d exceeds a certain (rather large) bound. Selmer [392] found Hofmeister's formula in the case when $d = 1$ and $t = 2$ without asking any extra condition, this is given by

$$\begin{aligned} &g(a, a+1, a+2, a+2^2, \ldots, a+2^{n-2}) \\ &\quad = (a+1)\left(\frac{a}{2^{n-2}}\right) + \sum_{i=0}^{n-3} 2^i \left\lfloor \frac{a+2^i}{2^{n-2}} \right\rfloor + (n-4)a - 1. \qquad (3.12) \end{aligned}$$

Notice that eqn (3.12) generalizes Theorem 2.4.1.

3.4 Regular bases

Let $A_n = \{a_0, a_1, \ldots, a_n\}$ with $a_0 > 1, (a_0, a_1) = 1$. If necessary by reindexing $a_2, \ldots, a_n$, Marstrander [287] gives A_n in the following *ordered form*

$$\begin{cases} a_i = a_1 b_i - a_0 c_i, \; i = 1, 2, \ldots, n+1 \; (a_{n+1} = 0) \\ 1 = b_1 < b_2 < \cdots < b_k < b_{n+1} = a_0 \\ 0 = c_1 < c_2 < \cdots < c_k < c_{k+1} = a_1. \end{cases}$$

To obtain this, some dependent bases are excluded (but there may still be dependencies in a basis in the ordered form). Set $B_n = \{1, b_2, \ldots, b_{n+1}\}$ and $C_n = \{0, c_2, \ldots, c_{n+1}\}$. Since $b_1 = 1$, any positive integer may be expressed by the basis $\{1, b_2, \ldots, b_j\}$, $j \leq n+1$, as $m = \sum_{i=1}^{j} x_i b_i$ with $x_i \geq 0$ (in many ways). Denote the (unique) *regular* representation by $m = \sum_{i=1}^{j} e_i b_i$. Now define $R(m,j) = \sum_{i=1}^{j} x_i c_i$, $R(m) = R(m,n)$ and $M(m,j) = \max\{\sum_{i=1}^{j} x_i c_i | m = \sum_{i=1}^{j} x_i b_i\}$. Marstrander [287] defined the (ordered) basis A_n to be *regular* if $R(m, n+1) = M(m, n+1)$ for every natural number m. This property depends on the choice of the (coprime) basis elements a_0 and a_1. Marstrander [287] used regular bases to improve some results given by Hofmeister in [198, 199].

Theorem 3.4.1 *[287] If A_n is regular and $a_1 > a_0 \max\limits_{2 \leq i \leq n} \{c_i - R(b_i - 1)\}$, then*

$$g(a_0, \ldots, a_n) = g(a_0, a_1) - a_0 R(a_0 - 1).$$

Selmer [395] extended the definitions and the results of Marstrander's paper and made a connection between regular bases and the *postage stamp* problem (see Chapter 6).

3.5 Extending basis

Suppose that the basis $a_1, \ldots, a_n$ is extended with a new element a_{n+1}. Selmer [392, Section 4] was the first to examine the influence of a_{n+1} on $g(a_1, \ldots, a_n)$. It is immediately clear that $g(a_1, \ldots, a_{n+1}) \leq g(a_1, \ldots, a_n)$. By showing that $g(a_1, a_2)$ has a representation by a_1, a_2 and a_3, Mendelsohn [292] proved the strict inequality in the case $n = 2$.

Theorem 3.5.1 *[292] Let a_1, a_2 and a_3 be relatively prime integers. Let s be an integer such that $a_3 \equiv s a_2 \bmod a_1$. Then, $g(a_1, a_2, a_3) < g(a_1, a_2)$ if $s a_2 > a_3$.*

Proof. The integer s always exists since $(a_1, a_2) = 1$, moreover, $1 < s < a_1$. Thus, $a_3 = s a_2 - t a_1$, so $t a_1 = s a_2 - a_3 > 0$ and since $a_1 > 0$ then $t > 0$. Hence,

$$g(a_1, a_2) = (t-1)a_1 + (a_1 - s - 1)a_2 + a_3,$$

with $t - 1 \geq 0$ and $a_1 - s - 1 \geq 0$ since $a_1 \geq s + 1$. Then, $g(a_1, a_2)$ is representable by integers a_1, a_2 and a_3. □

Kirfel [237] determined a condition under which $g(a_1, a_2, a_3, a_4) = g(a_1, a_2, a_3)$; see also [295]. Selmer [392] has pointed out that we can add a new term $c = a + kd$ (assuming $k < a$) to the arithmetic sequence

$A = \{a, a+d, a+2d, \ldots, a+(k-1)d\}$ where $d > 0$, and $(a,d) = 1$ without altering $g(A)$ if

$$\left\lfloor \frac{a-2}{k-1} \right\rfloor = \left\lfloor \frac{a-2}{k} \right\rfloor,$$

which is always possible by an appropriate choice of a and k.

In [354], Ritter gave the set of all independent numbers c satisfying $g(A,c) = g(A)$ when $A = \{a, a+d, \ldots, a+(k-1)d\}$. Moreover, in the case $a > k$, Ritter gave a set B of maximal cardinality such that $g(A \cup B) = g(A)$. Ritter [353] also studied the following question.

Question 3.5.2. *Which subsets of the generalized arithmetic sequence $A_k = \{a, ha+d, ha+2d, \ldots, ha+(k-1)d\}$ with $d, h > 0$ and $(a,d) = 1$ can be omitted without altering the value of $g(A_k)$?*

Theorem 3.5.3 *[353] Let l_k be the greatest number of elements that can be omitted from A_k without altering $g(A_k)$. Then,*

a) $1 - \frac{4}{\sqrt{k}} \leq \frac{l_k}{k} \leq 1 - \frac{3}{k}$ for every $k \geq 3$ provided $a > k$, or $a = k$ with $d > 2h\sqrt{k}$,

and b) $1 - \frac{4}{k} \leq \frac{l_k}{k} \leq 1 - \frac{3}{k}$ if $q > (k-4)k + 3$ and $k > 5$.

For Ritters' result it is assumed that $a \geq k$. Ritter [354] remarked that if $\bar{l}$ represents the greatest number of independent elements that can be added to $A = (a, a+d, \ldots, a+kd)$ without altering $g(A)$ then $\bar{l}$ and l_k behave quite differently. Frőberg *et al.* [149] have also studied the extending bases problem and came up with a complete characterization of sequences $a_1, \ldots, a_n$ such that there is an integer a_{n+1}, independent of $a_1, \ldots, a_n$ with $g(a_1, \ldots, a_n) = g(a_1, \ldots, a_n, a_{n+1})$. Their characterization is given in terms of semigroups (*cf.* Theorem 7.2.4).

3.6 Lower bounds

In this section, we discuss the known lower bounds for the Frobenius number. For the case $n = 3$, Davison [104] found the following bound.

Theorem 3.6.1 *[104] Let a_1, a_2, a_3 be integers such that $(a_1, a_2, a_3) = 1$. Then,*

$$g(a_1, a_2, a_3) \geq \sqrt{3}\sqrt{a_1 a_2 a_3} - a_1 - a_2 - a_3.$$

Davison [104] showed that the bound in Theorem 3.6.1 is sharp, that is, the constant $\sqrt{3}$ cannot be replaced by a larger value with the inequality remaining true for all a_1, a_2 and a_3. A slighly weaker lower bound (replacing 3 by 2) will be proved later on (see Theorem 3.6.5). Hujter [210] has given the following bounds.

Theorem 3.6.2 *[210] Let a_1, a_2, a_3 be integers such that $(a_1, a_2, a_3) = 1$. Then,*

$$2 \geq \liminf_{\frac{a_1 a_2}{a_3} \to \infty} \frac{g(a_1, a_2, a_3)}{\sqrt{a_1 a_2 a_3}} \geq \sqrt{2}.$$

Moreover, for any positive number h we have

$$(g(a_1, a_2, a_3) + h + a_1 + a_2 + a_3)^3 - (g(a_1, a_2, a_3) + 1)^3 \geq 6h\sqrt{a_1 a_2 a_3}.$$

General lower bounds are also known. For instance, Hujter [209] proved that

Theorem 3.6.3 *[209] Let n be a fixed integer. Then,*

$$1 > \liminf_{t \to \infty} \min_{a_1, \ldots, a_n \geq t} \frac{g(a_1, \ldots, a_n)}{(n-1)(\min a_j)^{1 + \frac{1}{(n-1)}}} > \frac{n-1}{ne}.$$

The proof for the upper bound of Theorem 3.6.3 is obtained by using Theorem 3.1.19, while the proof for the lower bound uses the following nice result also due to Hujter [209].

Theorem 3.6.4 *[209] Let $a_1, \ldots, a_n$ be integers such that $(a_1, \ldots, a_n) = 1$. Then,*

$$g(a_1, \ldots, a_n) \geq \left(\frac{n-1}{n}\right) ((n-1)! a_1 a_2 \cdots a_n)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$$

Proof. Consider the following linear condition

$$a_1 x_1 + \cdots + a_n x_n \leq g(a_1, \ldots, a_n) + h, \tag{3.13}$$

with $x_i \geq 0$, $i = 1, \ldots, n$ and h an arbitrary positive number. Let M be the number of non-negative solutions for which eqn (3.13) holds (obviously the vector $\mathbf{0}$ is one such solution). Thus, by inequality (4.9.2), we have

$$M \leq \frac{\left(g(a_1, \ldots, a_n) + h + \sum\limits_{i=1}^{n} a_i\right)^n}{n! \prod\limits_{i=1}^{n} a_i}.$$

By the definition of $g(a_1, \ldots, a_n)$, each number in the set $E = \{g(a_1, \ldots, a_n) + 1, \ldots, g(a_1, \ldots, a_n) + \lfloor h \rfloor\}$ can be written in the form $\sum_{i=1}^{n} x_i a_i$ with $x_i \geq 0$. It is obvious that the vectors $x_1, \ldots, x_n$ differ from each other for different numbers in E and are not equal to the vector $\mathbf{0}$. So, $M-1 \geq \lfloor h \rfloor$ and we obtain

$$\frac{\left(g(a_1,\ldots,a_n)+h+\sum\limits_{i=1}^{n} a_i\right)^n}{n!\prod\limits_{i=1}^{n} a_i} \geq \lfloor h \rfloor > h,$$

that is

$$\frac{\left(g(a_1,\ldots,a_n)+h+\sum\limits_{i=1}^{n} a_i\right)^n}{h} > n!\prod_{i=1}^{n} a_i. \tag{3.14}$$

If we assume that $n, a_1, \ldots, a_n$ are fixed and h is a variable then we are interested in finding the minimum of the left-hand side of inequality (3.14). We then calculate $f(h)' = 0$ where $f(h) = (g+h+a)^n/h$ with $g = g(a_1,\ldots,a_n)$ and $a = \sum_{i=1}^{n} a_i$. We obtain that the minimum is given by $h^* = \frac{g+a}{n-1}$ and that

$$f(h^*) = \frac{\left(g+\frac{g+a}{n-1}+a\right)^n}{\frac{g+a}{n-1}} = \frac{\left(\frac{n(g+a)}{n-1}\right)^n}{\frac{g+a}{n-1}} = \frac{n^n(g+a)^{n-1}}{(n-1)^{n-1}}.$$

Thus, by eqn (3.14)

$$\frac{n^n(g+a)^{n-1}}{(n-1)^{n-1}} > n!\prod_{i=1}^{n} a_i,$$

or equivalently

$$\frac{n^{n-1}(g+a)^{n-1}}{(n-1)^{n-1}} > (n-1)!\prod_{i=1}^{n} a_i,$$

that is,

$$\left(\frac{n(g+a)}{n-1}\right)^{n-1} > (n-1)!\prod_{i=1}^{n} a_i,$$

from which the result follows. □

A lower bound has also been obtained by Killingbergtrø [236]

Theorem 3.6.5 *[236] Let $a_1,\ldots,a_n$ be integers such that $(a_1,\ldots,a_n)$=1. Then,*

$$g(a_1,\ldots,a_n) \geq ((n-1)!a_1a_2\cdots a_n)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$$

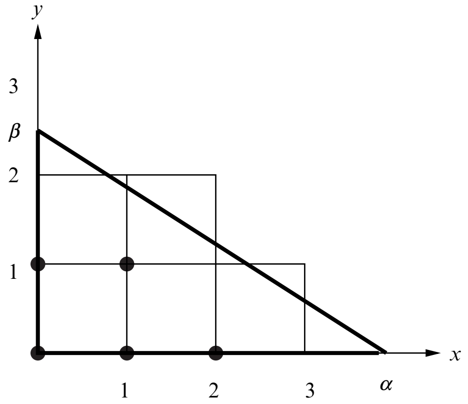

Figure 3.2: $\mathcal{R}[5,7,11]$ and its corresponding simplex (in bold lines).

The proof of Theorem 3.6.5 uses the cube-figure method (see Section 1.1.3). Let us see how this proceeds in the case $n = 3$ (an analogous idea can be applied for any $n \geq 4$).

A sketch of the proof of Theorem 3.6.5 when $n = 3$. Let $\mathcal{R}[a_1, a_2, a_3]$ be the cube-figure defined in Section 1.1.3. Let S be the simplex defined by points $(0,0), (\alpha, 0)$ and $(0, \beta)$ where $a_2\alpha = a_3\beta = \sqrt{2!a_1a_2a_3}$. Notice that this choice of α and β is such that

(a) $(a_2, a_3) \cdot (x, y)$ is constant for all points (x, y) lying on the hypotenuse of S, given by $y = -\beta/\alpha(x-\alpha)$, that is, $\alpha y + \beta x = \alpha\beta = 2a_1$,

and (b) the volume of $S = \alpha\beta/2 = 2a_1/2 = a_1$; see Fig. 3.2.

Since the volume of $\mathcal{R}[a_1, a_2, a_3]$ is also a_1 (*cf.* Remark 1.1.3) then there must be corners of $\mathcal{R}[a_1, a_2, a_3]$ lying just outside of S (*i.e.* not lying in either the interior or the boundary of S). Thus, we must have

$$g(a_1, a_2, a_3) \geq \sqrt{2!a_1a_2a_3} - a_1 - a_2 - a_3.$$

□

Example 3.6.6 From Example 1.1.4, we have that $\alpha = \frac{\sqrt{770}}{7}$ and $\beta = \frac{\sqrt{770}}{11}$; see Fig. 3.2. Thus, $g(5,7,11) \geq \lceil\sqrt{770}\,\rceil - 23 = 5$.

Example 3.6.7 From Example 1.1.5, we have that $\alpha a_2 = \beta a_3 = \gamma a_4 = (3!a_1a_2a_3a_4)^{1/3} \approx 1456.8$; see Fig. 3.3. Thus, $g(103, 133, 165, 228) \geq 1457 - 629 = 828$.

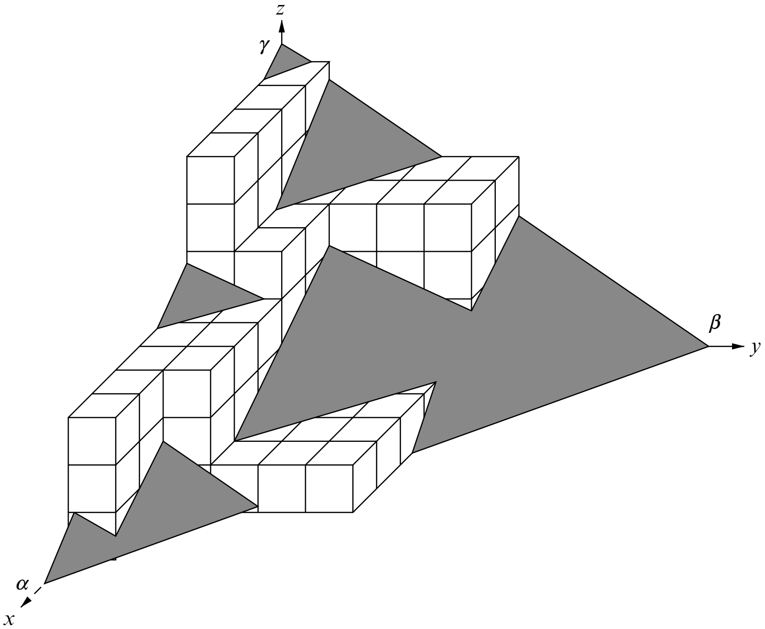

Figure 3.3: Cube-figure $\mathcal{R}'$ and its corresponding simplex.

Vizvári [471] studied the interrelation between **FP** and discrete optimization and gave different lower bounds by using the *Gomory cuts* method[8]. After stating a parametric knapsack problem, Vizvári showed that **FP** is equivalent to finding the value of the parameter where the optimal objective function value is maximal. Then Gomory's cutting plane method is applied to the knapsack problem. Let us mention one of the Vizvári's lower bounds (the other bounds, rather long and complicated, can be found in [471]).

Theorem 3.6.8 *[471] Let $a_1 < a_j$, for $j = 2, \ldots, n$ and let c_j and d_j be natural numbers such that $a_j = c_j a_1 + d_j$, where $1 \leq d_j < a_1$ and $\frac{c^*}{d^*} = \min\limits_{2 \leq j \leq n} \frac{c_j}{d_j}$. Then,*

$$g(a_1, \ldots, a_n) \geq \frac{c^*}{d^*} a_1^2 - \frac{c^*}{d^*} a_1 - 1.$$

[8] The *Gomory method* is one of the first methods to solve linear integer programming problems. It is based on the dual simplex method of linear programming; see [160–162] for further details.

The above bound is sharp when $n = 2$ and $d_2 = 1$. Moreover, if $d^* = 1$ then the bound is sharp in which case $d_j = 1$ for some $2 \leq j \leq n$ and $d^*|(a_1 - 1)$.

Boros [55] has also obtained another lower bound of similar flavour to the above theorem.

Theorem 3.6.9 *[55] Let a_i, c_i, c^* and d_i as in Theorem 3.6.8. Then,*

$$g(a_1, \ldots, a_n) \geq \left\lfloor \frac{d(a_1 - 1)c^*}{d^*} \right\rfloor a_1 + a_1 d - a_1 - d,$$

where $d = (d_2, \ldots, d_n)$.

3.7 Supplementary notes

Schoch [388, 389] presented another proof of Theorem 3.3.1 and calculated the Frobenius number for further special cases. Rødseth [379] gave a different proof of Theorem 3.1.4.

Gupta and Tripathi have studied the following problem: for a given set M of positive integers, a set S of non-negative integers is called an M-set if $a, b \in S$ implies $a - b \notin M$. In an upublished problem collection, Motzkin posed the problem of determing the quantity

$$\mu(M) = \sup_S \bar{\delta}(S),$$

where the supremum is taken over the class of all M-sets S and $\bar{\delta}(S)$ is defined as $\lim \sum_{n\to\infty} S(n)/n$, where $S(x)$ denotes the number of elements in S less than or equal to x. In [175], Gupta and Tripathi determined $\mu(M)$ in the case where the elements of M form an arithmetic progression. Their method gives a straightforward proof of Theorem 3.3.2.

In [374], Rødseth has provided a formula for $g(a, a + d, a + 2d, \ldots, a + kd, c)$ for positive integers a, c, d, k with $(a, d) = 1$ and Shao [412] obtained a formula for $g(a, a + d, a + 2d, \ldots, a + kd, a + (k + s)d)$ with $0 < s - 1 \leq 2k$. Tsang [458] gave a minimization approach for **FP** refining the latter result by Rødseth. The main tool of Tsang's proof is an explicit optimum value for the problem

$$\min_{x \geq \xi} \left\{ \delta x + \gamma \left\lfloor \frac{\beta x}{\alpha} \right\rfloor \right\},$$

with positive integers α, β, γ and δ and an arbitrary integer ξ. L'vovsky [284] gave the following upper bound by using some cohomological machinery

$$g(a_1, \ldots, a_n) \leq (\delta - 2)a_n + 1,$$

where $\delta = \max_{1\leq i<j\leq n} \{(a_i - a_{i-1}) + (a_j - a_{j-1})\}$ with $a_0 = 0$.

In [472], Vizvári applied greedy algorithms to the knapsack problem and proposed polynomial time algorithms that produce sharp estimates for **FP**. In many cases these estimates coincide with the exact solutions. This approach is simplified in [473] by using the optimal behaviour of the greedy method for the knapsack problem; see also [208, 211, 288].

Milanov [297] showed some connections between **FP** and particular discrete optimization problems. A relatively easy upper bound is computed by Djawadi and Hofmeister [118] when $a_{n-1} + 1 = a_n$. The covering radius approach used in [346] leads to a general lower bound. Cornuejols *et al.* [98] generalized Lemma 3.1.6 by applying techniques for decomposing the matrix of coefficients of a family of integer programs. In [1], Aardal and Lenstra also gave a similar formulation for computing the Frobenius number and obtained upper and lower bounds for **FP** when the sequences are of the form $a_i = p_iC + r_i$ for some special integers p_i, r_i and C. Tinaglia [447] has estimated $g(a_1, \ldots, a_n)$ when $(a_1, \ldots, a_k) = d_1$ and $(a_{k+1}, \ldots, a_n) = d_2$ with $(d_1, d_2) = 1$.

In [456], Tripathi investigated the following problem. Let $\Gamma(a_1, \ldots, a_n)$ denote the set of all non-negative integer combinations of $a_1, \ldots, a_n$, that is, Γ is the set of all integers representable by $a_1, \ldots, a_n$. Let

$$S = \{n \notin \Gamma | n + a \in \Gamma \text{ for any } a \in \Gamma\}.$$

Let g^* (respectively n^*) be the smallest integer (the number of elements) in S. Since $g(a_1, \ldots, a_n)$ is the largest integer in S then $g^* \leq g(a_1, \ldots, a_n)$ and $n^* \geq 1$ with equality if and only if $g^* = g(a_1, \ldots, a_n)$. Tripathi found the values of g^* and n^* when the sequence $a_1, \ldots, a_n$ is an arithmetic progression. The latter problem arises in the study of the derivation modules of certain curves [324].

Temkin [443] has also studied the Frobenius number for an almost arithmetic set and Boros [56] has determined the Frobenius number for *geometrical type* sequences. In [407], Sertöz and Özlük constructed, from integers $a_1, \ldots, a_n$, an infinite set I and showed that $g(a_1, \ldots, a_n)$ can be found from I; see also [52, 94, 405].

We finally mention that in [436, Section 1] Sun gave a brief survey on the Chinese research work about **FP**. Unfortunately the titles of the manuscripts, cited in the bibliography, are missing and the original sources [88, 247, 248, 281, 282] are not readily accessible.

4

Sylvester denumerant

4.1 From partitions to denumerants

Let $p(m)$ be the *partition function* of an integer m, *i.e.* the number of ways a positive integer m can be written as a sum of positive integers (without restriction). The theory of the general partition function of an integer m is an old problem (a detailed account of this theory can be found in [114, pages 101–64]). This theory was established at the end of the eighteenth century by Euler [136] who found the generating function of $p(m)$.

Theorem 4.1.1 *[136] The generating function of* $p(m)$ *is given by*

$$\prod_{i=1}^{\infty} \tfrac{1}{(1-z^i)}.$$

Euler also proved the following recursive relation

$$mp(m) = \sum_{k=1}^{m} p(m-k)\sigma(k),$$

where $\sigma(k)$ denotes the sum of the divisors of m. The importance of the partition theory was enhanced by Hardy and Ramanujan and Rademacher [339, 340]; see also [86]. Hardy and Ramanujan [185] proved for $p(m)$ the following asymptotic formula; see also [14].

$$p(m) \sim \frac{e^{\pi\sqrt{\frac{2m}{3}}}}{4\sqrt{3}m}.$$

Erdős [130] gave an elementary proof of the relation

$$p(m) \sim \frac{a \cdot e^{\pi(2/3)^{1/2}} m^{1/2}}{m},$$

but was unable to show that $a = \frac{1}{4\sqrt{3}}$. Krätzel [254] showed that $p(m) \leq 5^{m/4}$ with equality only when $m = 4$.

In 1857, Sylvester [438] investigated the number of partitions into specified parts, repeated or not and defined the function $d(m; a_1, \ldots, a_n)$, called the *denumerant*, as the number of non-negative integer representations of m by $a_1, \ldots, a_n$, that is, the number of solutions of the form

$$m = \sum_{i=1}^{n} x_i a_i,$$

with integers $x_i \geq 0$.

In [85, page 341], Cayley remarked

> *"The notion of a denumerant is, in fact, an important generalization of the notion of a number of partitions".*

Notice that $d(m; a_1, \ldots, a_n)$ is actually the number of partitions of m whose summands are taken (repetitions allowed) from the sequence $a_1, \ldots, a_n$. Apostol [14] generalized Euler's result by showing that

$$md(m; a_1, \ldots, a_n) = \sum_{k=1}^{m} d(m-k; a_1, \ldots, a_n)\sigma_n(k),$$

where $\sigma_n(k)$ denotes the sum of those a_i that divide m.

Sylvester [439] found the generating function[1] of $d(m; a_1, \ldots, a_n)$; see also [440].

Theorem 4.1.2 *[439] The generating function of $d(m; a_1, \ldots, a_n)$ is given by*

$$f(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})}.$$

Proof. Recall that $\frac{1}{1-z^r}$ has the expansion $\sum_{i=0}^{\infty} z^{ir}$ and let us restrict ourselves to $|z| < 1$ wherein convergence is absolute. By taking $r = a_1, \ldots, a_n$ we find

$$\begin{aligned}\prod_{i=1}^{n} \tfrac{1}{1-z^{a_i}} &= (1 + z^{1a_1} + z^{2a_1} + \cdots)(1 + z^{1a_2} + z^{2a_2} + \cdots)\\ &\quad \times \cdots \times (1 + z^{1a_n} + z^{2a_n} + \cdots)\\ &= \sum_{i_1=0}^{\infty} \sum_{i_2=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} z^{i_1 a_1 + \cdots + i_n a_n} = \sum_{i=0}^{\infty} c_i z^i,\end{aligned}$$

where c_m is the number of solutions of $i_1 a_1 + \cdots + i_n a_n = m$ in non-negative integers $i_1, \ldots, i_n$. That is, $c_m = d(m; a_1, \ldots, a_n)$. □

Remark 4.1.3 *$g(a_1, \ldots, a_n)$ is the greatest integer k* with *$f^k(0) = 0$.*

[1] A more general setting was previously pointed out by Euler; see Section 8.7.2.

4.2 Formulas and bounds for $d(m; a_1, \dots, a_n)$

The knowledge of an exact formula for $d(m; a_1, \dots, a_n)$ is not only of intrisic interest in number theory but also very important in other areas of mathematics; see Section 8.7. It is not surprising that finding formulas for denumerants is very difficult since even the problem of determing if $d(m; a_1, \dots, a_n) > 0$ is well known to be a $\mathcal{NP}$-complete problem [322, page 376]; see also [3]. Thus, approximations and formulas for $d(m; a_1, \dots, a_n)$ in particular cases are of great interest. In Section 4.3.1 some methods for computing $d(m; a_1, \dots, a_n)$ are explained.

In 1877, Laguerre [261] investigated the general behaviour of $d(m; a_1, \dots, a_n)$. In 1926, Schur [390] gave the following estimation for the value of $d(m; a_1, \dots, a_n)$.

Theorem 4.2.1 *[390] Let* $a_1, \dots, a_n$ *be positive integers with* $(a_1, \dots, a_n) = 1$ *and let* $P_n = \prod_{i=1}^{n} a_i$. *Then,*

$$d(m; a_1, \dots, a_n) \sim \tfrac{m^{n-1}}{P_n(n-1)!} \text{ as } m \to \infty.$$

Proof. Consider the generating function of $d(m; a_1, \dots, a_n)$, that is,

$$f(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})} = \sum d(m; a_1, \dots, a_n) z^m,$$

and let us simply look for one of the *heaviest* term in this expansion. $f(z)$ is a rational function whose poles all lie on the unit circle $|z| = 1$. The point $z = 1$ is a pole of multiplicity n because the denominator has an n-fold zero and so there will be a term $\frac{c}{(1-z)^n}$. All the other zeros are roots of unity (*i.e.* they are of the form $\omega = e^{2\pi i r/s}$ where $(r, s) = 1$) and all will be of order lower than n. Indeed, the multiplicity with which point ω occurs as a pole of $f(z)$ is equal to the number of a_is that are divisable by s that is stricly less than n since $(a_1, \dots, a_n) = 1$.

The coefficient of the term $\frac{c}{(1-z)^n}$ is $c \times \binom{m+n-1}{n-1}$ and the coefficients of all other terms $\frac{b}{(1-\omega z)^j}$ will be $b \times \omega^j \binom{n+j}{j-1}$. Thus the total sum of all these terms is negligible compared to the term $c \times \binom{m+n-1}{n-1}$ since $j < n$, hence for $m \to \infty$ we have $d(m; a_1, \dots, a_n) \sim c\binom{m+n-1}{n-1}$ or $d(m; a_1, \dots, a_n) \sim c\frac{m^{n-1}}{(n-1)!}$. Let us now find the value of c. The partial expansion of $f(z)$ is of the form

$$f(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})} = \frac{c}{(1 - z)^n} + O\left((1 - z)^{-n+1}\right),$$

multiply both sides by $(1-z)^n$ to get

$$\frac{(1-z)}{(1-z^{a_1})}\frac{(1-z)}{(1-z^{a_2})}\cdots\frac{(1-z)}{(1-z^{a_n})} = c + (1-z)^n O\left((1-z)^{-n+1}\right).$$

By L'Hopital's rule we have that $\lim_{z\to\infty}\frac{1-z}{1-z^{a_i}} = \frac{1}{a_i}$ while $(1-z)^n O\left((1-z)^{-n+1}\right) \to 0$ as $z\to\infty$. Thus, $c = \frac{1}{P_n}$ and

$$d(m;a_1,\ldots,a_n) \sim \tfrac{m^{n-1}}{P_n(n-1)!} \text{ as } m\to\infty.$$

□

This result was also found by Netto [307]; see also [333, Problem 27] and [182]. It is clear that Theorem 4.2.1 implies that for given integers $a_1,\ldots,a_n$ with $(a_1,\ldots,a_n)=1$ there exists a sufficiently large integer M so that $d(m;a_1,\ldots,a_n)\geq 1$ for any $m\geq M$; see Theorem 1.0.1. Erdős and Lehner [134] gave the following asymptotic formula

$$d(m;1,\ldots,k) \sim \frac{m^{k-1}}{k!(k-1)!} \tag{4.1}$$

that holds uniformly for $k=o(m^{1/3})$. In [408, Theorem 1], Sertöz and Özlük proved, by induction on n, the following more accuarate result.

$$d(m;a_1,\ldots,a_n) = \frac{m^{n-1}}{P_n(n-1)!} + O\left(m^{n-1}\right), \tag{4.2}$$

with $P_n = \prod_{i=1}^n a_i$ (the $O(\cdot)$ notation is used in the sense that $\lim_{m\to\infty}\frac{O(m^{n-1})}{m^{n-1}} = 0$). Blom and Frőberg [50] showed that

$$\frac{m^{n-1}}{P_n(n-1)!} \leq d(m;a_1,\ldots,a_n) \leq \frac{(m+s_n)^{n-1}}{P_n(n-1)!},$$

where $s_1 = 1, s_2 = a_2$ and $s_i = a_2 + \frac{1}{2}(a_3+\cdots+a_i)$ for $i\geq 3$. Recently, Nathanson [306] came out with a purely arithmetic proof of the following even more accurate result than eqn (4.2).

$$d(m;a_1,\ldots,a_n) = \frac{m^{n-1}}{P_n(n-1)!} + O(m^{n-2}). \tag{4.3}$$

In [408], Sertöz and Özlük gave the folllowing nice relation for $d(m;a_1,\ldots,a_n)$.

Theorem 4.2.2 *[408] Let $P_n = \prod_{i=1}^n a_i$, $S_n = \sum_{i=1}^n a_i$ and $m > P_n - S_n + n - 2$. Then,*

$$1 = \sum_{i=0}^{n-2}(-1)^i\binom{n-2}{i}\left(d(m-i;a_1,\ldots,a_n) - d(m-i-P_n;a_1,\ldots,a_n)\right)\cdot$$

Proof. Let $Q_n(z)$ be defined as

$$Q_n(z) = \frac{(1 - z^{P_n})(1 - z)^{n-2}}{(1 - z^{a_1}) \cdots (1 - z^{a_n})} - \frac{1}{1 - z}. \tag{4.4}$$

$Q_n(z)$ is a polynomial of degree $P_n - S_n + n - 2$ since every root of the denominator is a root of the denominator with the same multiplicity. By Theorem 4.1.2 we have

$$\frac{1}{\prod_{i=1}^{n}(1 - z^{a_i})} = \sum_{t=0}^{\infty} d(t; a_1, \ldots, a_n) z^t. \tag{4.5}$$

Substituting eqn (4.5) and the usual expansion of $\frac{1}{(1-z)}$ into eqn (4.4) we obtain

$$\begin{aligned}
Q_n(z) &= \sum_{t=0}^{\infty} \Big((1 - z^{P_n})(1 - z)^{n-2} d(t; a_1, \ldots, a_n) - 1 \Big) z^t \\
&= \sum_{t=0}^{\infty} \left((1 - z^{P_n}) \left(\sum_{i=0}^{n-2} \binom{n-2}{i} z^i (-1)^i \right) d(t; a_1, \ldots, a_n) - 1 \right) z^t \\
&= \sum_{t=0}^{\infty} \left(\left(\sum_{i=0}^{n-2} \binom{n-2}{i} (-1)^i (z^i - z^{P_n + i}) \right) d(t; a_1, \ldots, a_n) - 1 \right) z^t \\
&= \sum_{t=0}^{\infty} \sum_{i=0}^{n-2} \binom{n-2}{i} (-1)^i (z^{i+t} d(t; a_1, \ldots, a_n) \\
&\quad - z^{P_n + i + t} d(t; a_1, \ldots, a_n)) - z^t \\
&= \sum_{t=0}^{\infty} \sum_{i=0}^{n-2} \binom{n-2}{i} (-1)^i (d(t - i; a_1, \ldots, a_n) \\
&\quad - d(t - i - P_n; a_1, \ldots, a_n) - 1) z^t.
\end{aligned}$$

Since $Q_n(z)$ is a polynomial the coefficient of z^m is zero beyond the degree of $Q_n(z)$ and the result follows. □

In [5], Agnarsson used direct combinatorial methods to find the following upper and lower bounds for denumerants.

Theorem 4.2.3 *[5] Let $a_1, \ldots, a_n$ be positive integers with $(a_1, \ldots, a_n) = d$. Then,*

$$\frac{d}{P_n} \binom{m - B_n}{n - 1} \leq d(m; a_1, \ldots, a_n) \leq \frac{d}{P_n} \binom{m + A_n}{n - 1},$$

where the A_i's and B_i's are defined recursively as follows:

$$A_1 = 0 \text{ and } A_i = A_{i-1} + a_i^{\frac{(a_1,\ldots,a_{i-1})}{(a_1,\ldots,a_i)}}, \text{ for } 2 \leq i \leq n,$$

and

$$B_1 = 0 \text{ and } B_i = B_{i-1} + a_i\left(\tfrac{(a_1,\ldots,a_{i-1})}{(a_1,\ldots,a_i)}\right) - 1, \text{ for } 2 \leq i \leq n.$$

Sylvester [438] and Cayley [85] showed that

$$d(m; a_1, \ldots, a_n) = A_n(m) + R_n(m), \tag{4.6}$$

where $A_n(m)$ is a polynomial in m of degree $n-1$ and $R_n(m)$ is a periodic function of period $\prod_{i=1}^n a_i$; see [307, pages 319–320]. The coefficients of $A_n(m)$ for $n \leq 4$ can be found in [96, page 113].

In the case $n = 1$ we have $A_1(m) = 1/a_1$ and $R_1(m) = -1/a_1 + 1$ or $-1/a_1$ according to whether a_1 divides or not m. In the case $n = 2$ we have, by Theorem 4.4.1, that

$$A_2(m) = \frac{m}{a_1 a_2}, \quad R_2(m) = -\frac{1}{a_1}a_1' - \frac{1}{a_2}a_2' + 1,$$

where $a_1'a_1 \equiv -m \bmod a_2$, $1 \leq a_1' \leq a_2$ and $a_2'a_2 \equiv -m \bmod a_1$, $1 \leq a_2' \leq a_1$; see Theorem 4.4.1.

The polynomial part in eqn (4.6) when $n = 3$ can be obtained from the formulas in [96, page 113]. In particular, if a_1, a_2, a_3 are pairwise relatively prime positive integers then

$$A_3(m) = \frac{m(m + a_1 + a_2 + a_3)}{2a_1a_2a_3}.$$

Moreover, a result due to Popoviciu [335, page 28] states that for each $i = 1, 2, \ldots, a_1 + a_2 + a_3 - 1$ we have

$$R_3(a_1a_2a_3 - (a_1 + a_2 + a_3) + i) = \frac{i(a_1 + a_2 + a_3 - i)}{2a_1a_2a_3}.$$

We observe that if $(a_i, a_j) = 1$ for all $1 \leq i < j \leq n$ then the periodic part $R_n(m)$ in eqn (4.6) is expressible as a sum $\sum_{i=1}^n R_i$, where each R_i, is periodic with period a_i. Then, a linear system can be set up for the unknowns $R_i(j)$, $1 \leq i \leq n$ and $0 \leq j \leq a_i - 1$. And, solving this system by Gaussian elimination requires $O\left(\left(\sum_{i=1}^n a_i\right)^3\right)$ elementary operations. Beck *et al.* [33] have derived the following explicit formula for the polynomial part $A_n(m)$ (defined in eqn (4.6)).

$$A_n(m) = \frac{1}{a_1 \cdots a_n} \sum_{k=0}^{n-1} \frac{(-1)^k}{(n-1-k)!} \sum_{k_1+\cdots+k_n=m} a_1^{k_1} \cdots a_n^{k_n} \frac{B_{k_1} \cdots B_{k_n}}{k_1! \cdots k_n!} t^{n-1-k},$$

where B_j is the Bernoulli number (see Appendix B.5).

4.3 Computing denumerants

4.3.1 Partial fractions

The traditional method for computing denumerants is typically based on a decomposition of the rational fraction into partial fractions. This method can be helpful and easy to apply in some cases (see Example 4.3.1) but this is rare, normally it is more complicated and messy (see Example 4.3.2).

Example 4.3.1 We may compute $d(m;1,2)$.

$$\begin{aligned} f(z) = \frac{1}{(1-z)(1-z^2)} &= \frac{1}{4}\left(\frac{1}{1+z} + \frac{1}{1-z} + \frac{1}{(1-z)^2}\right) \\ &= \frac{1}{4}\left(\sum_{m\geq 0}(-z)^m + \sum_{m\geq 0} z^m + 2\sum_{m\geq 0}(m+1)z^m\right), \end{aligned}$$

which gives the value $d(m;1,2) = \frac{1}{4}(2m+3+(-1)^m)$ as a coefficient of z^m.

Example 4.3.2 (obtained from [184, pages 9–10]) We may compute $d(m;1,2,3)$.

$$\begin{aligned} f(z) = \frac{1}{(1-z)(1-z^2)(1-z^3)} &= \frac{1}{6(1-z)^3} + \frac{1}{4(1-z)^2} \\ &+ \frac{1}{72(1-z)} + \frac{1}{8(1+z)} + \frac{1}{9(1+z+z^2)} \\ &= \frac{1}{6(1-z)^3} + \frac{1}{4(1-z)^2} + \frac{1}{4(1-z^2)} + \frac{1}{3(1-z^3)}. \end{aligned}$$

We may use the fact that $\frac{1}{(1-\alpha z)^k}$ is just a constant times the $(m-1)-th$ derivative of $\frac{1}{(1-\alpha z)} = \sum \alpha^m z^m$. Thus, since

$$\frac{1}{(1-z)^2} = \frac{d}{dz}\frac{1}{(1-z)} = \frac{d}{dz}\sum z^m = \sum(m+1)z^m,$$

and

$$\frac{1}{(1-z)^3} = \frac{d}{dz}\frac{1}{2(1-z)^2} = \frac{d}{dz}\sum \frac{m+1}{2}z^m = \sum \frac{(m+2)(m+1)}{2}z^m,$$

then

$$d(m;1,2,3) = \frac{(m+2)(m+1)}{12} + \frac{(m+1)}{4} + \frac{s_1(m)}{4} + \frac{s_2(m)}{4}, \qquad (4.7)$$

where

$$s_1(m) = \begin{cases} 1 & \text{if } 2|m, \\ 0 & \text{otherwise} \end{cases} \qquad \text{and} \qquad s_2(m) = \begin{cases} 1 & \text{if } 3|m, \\ 0 & \text{otherwise.} \end{cases}$$

And eqn (4.7) can be shortened nicely into

$$d(m;1,2,3) = \left\lfloor \frac{m^2+6m+5}{12} \right\rfloor.$$

4.3.2 Bell's method

Bell [38] gave an elementary proof of the fact that, for any fixed q, $d(pm+q;a_1,\ldots,a_n)$ is a polynomial in m of degree $n-1$.

Theorem 4.3.3 *[38] Let p be the least common multiple of $a_1,\ldots,a_n$. Then, for any integer q such that $0 \le q \le p-1$ and every integer $s \ge 0$, we have*

$$d(ps+q;a_1,\ldots,a_n) = c_0 + c_1 s + \cdots + c_{n-1}s^{n-1},$$

where c_i are constants independent of s.

The constants are fully determined when the denumerant is known for n different values of s, say $s_1,\ldots,s_n$. Indeed, by *Lagrange's interpolation* formula

$$d(ps+q;a_1,\ldots,a_n) = \sum_{j=1}^{n} \frac{F_j(s)}{F_j(s_j)} d(ps_j+q;a_1,\ldots,a_n), \qquad (4.8)$$

where $F_j(x) = h(x)/(x-s_j)$ and $h(x) = (x-s_1)(x-s_2)\cdots(x-s_n)$. By putting $s_j = j$, eqn (4.8) becomes

$$d(ps+q;a_1,\ldots,a_n) = \binom{s-1}{n}\sum_{j=1}^{n}(-1)^{n-j}\binom{n}{j}\left(\frac{jd(jp+q;a_1,\ldots,a_n)}{s-j}\right). \qquad (4.9)$$

Example 4.3.4 Let us calculate $d(2s; 1, 2)$ by using Bell's result. From eqn (4.9) we have

$$\begin{aligned} d(2s; 1, 2) &= \binom{s-1}{2} \sum_{j=1}^{2} (-1)^{2-j} \binom{2}{j} \frac{jd(js; 1, 2)}{s-j} \\ &= \binom{s-1}{2} \left(\frac{-2d(2; 1, 2)}{s-1} + \frac{2d(4; 1, 2)}{s-2} \right). \end{aligned}$$

Since $d(2; 1, 2) = 2$ and $d(4; 1, 2) = 3$ then

$$d(2s; 1, 2) = \frac{(s-1)(s-2)}{2} \left(\frac{-4}{s-1} + \frac{6}{s-2} \right) = s + 1.$$

Notice that $d(2s; 1, 2)$ can also be obtained from Example 4.3.1 by taking $m = 2s$. Bell [39] also found the following determinant expression for $d(m; a_1, \ldots, a_n)$.

Theorem 4.3.5 *[39] Let $\phi_1(m)$ (resp. $\phi_2(m)$) be the number of partitions of integer m into an even (resp. odd) number of distinct parts chosen from integers $a_1, \ldots, a_n$. If $\phi(m) = \phi_1(m) - \phi_2(m)$ then*

$$\begin{aligned} &d(m; a_1, \ldots, a_n) \\ &= (-1)^m \begin{vmatrix} \phi(1) & \phi(2) & \phi(3) & \cdots & \phi(m-1) & \phi(m) \\ 1 & \phi(1) & \phi(2) & \cdots & \phi(m-2) & \phi(m-1) \\ 0 & 1 & \phi(1) & \cdots & \phi(m-3) & \phi(m-2) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & \phi(1) \end{vmatrix}. \end{aligned}$$

Example 4.3.6 We compute $d(5; 2, 3)$ via Bell's determinant. Figure 4.1 shows the values of ϕ_1, ϕ_2 and ϕ.

Thus, we have that

$$\begin{aligned} d(5; 2, 3) &= (-1)^5 \begin{vmatrix} 0 & -1 & -1 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{vmatrix} \\ &= (-1)(-1) \begin{vmatrix} -1 & -1 & 1 & 1 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{vmatrix} \end{aligned}$$

i	$\phi_1(i)$	$\phi_2(i)$	$\phi(i)$
1	0	0	0
2	0	1	-1
3	0	1	-1
4	1	0	1
5	1	0	1

Figure 4.1: The values of ϕ_1, ϕ_2 and ϕ.

$$\begin{aligned}
&= (-1)(-1)(-1)\begin{vmatrix} -1 & -1 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{vmatrix} \\
&= (-1)\left((-1)\begin{vmatrix} -1 & 1 \\ 1 & -1 \end{vmatrix} + (-1)\begin{vmatrix} -1 & -1 \\ 1 & 0 \end{vmatrix}\right) \\
&= (-1)((-1)0 + (-1)(1)) = 1,
\end{aligned}$$

which is correct, since $2x + 3y = 5$ has only the solution $(x, y) = (1, 1)$.

4.4 $d(m; p, q)$

Let p and q be positive integers. It is known that for any non-negative integer m if $m = qpq + s$ with $0 \leq s < pq$ then $d(m; p, q) = q + d(s; p, q)$. In fact,

$$d(m; p, q) = \begin{cases} 0 \text{ or } 1 & \text{if } 0 < m < pq, \\ 1 & \text{for all } pq - p - q < m < pq, \\ 0 & \text{if } m = pq - p - q. \end{cases} \tag{4.10}$$

Notice that $d(pq; p, q) = 2$ if $(p, q) = 1$, since $pq = x_1 p + x_2 q$ and either $x_1 = q$ and $x_2 = 0$ or $x_1 = 0$ and $x_2 = p$.

It is also known that $d(m; p, q)$ is always one of the two consecutive integers $\left\lfloor \frac{m}{pq} \right\rfloor$ or $\left\lfloor \frac{m}{pq} \right\rfloor + 1$; see for instance [313, page 214] or [481, page 90]. In 1953, Popoviciu [335] found the exact value of $d(m; p, q)$.

Theorem 4.4.1 *[335]Let p, q and m be positive integers with $(p, q) = 1$. Then,*

$$d(m; p, q) = \frac{m + pp'(m) + qq'(m)}{pq} - 1,$$

where $p'(m)p \equiv -m \bmod q$, $1 \leq p'(m) \leq q$ and $q'(m)q \equiv -m \bmod p$, $1 \leq q'(m) \leq p$.

Theorem 4.4.1 has been rediscovered by Sertöz [405] and by Tripathi [454] (the proofs of which involved generating functions). Recentely, Brown, *et al.* [74] gave a short simple proof that we present here; see also [481, page 90] and [96, pages 113–114].

Proof of Theorem 4.4.1. By equality (4.10), we may assume that $0 < m < pq - p - q$. Since pq divides $pp'(m) + qq'(m) + m$ (as both p and q divides $pp'(m)+qq'(m)+m$) and $0 < pp'(m)+qq'(m)+m < 3pq$ then either $pp'(m) + qq'(m) + m = pq$ or $2pq$.

Case I] If $pp'(m) + qq'(m) + m = pq$. We claim that $d(m; p, q) = 0$. Suppose that $d(m; p, q) > 0$ then there exist integers $s, t \geq 0$ such that $ps + qt = m$. Hence, $pp'(m) + qq'(m) + ps + qt = pq$ or equivalently $p(p'(m) + s) + q(q'(m) + t) = pq$. So, p divides $q'(m) + t$ and q divides $p'(m) + s$ but since $0 < q'(m) + t \leq p$ and $0 < p'(m) + s \leq q$ then $p = q'(m) + t$ and $q = p'(m) + s$ obtaining that $2pq = pq$, which is a contradiction

Case II] If $pp'(m) + qq'(m) + m = 2pq$. We just notice that $m = p(q - p'(m)) + q(p - q'(m))$. Then, $d(m; p, q) = 1$. □

Theorem 4.4.1 can be easily generalized when $(p, q) = d > 1$.

Corollary 4.4.2 *Let* $(p, q) = d > 1$. *Then,*

$$d(m; p, q) = \begin{cases} 0 & \text{if } d \not| \, m, \\ \frac{m+pp'(m)+qq'(m)}{[p,q]} - 1 & \textit{otherwise}, \end{cases}$$

where $p'(m)(\frac{p}{d}) \equiv -(m/d) \bmod (q/d)$ *and* $q'(m)(\frac{q}{d}) \equiv -(m/d) \bmod (p/d)$ *if* d *divides* m.

Theorem 4.4.1 gives a formula for $d(m; p, q)$, generalizing eqn (4.10).

Corollary 4.4.3 *Let* $(p, q) = 1$ *and let* $m = qpq + s$ with $0 \leq s < pq$. *Then,*

$$d(m; p, q) = \begin{cases} q + 1 & \textit{if } pq - p - q < s < pq, \\ q & \textit{if } s = pq - p - q, \\ q + 1 & \textit{if } s < pq - p - q \text{ and } pp'(s) + qq'(s) + s = 2pq, \\ q & \textit{if } s < pq - p - q \text{ and } pp'(s) + qq'(s) + s = pq, \end{cases}$$

where $p'(s)$ *and* $q'(s)$ *are defined as in Theorem 4.4.1.*

4.5 $d(m; a_1, a_2, a_3)$ and $d(m; a_1, a_2, a_3, a_4)$

In connection with **FP**, Sertöz and Özlük [408] have also investigated the function $d(m; a_1, \ldots, a_n)$ with $2 \leq n \leq 4$. They found the following old results due to Ehrhart [123, 124].

Theorem 4.5.1 *[123, 408] Let $S_n = \sum_{i=1}^{n} a_i$, $P_n = \prod_{i=1}^{n} a_i$ and let r_n and x_n be defined by $m = r_n P_n + x_n$ with $0 < x_n < P_n$. If $m \geq P_n$ then*

(a) $d(m; a_1, a_2) = \frac{m - x_2}{P_2} + d(x_2; a_1, a_2)$,

(b) $d(m; a_1, a_2, a_3) = \frac{m(m+S_3) - x_3(x_3+S_3)}{2P_3} + d(x_3; a_1, a_2, a_3)$,

(c) $d(P_3 - x_3; a_1, a_2, a_3) = d(P_3 - x_3 - 1; a_1, a_2, a_3) + 1$ *for* $1 \leq x_3 \leq S_3 - 2$,

(d)

$$\begin{aligned} d(m; a_1, a_2, a_3, a_4) = A &- Bd(P_4 - 2; a_1, a_2, a_3, a_4) \\ &+ (B + r_4) d(P_4 - 1; a_1, a_2, a_3, a_4) \\ &+ d(x_4; a_1, a_2, a_3, a_4), \end{aligned}$$

where $A = \frac{1}{2} \sum_{k=1}^{r_4} (m - kP_4 + 2)$ and $B = \frac{1}{2} r_4 (m + x_4 - P_4 + 2)$.

Proof. By putting $n = 2$ in the equation of Theorem 4.2.2 we have

$$d(m; a_1, a_2) = d(m - P_2; a_1, a_2) + 1.$$

Part (a) follows by successively substracting P_2 from m. We now put $n = 3$ in the same equation, obtaining

$$\begin{aligned} d(m; a_1, a_2, a_3) = d(m-1; a_1, a_2, a_3) &+ d(m - P_3; a_1, a_2, a_3) \\ &- d(m - P_3 - 1; a_1, a_2, a_3) + 1, \end{aligned}$$

which is valid for $m < deg(Q_3) = P_3 - S_3 + 1$. It can be found, inductively, that

$$\begin{aligned} d(m; a_1, a_2, a_3) = d(m-k; a_1, a_2, a_3) &+ d(m - P_3; a_1, a_2, a_3) \\ &- d(m - P_3 - k; a_1, a_2, a_3) + k. \end{aligned}$$

We replace k by $m - P_3$ (where $d(-t) = 0$ for any positive integer t) to obtain

$$d(m; a_1, a_2, a_3) = d(P_3; a_1, a_2, a_3) + d(m - P_3 - 1; a_1, a_2, a_3) + m - P_3.$$

Finally, by successively substracting P_3 from m we obtain

$$\begin{aligned} d(m; a_1, a_2, a_3) = \frac{m^2}{2P_3} &+ \left(\frac{2d(P_3; a_1, a_2, a_3) - P_3}{2P_3} \right) m \\ &+ \frac{x_3 P_3 - 2x_3 d(P_3; a_1, a_2, a_3) - x_3^3}{2P_3} + d(x_3; a_1, a_2, a_3) \cdot \end{aligned}$$

Part (b) follows by replacing Theorem 4.5.3 part (a) in the above equation.

Parts (c) and (d) can be obtained by similar (but more tedious) arguments as that used in part (b). □

The following useful proposition was given by Brown *et al.* [74].

Proposition 4.5.2. *[74] Let a_1, a_2, a_3 and m be non-negative integers. Let $S_3 = \sum_{i=1}^{3} a_i$, $P_3 = \prod_{i=1}^{3} a_i$. Then,*

$$d(m; a_1, a_2, a_3) = \begin{cases} d(m - S_3; a_1, a_2, a_3) + q(m; a_1, a_2, a_3) & \text{if } m \geq S_3, \\ q(m; a_1, a_2, a_3) & \text{otherwise,} \end{cases}$$

where $q(m; a_1, a_2, a_3) = d(m; a_2, a_3) + d(m; a_1, a_3) + d(m; a_1, a_2) - \epsilon_{a_1}(m) - \epsilon_{a_2}(m) - \epsilon_{a_3}(m)$ and

$$\epsilon_d(t) = \begin{cases} 1 & \text{if } d|t, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $E_{\{a_1,a_2,a_3\}}(m) = \{(x, y, z) | x, y, z \geq 0,\ \textit{integers and } a_1x + a_2y + a_3z = m\}$. Let $(x_1, y_1, z_1) \in E_{\{a_1,a_2,a_3\}}(m)$. If $0 < m < a_1 + a_2 + a_3$ then $x_1y_1z_1 = 0$. Thus, $d(m - a_1 - a_2 - a_3; a_1, a_2, a_3) = E_{\{a_1,a_2,a_3\}}(m) \setminus \{E_{\{a_1,a_2,0\}}(m) \cup E_{\{a_1,0,a_3\}}(m) \cup E_{\{0,a_2,a_3\}}(m)\}$ and the results follows by the inclusion-exclusion formula. □

Corollary 4.5.3 *[74, 123, 408] Let a_1, a_2 and a_3 be non-negative integers. Let $S_3 = \sum_{i=1}^{3} a_i$, $P_3 = \prod_{i=1}^{3} a_i$. Then,*

(a) $d(P_3; a_1, a_2, a_3) = \frac{P_3+S_3}{2} + 1,$

(b) $d(P_3 - S_3 + 1; a_1, a_2, a_3) = \frac{P_3-S_3}{2} + 1,$

(c) $d(P_3 - S_3; a_1, a_2, a_3) = \frac{P_3-S_3}{2} + 1,$

(d) $d(P_3 - S_3 - 1; a_1, a_2, a_3) = \frac{P_3-S_3}{2} - 1.$

Proof. Consider the following equality

$$d(P_3; a_1, a_2, a_3) = \sum_{i=0}^{P_2} d(P_3 - ia_3; a_1, a_2), \tag{4.11}$$

and define f_i and k_i as

$$P_3 - ia_3 = f_iP_2 + k_i \text{ with } 0 \leq k_i < P_2. \tag{4.12}$$

By Theorem 4.5.1 part (a) and by eqn (4.11) we have

$$d(f_iP_2 + k_i) = \frac{f_iP_2 + k_i - k_i}{P_2} + d(k_i; a_1, a_2) = f_i + d(k_i; a_1, a_2),$$

and thus

$$d(P_3; a_1, a_2, a_3) = \sum_{i=0}^{P_2} \left(f_i + d(k_i; a_1, a_2)\right). \tag{4.13}$$

Since $d(m; a_1, a_2) = 0$ for exactly half of the integers between 0 and $P_2 - S_2$ (*cf.* Theorem 5.1.1) and $d(m; a_1, a_2) = 1$ for $P_2 - S_2 + 1 \le m \le P_2$ (*cf.* Theorem 4.4.3) then

$$\sum_{i=0}^{P_2} d(k_i; a_1, a_2) = \sum_{i=0}^{P_2 - S_2} d(k_i; a_1, a_2) + \sum_{i=P_2-S_2+1}^{P_2} d(k_i; a_1, a_2) = \frac{P_2 + S_2 + 1}{2}\cdot \tag{4.14}$$

Now, the other sum in eqn (4.13), that is $\sum_{i=0}^{P_2} f_i$, is the number of lattice points in and on the triangle T (except the ones on the x-axis) defined by the line $P_2 y + a_3 x = P_3$ in the first quadrant (the latter follows by comparing this with eqn (4.12)). This set of lattice points can be computed by using Pick's theorem, that is, the area of T equals the number of interior lattice points of T plus half of the number of lattice points in its boundary minus one (see Theorem 2.1.2). Since the area of T is equals to $\frac{P_2 a_3}{2}$ and the number of lattice points in its boundary is $a_3 + P_2 + 1$ then the number of interior lattice points of T is $\frac{P_3 - a_3 - P_2 + 1}{2}$. So, the number of lattice points in and on the triangle T (except the ones on the x-axis) is

$$\frac{P_3 - a_3 - P_2 + 1}{2} + a_3 = \frac{P_3 + a_3 - P_2 + 1}{2},$$

and then

$$\sum_{i=0}^{P_2} f_i = \frac{P_3 - P_2 + a_3 + 1}{2}\cdot \tag{4.15}$$

Part (a) follows by adding eqns (4.14) and (4.15). Part (b) follows by combining Theorem 4.5.1 parts (a) and (b).

(c) By Proposition 4.5.2, we have

$$\begin{aligned} d(P_3 - S_3; a_1, a_2, a_3) = {} & d(P_3; a_1, a_2, a_3) - d(P_3; a_2, a_3) - d(P_3; a_1, a_3) \\ & - d(P_3; a_1, a_3) + \epsilon_{a_1}(P_3) + \epsilon_{a_2}(P_3) + \epsilon_{a_3}(P_3). \end{aligned}$$

From Corollary 4.4.3 part (a), we obtain that $d(P_3; a_2, a_3) = a_1 + 1$, $d(P_3; a_1, a_3) = a_2 + 1$ and $d(P_3; a_1, a_2) = a_3 + 1$. And, since $\epsilon_{a_1}(P_3) = \epsilon_{a_2}$ $(P_3) = \epsilon_{a_3}(P_3) = 1$ then

$$d(P_3 - S_3; a_1, a_2, a_3) = \frac{P_3 - S_3}{2} + 1.$$

(d) Again, from Proposition 4.5.2, we have

$$\begin{aligned} d(P_3 - S_3; a_1, a_2, a_3) = {} & d(P_3 - 1; a_1, a_2, a_3) - d(P_3 - 1; a_2, a_3) \\ & -d(P_3 - 1; a_1, a_3) - d(P_3 - 1; a_1, a_2) \\ & +\epsilon_{a_1}(P_3 - 1) + \epsilon_{a_2}(P_3 - 1) + \epsilon_{a_3}(P_3 - 1). \end{aligned}$$

By Theorem 4.5.1 part (b), we have that $d(P_3 - 1; a_1, a_2, a_3) = \frac{(P_3 - S_3)}{2} - 1$ and by Corollary 4.4.3, we obtain $d(P_3 - 1; a_2, a_3) = d((a_1 - 1)a_2a_3 + (a_2a_3 - 1); a_2, a_3) = a_1$ (similarly, $d(P_3 - 1; a_1, a_3) = d((a_2 - 1)a_1a_3 + (a_1a_3 - 1); a_1, a_3) = a_2$ and $d(P_3 - 1; a_1, a_2) = d((a_3 - 1)a_1a_2 + (a_1a_2 - 1); a_1, a_2) = a_3$). Since $\epsilon_{a_1}(P_3 - 1) = \epsilon_{a_2}(P_3 - 1) = \epsilon_{a_3}(P_3 - 1) = 0$ then

$$d(P_3 - S_3 - 1; a_1, a_2, a_3) = \frac{P_3 - S_3}{2} - 1.$$

□

In [74], Brown *et al.* found a recursive formula for $d(m; a_1, a_2, a_3)$.

Theorem 4.5.4 *[74] Let n be an integer with $1 \leq n \leq a_1a_2a_3 - a_1 - a_2 - a_3$ and let t be the largest integer such that $m - t(a_1 + a_2 + a_3) \geq 0$. Then,*

$$\begin{aligned} d(m; a_1, a_2, a_3) = {} & \frac{2m(t+1)S_3 - t(t+1)S_3^2}{2a_1a_3a_3} + \frac{1}{a_1}\sum_{i=0}^{t}(a_2'(a_1, m - iS_3) \\ & + a_3'(a_1, m - iS_3)) + \frac{1}{a_2}\sum_{i=0}^{t}(a_3'(a_2, m - iS_3) \\ & + a_1'(a_2, m - iS_3)) + \frac{1}{a_3}\sum_{i=0}^{t}(a_1'(a_3, m - iS_3) \\ & + a_2'(a_3, m - iS_3)) - \sum_{i=0}^{t}(\epsilon_{a_1}(m - iS_3) + \epsilon_{a_2}(m - iS_3) \\ & + \epsilon_{a_3}(m - iS_3)) - 3(t+1), \end{aligned}$$

where $v'(e, m)$ denotes the integer satisfying $vv'(e, m) \equiv -m \bmod e$ with positive integers, v, e, m such that $(v, e) = 1$ and with $\epsilon_d(t)$ defined as in Proposition 4.5.2.

Proof. By applying recursively Proposition 4.5.2, we have that

$$d(m; a_1, a_2, a_3) = \sum_{i=0}^{t-1} q(m - iS_3; a_1, a_2, a_3) + d(m - tS_3; a_1, a_2, a_3)$$

$$= \sum_{i=0}^{t} q(m - iS_3; a_1, a_2, a_3),$$

where $q(m; a_1, a_2, a_3)$ is defined as in Proposition 4.5.2. Hence,

$$\begin{aligned}\sum_{i=1}^{t} q(m - iS_3; a_1, a_2, a_3) = \sum_{i=1}^{t} &(d(m - iS_3; a_2, a_3) \\ &+ d(m - iS_3; a_1, a_3) + d(m - iS_3; a_1, a_2)) \\ &- \sum_{i=0}^{t} (\epsilon_{a_1}(m - iS_3) + \epsilon_{a_2}(m - iS_3) \\ &+ \epsilon_{a_3}(m - iS_3)) \,.\end{aligned}$$

The result follows by using Theorem 4.4.1. □

The following example illustrates Theorem 4.5.4.

Example 4.5.5 (Obtained from [74]) Let $a_1 = 5, a_2 = 7$ and $a_3 = 11$. Then, $S_3 = 23$ and $t = 1$. We may find $d(41; 5, 7, 11) = 3$. Indeed, there are exactly three partitions of 41 with parts in $\{5, 7, 11\}$, namely

$$\begin{aligned}41 &= 5 + 5 + 5 + 5 + 7 + 7 + 7 \\ &= 5 + 5 + 5 + 5 + 5 + 5 + 11 \\ &= 5 + 7 + 7 + 11 + 11.\end{aligned}$$

4.6 Hilbert series

In this section we will explain the connection of Hilbert series, denumerants and the Frobenius number (we refer the reader to Appendix B.3 for a basic presentation of modules, resolutions and Hilbert series needed throughout this section). Let k be a field and let $R = k[X_1, \ldots, X_n]$ be a graded polynomial ring where X_i has degree a_i, denoted by $deg(X_i) = a_i$ (sometimes called the *weight* or *graduation* of X_i) with a_i a non-negative integer. Then a monomial $X^{b_1} \cdots X^{b_n}$ has (weighted) degree $t = a_1b_1 + \cdots + a_nb_n$. This gives a grading on R such that R_t is the set of n-linear combinations of monomials of degree t.

It is not difficult to show (see proof of Theorem 4.1.2) that the Hilbert series of R is given by

$$H(R, z) = \sum_{t=0}^{\infty} \dim_k(R_t) z^t = \frac{1}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}, \tag{4.16}$$

where $\dim_k$ means dimension as a vector space over k. In other words, $H(R, z)$ is the generating function of $d(m; a_1, \ldots, a_n)$. Let $A[S] =$

$k[z^{a_1}, \ldots, z^{a_n}]$ be the *semigroup ring* over a field k associated to the semigroup $S =< a_1, \ldots, a_n >$ (note that $A[S]$ is a graded subring of $k[z]$). Then, it turns out that the generating function of the elements in S is actually the Hilbert series of $A[S]$, which is a rational function (see [433, 434]), that is,

$$H(A[S], z) = \sum_{i \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}. \tag{4.17}$$

Combining eqn (4.17) with the equality

$$\sum_{i \in S} z^s + \sum_{i \notin S} z^s = \frac{1}{1 - z}$$

we obtain that

$g(a_1, \ldots, a_n)$ is equal to the degree of the rational function $H(A[S], z)$.

We are thus interested in calculating $H(A[S], z)$. We notice that the $\mathcal{NP}$-hardness result on the **FP** given in Theorem 1.3.1 implies that the computation of $H(A[S], z)$ is a difficult task from the computational point of view. In fact, Bayer and Stillman [30] proved that the computation of Hilbert series is $\mathcal{NP}$-complete, in general.

By using a classical method to compute Hilbert series via graded resolution (see Appendix B.3), we obtain that, if

$$0 \longrightarrow R^{d_m} \longrightarrow R^{d_{m-1}} \longrightarrow \cdots \longrightarrow R^{d_1} \longrightarrow R \xrightarrow{I} A \longrightarrow 0$$

is a graded resolution of $A[S]$ where the map I is given by the kernel of the map

$$\phi : x_i \rightarrow z^{a_i}$$

for each i (I is sometimes called the *toric ideal* of the semigroup S) then

$$H(A[S], z) = \sum_{j=0}^{m} (-1)^j H(R^{d_j}, z), \tag{4.18}$$

where $d_0 = 1$. We illustrate how this approach works with the following two examples.

Example 4.6.1 We compute $g(11, 19, 23, 37)$ by calculating the Hilbert serie of the semigroup ring $A[S]$ associated to $S =< 11, 19, 23, 37 >$. Let $R = k[X, Y, Z, T]$, where $deg(X) = 11, deg(Y) = 19, deg(Z) = 23$ and $deg(T) = 37$. The graded resolution of $A[S]$ is given by

$$0 \rightarrow R^8 \overset{\psi_3}{\rightarrow} R^6 \xrightarrow{\psi_2} R^1 \xrightarrow{\psi_1} R \xrightarrow{I} A \rightarrow 0,$$

where the map I is given by the kernel of the map $X \to z^{11}$, $Y \to z^{19}$, $Z \to z^{23}$, $T \to z^{37}$ and homomorphism ψ_i is given by matrix M_i where

$$M_1 =$$
$$(X^3Z - YT \quad XZ^2 - Y^3 \quad ZT - X^2Y^2 \quad T^2 - YX^5 \quad X^8 - Z^3Y \quad Z^4 - TX^5)$$

$$M_2 = \begin{pmatrix} Z & T & Y^2 & X^2Y & X^5 & Z^3 & 0 & 0 \\ -X^2 & 0 & -T & 0 & 0 & 0 & Z^3 & 0 \\ Y & -X^3 & ZX & -T & 0 & 0 & -X^6 & -Z^3 \\ 0 & Y & 0 & Z & 0 & 0 & 0 & X^5 \\ 0 & 0 & 0 & 0 & -Z & -T & -Y^2 & X^2Y \\ 0 & 0 & 0 & 0 & -Y & -X^3 & -XZ & T \end{pmatrix}$$

and

$$M_3 = \begin{pmatrix} T & Z^3 & 0 \\ -Z & -X^5 & 0 \\ X^2 & 0 & Z^3 \\ Y & 0 & -X^6 \\ 0 & T & X^3Y \\ 0 & -Z & -Y^2 \\ 0 & X^2 & T \\ 0 & Y & XZ \end{pmatrix}.$$

Thus, by eqn (4.18) we have that the Hilbert series of $A[S]$ is given by

$$H(A[S], z) =$$
$$\frac{z^{56} + z^{57} + z^{60} + z^{74} + z^{88} + z^{92} - (z^{79} + z^{93} + z^{94} + z^{97} + z^{111} + z^{125} + z^{126} + z^{129}) + z^{116} + z^{148} + z^{163}}{(1 - z^{11})(1 - z^{19})(1 - z^{23})(1 - z^{37})}.$$

So, $g(11, 19, 23, 37) = 163 - 90 = 73$.

The following example shows that *symmetry* in semigroups (see Section 7.2) does not imply *complete intersection* (see Section 7.3.2).

Example 4.6.2 Let us compute g(5,6,7,8) by calculating the Hilbert serie of the semigroup ring $A[S]$ associated to $S =< 5, 6, 7, 8 >$. Let $R = k[X, Y, Z, T]$, where $deg(X) = 5, deg(Y) = 6$, $deg(Z) = 7$ and $deg(T) = 8$. The graded resolution of $A[S]$ is given by

$$0 \to R^5 \overset{\psi_3}{\to} R^5 \xrightarrow{\psi_2} R^1 \xrightarrow{\psi_1} R \xrightarrow{I} A \to 0,$$

where the map I is given by the kernel of the map $X \to z^5$, $Y \to z^6$, $Z \to z^7$, $T \to z^8$ and homomorphism ψ_i is given by matrix M_i where

$$M_1 =$$
$$(Y^2 - XZ \qquad YZ - TX \qquad Z^2 - TY \qquad X^3 - TZ \qquad T^2 - X^2Y)$$

$$M_2 = \begin{pmatrix} Z & T & 0 & X^2 & 0 \\ -Y & -Z & T & 0 & X^2 \\ X & Y & 0 & T & 0 \\ 0 & 0 & Y & Z & T \\ 0 & 0 & X & Y & Z \end{pmatrix},$$

and

$$M_3 = \begin{pmatrix} T^2 - X^2Y \\ X^3 - TZ \\ TY - Z^2 \\ YZ - TX \\ Y^2 - XZ \end{pmatrix}.$$

Thus, by eqn (4.18) we have that the Hilbert series of $A[S]$ is given by

$$H(A[S], z) = \frac{z^{12} + z^{13} + z^{14} + z^{15} + z^{16} - (z^{19} + z^{20} + z^{21} + z^{22} + z^{23}) + z^{35}}{(1 - z^5)(1 - z^6)(1 - z^7)(1 - z^8)}.$$

Then, $g(5, 6, 7, 8) = 35 - 26 = 9$.

4.7 A proof of a formula for $g(a_1, a_2, a_3)$

Let $a_1, a_2, a_3 > 1$ be pairwise relatively prime integers. After, Herzog [191, 258], it is known that if $R = k[X, Y, Z]$ is a polynomial ring graded by $deg(X) = a_1$, $deg(Y) = a_2$ and $deg(Z) = a_3$ is not a complete intersection (that is, if the semigroup $S =< a_1, a_2, a_3 >$ is not symmetric) then $A[S] = k[z^{a_1}, z^{a_2}, z^{a_3}]$ has graded resolution

$$0 \to R^2 \xrightarrow{M_2} R^3 \xrightarrow{M_1} R \xrightarrow{I} A \to 0, \tag{4.19}$$

where the map I is given by $X \to z^{a_1}$, $Y \to z^{a_2}$ and $Z \to z^{a_3}$.

Moreover, Herzog [191] proved that the toric ideal I of the semigroup $S =< a_1, a_2, a_3 >$ is generated by the entries of the matrix

$$M_1 = \begin{pmatrix} X^{L_1} - Y^{x_{12}} Z^{x_{13}} \\ Y^{L_2} - X^{x_{21}} Z^{x_{23}} \\ Z^{L_3} - X^{x_{31}} Y^{x_{32}} \end{pmatrix},$$

where L_i and $x_{i,j}$ are the integers appearing in the system of eqns (2.2).

We use these to calculate the Hilbert series of $A[S]$ from which the formula for $g(a_1, a_2, a_3)$, stated in Theorem 2.2.3, is obtained.

Proof of Theorem 2.2.3. In each case, we compute the Hilbert series of $H(A[S], z)$ by using eqn (4.18).

Case I] $x_{ij} > 0$ for all i, j. This case is reduced to find matrix M_2 as in eqn (4.19). We claim that M looks as follows

$$M_2 = \begin{pmatrix} Z^{x_{23}} & X^{x_{31}} & Y^{x_{12}} \\ Y^{x_{32}} & Z^{x_{13}} & X^{x_{21}} \end{pmatrix}.$$

Indeed,

$$\begin{aligned} M_2 \times M_1 &= \begin{pmatrix} Z^{x23} X^{L1} - Y^{x12} Z^{x13+x23} + X^{x31} Y^{L2} - X^{x21+x31} Z^{x23} + Y^{x12} Z^{L3} - X^{x31} Y^{x32+x12} \\ Y^{x32} X^{L1} - Y^{x12+x32} Z^{x13} + Z^{x13} Y^{L2} - X^{x21} Z^{x23+x13} + X^{x21} Z^{L3} - X^{x31+x21} Y^{x32} \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \end{aligned}$$

where the last equality follows by using Proposition 4.7.1 part (a). As all of the terms, in each entry, are homogeneous, we have that

$$u = a_3 x_{21} + a_1 L_1 = a_1 x_{31} + a_2 L_2 = a_2 x_{12} + a_3 L_3,$$

and

$$v = a_2 x_{32} + a_1 L_1 = a_3 x_{13} + a_2 L_2 = a_1 x_{21} + a_3 L_3.$$

So, by eqn (4.18), we have

$$H(A[S], z) = \frac{1 - z^{a_1 L_1} - z^{a_2 L_2} - z^{a_3 L_3} + z^u + z^v}{(1 - z^{a_1})(1 - z^{a_n})(1 - z^{a_3})}.$$

Therefore, the degree of $H(A[S], z)$ is $\max\{u, v\} - a_1 - a_2 - a_3$ and the formula follows.

Case II] $x_{ij} = 0$ for some i, j. Without loss of generality, suppose that $x_{12} = 0$. By Proposition 4.7.1 part (b), the toric ideal I is then generated by the entries of the matrix

$$M_1 = \begin{pmatrix} X^{L_1} - Z^{L_3} \\ Y^{L_2} - X^{x_{21}} Z^{x_{23}} \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

In this case, $A[S]$ has graded resolution

$$0 \to R \xrightarrow{M_2} R^2 \xrightarrow{M_1} R \xrightarrow{I} A \to 0,$$

where $M_2 = (b, -a)$. So, by eqn (4.18) again, we have

$$H(A[S], z) = \frac{1 - z^{a_1 L_1} - z^{a_2 L_2} + z^{a_1 L_1 + a_2 L_2}}{(1 - z^{a_1})(1 - z^{a_n})(1 - z^{a_3})} = \frac{(1 - z^{a_1 L_1})(1 - z^{a_2 L_2})}{(1 - z^{a_1})(1 - z^{a_n})(1 - z^{a_3})}.$$

And the degree of $H(A[S], z)$ is $a_1 L_1 + a_2 L_2 - a_1 - a_2 - a_3$. □

We finally prove the following proposition used in the above proof.

Proposition 4.7.1. *Let L_i, $i = 1, \ldots, 3$ and x_{ij} be the integers satisfying eqns (2.2).*

(a) *If $x_{ij} > 0$ for all i, j then*

$$\begin{aligned} L_1 &= x_{21} + x_{31} \\ L_2 &= x_{12} + x_{32} \\ L_3 &= x_{13} + x_{23}. \end{aligned}$$

(b) *If $x_{ij} = 0$ for some i, j then $L_i a_i = L_k a_k$, $k \neq j$ and $L_j a_j = x_{ji} a_i + x_{jk} a_k$ with $x_{ji}, x_{jk} > 0$.*

Proof. Part (a) can be easily checked as a consequence of minimality (see [191, Proposition 3.2]). Part (b) If $x_{ij} = 0$ for some i, j then $L_i a_i = x_{ik} a_k$ with $k \neq j$. We claim that $x_{kj} = 0$. We do this by contradiction. Suppose that $x_{kj} > 0$, we notice, by the minimality of L_k, that $x_{ik} \geq L_k$. Also note that $x_{ki} > 0$. So, we have

$$L_i a_i = x_{ki} a_i + (x_{ik} - L_k) a_k + x_{kj} a_j,$$

and thus

$$(L_i - x_{ki}) a_i = (x_{ik} - L_k) a_k + x_{kj} a_j,$$

with $x_{ik} - L_k \geq 0$ and $x_{kj} > 0$, which is a contradiction with the minimality of L_i. Thus, if $x_{ij} = x_{kj} = 0$ then $L_i a_i = x_{ik} a_k$ and $L_k a_k = x_{ki} a_i$. Now, the minimality of L_i implies that $(L_i, x_{ik}) = 1$ and then x_{ki} (resp. L_k) is a multiple of L_i (resp. x_{ik}). And, by minimality, we have that $L_i = x_{ki}$ and $x_{ik} = L_k$. Moreover, if $x_{ji} = 0$ (respectively $x_{jk} = 0$) then, by similar arguments as in Part (a), this would imply that $x_{ki} = 0$ (respectively $x_{ik} = 0$), which is impossible. □

The above connection between the Frobenius number and Hilbert series has been observed earlier by Morales [299]; see also [300]. However, Morales' motivation was in the converse direction, that is, to use results related to the Frobenius number in order to calculate some special resolutions; see Section 8.4.

4.8 Ehrhart polynomial

A set $C \subset \mathbb{R}^n$ is called *convex* if, for all $x, y \in C$, $x \neq y$, the line segment $\{\lambda x + (1 - \lambda) y | 0 \leq \lambda \leq 1\}$ is contained in C. A *convex polytope* is the convex hull of finitely many points in $\mathbb{R}^n$. A hyperplane

H is called a *supporting hyperplane* of a convex polytope $P \subset \mathbb{R}^n$ if $H \cap P \neq \emptyset$ and $P \subset H^-$ or $P \subset H^+$. If H is a supporting hyperplane of P then we call $F = P \cap H$ a *face* of P. A 1-,2- and $(n-1)$-face of a polytope $\subset \mathbb{R}^n$ is called *vertex*, *edge* and *facet* of P. Let P be a convex polytope of dimension n. A polytope is called *integral* (respectively *rational*) if all its vertices have integer (respectively rational) coordinates. Let t be a positive integer and let $i(P,t)$ be the number of lattice points in P dilated by a factor of t, that is,

$$i(P,t) = \#(tP \cap \mathbb{Z}^n),$$

where $tP = \{(tx_1, \ldots, tx_n) | (x_1, \ldots, x_n) \in P\}$. In other words, $i(P,t)$ counts the number of lattice points that lie inside the dilated polytope tP.

Ehrhart [127] initiated the systematic study of the function $i(P,t)$ (see also [123, 124]).

Theorem 4.8.1 *[127] Let P be an integral convex polytope of dimension n. Then, $i(P,t)$ is always a polynomial in $t \in \mathbb{N}$ of degree n. That is,*

$$i(P,t) = e_n(P)t^n + e_{n-1}(P)t^{n-1} + \cdots + e_0(P). \tag{4.20}$$

Moreover, for positive integers n the value of $(-1)^{deg\ i(t,P)} i(P,-t)$ is equal to the number of integral points in the relative interior of the polytope tP (the 'reciprocity law').

The polynomial $i(P,t)$ is called the *Ehrhart polynomial.* We refer the reader to the monograph [126] that collects Ehrhart's work and where detailed references are given; see also [290, 291] for another proof of Theorem 4.8.1 and related results. It is known that $e_0 = 1$, $e_n = vol(P)$ ($vol(P)$ denotes the volume of P) and e_{n-1} is the sum of the volumes of the $(n-1)$-dimensional faces of P. The other coefficients of $i(P,t)$ remained a mystery. However, in the special case when P is a *unimodular zonotope* (*i.e.* a polytope that *tiles* the space) there is a nice interpretation of these coefficients in terms of the *Tutte polynomial* associated to P; see [479] for further details.

There exists a close relationship among denumerants and Ehrhart polynomials. Indeed, given a set of positive integers $a_1, \ldots, a_n$, we consider the following rational polytope

$$\mathcal{P} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_k \geq 0, \sum_{k=1}^{n} a_k x_k \leq 1\}. \tag{4.21}$$

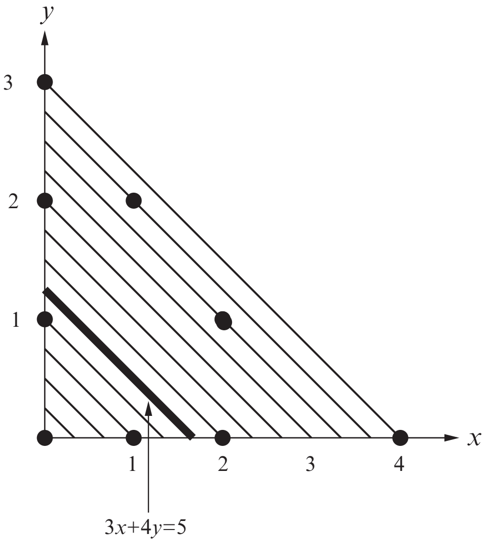

Figure 4.2: Dilates of $3x + 4y = t$ and some points of the integer lattice.

Note that $\mathcal{P}$ has vertices $(0, \ldots, 0)$, $(\frac{1}{a_1}, 0, \ldots, 0)$, $(0, \frac{1}{a_2}, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, \frac{1}{a_n})$. Thus, geometrically, $d(m; a_1, \ldots, a_n)$ enumerates the lattice points on the skewed facet of $\mathcal{P}$.

Remark 4.8.2 *$g(a_1, \ldots, a_n)$ is the largest integer t such that the facet $\{\sum_{k=1}^{n} x_k a_k = t\}$ of the dilated polytope $t\mathcal{P}$ contains no lattice point, that is, the largest t such that $d(t; a_1, \ldots, a_n) = 0$.*

Example 4.8.3 Let $a_1 = 3$ and $a_2 = 4$. Figure 4.2 shows that the hypotenuse of $\mathcal{P}$ is given by $3x + 4y = t$ (that is, the hypotenuse of the t-dilated triangle $3x + 4y \leq 1$). It is clear that this line has no integer points if $t = 5$ but it always does for any integer $t \geq 6$; see the third proof of Theorem 2.1.1.

In the case when P is a rational polytope it is known that $i(P, t)$ is not a polynomial but a *quasipolynomial* (a *quasipolynomial* of degree n is a function $f : \mathbb{N} \to \mathcal{C}$ of the form $f(t) = c_n(t)t^n + \cdots + c_1(t)t + c_0(t)$, where each $c_i(t)$ is a *periodic function* (with integer period), and where $c_n(t)$ is not the zero function.

Beck *et al.* [31] presented two different procedures for computing the terms appearing in the quasipolynomials

$$i(\mathcal{P},t) = \#(t\mathcal{P} \cap \mathbb{Z}^n) \text{ and } i(\mathcal{P}^0,t) = \#(t\mathcal{P}^0 \cap \mathbb{Z}^n),$$

where $\mathcal{P}^0$ denotes the interior of polytope $\mathcal{P}$ (defined in eqn (4.21)). Their proof is based on the *Fourier–Dedekind* sums and the *Fourier analytical* method [70, 338]. From these results, they showed that $d(m; a_1, \ldots, a_n)$ has an explicit representation as a quasipolynomial. In [35], Beck and Zacks used Remark 4.8.2 to obtain upper bounds for $g(a_1, a_2, a_3)$ that depends on upper bounds for the periodic part of $d(m; a_1, a_2, a_3)$.

For $n = 2$, eqn (4.20) correspond to Pick's theorem. Let $\mathcal{S}$ be a polygon, by Theorem 2.1.2, we have

$$A(\mathcal{S}) = I(\mathcal{S}) + \frac{B(\mathcal{S})}{2} - 1,$$

where $A(\mathcal{S})$ denotes the area of $\mathcal{S}$, $I(\mathcal{S})$ and $B(\mathcal{S})$ are the number of lattice points in the interior and in the boundary of $\mathcal{S}$ respectively. So,

$$I(\mathcal{S}) + B(\mathcal{S}) = A(\mathcal{S}) - \frac{B(\mathcal{S})}{2} + 1 + B(\mathcal{S}) = A(\mathcal{S}) + \frac{B(\mathcal{S})}{2} + 1.$$

This yields to

$$i(\mathcal{S},t) = vol(\mathcal{S})t^2 + \frac{1}{2}vol(\partial\mathcal{S})t + 1,$$

where $vol(\partial\mathcal{S})$ denotes the sum of the lattice lengths of the edges of $\mathcal{S}$.

For a three-dimensional integral convex polytope $\mathcal{T}$ we have

$$i(\mathcal{T},t) = vol(\mathcal{T})t^3 + \frac{1}{2}vol(\partial\mathcal{T})t^2 + e_1 t + 1,$$

where $vol(\partial\mathcal{T})$ denotes the sum of the lattice volumes of the two-dimensional faces of $\mathcal{T}$. An interesting problem is to determine the value of e_1. By analogy with Pick's theorem, one would hope to express e_1 in terms of the volumes of the one-dimensional faces of $\mathcal{T}$. In [348], it is shown that this is not possible in general. To see this, we consider the tetrahedron $\mathcal{T}_r \in \mathbb{Z}^3$ with vertices at $(0,0,0), (1,0,0), (0,1,0)$ and $(1,1,r)$ with $r \in \mathbb{Z}$. It can be proved that $e_1 = 1 - \frac{r}{6}$, but the lattice volumes of the one-dimensional and two-dimensional faces of $\mathcal{T}_r$ are independent of r. Thus, even in case of a tetrahedron, a formula for e_1 cannot just depend on the volumes of the faces of $\mathcal{T}$.

Pommersheim [334] used techniques from algebraic geometry related to the *Todd classes* of toric varieties to express e_1 in terms of *Dedekind sums*[2] in the case of a general lattice tetrahedron. Mordell [301] had already made the connection between lattices points in a tetrahedron and Dedekind sums by considering the tetrahedron $\mathcal{T}(a, b, c)$ with vertices $(0, 0, 0), (a, 0, 0), (0, b, 0)$ and $(0, 0, c)$. Mordell gave a formula for $i(\mathcal{T}(a, b, c), t)$ expressed in terms of three Dedekind sums when the integers a, b, c are pairwise relatively prime. Pommersheim [334] derived a formula for $i(\mathcal{T}(a, b, c), t)$ for arbitrary positive integers a, b, c by using the connection between convex polytopes and toric varieties.

Theorem 4.8.4 *[334] Let a, b, c integers with $(a, b, c) = 1$. Then,*

$$\begin{aligned} i(\mathcal{T}(a,b,c),t) = \frac{abc}{6}t^3 &+ \left(\frac{ab+ac+bc+d}{4}\right)t^2 \\ &+ \left[\frac{1}{12}\left(\frac{ac}{b}+\frac{bc}{a}+\frac{ab}{c}+\frac{d^2}{abc}\right)\right. \\ &+ \frac{a+b+c+d_1+d_2+d_3}{4} - d_1 s\left(\frac{bc}{d},\frac{ad_1}{d}\right) \\ &\left. - d_2 s\left(\frac{ac}{d},\frac{bd_2}{d}\right) - d_3 s\left(\frac{ab}{d},\frac{cd_3}{d}\right)\right]t + 1, \end{aligned}$$

where $d_1 = (b, c)$, $d_2 = (a, c)$, $d_3 = (a, b)$ and $d = d_1 d_2 d_3$.

In the next section, we shall see how the value of $i(\mathcal{T}(a, b, c), t)$ could be obtained as a particular case of a more general function (see Remark 4.9.1).

4.9 Variations of the denumerant

In this section we discuss some variations of the denumerant.

[2] The *Dedekind sum* $s(p, q)$ for relatively prime integers p and q is defined by

$$s(p,q) = \sum_{i=1}^{q} \left(\left(\frac{i}{q}\right)\right)\left(\left(\frac{pi}{q}\right)\right),$$

where

$$((x)) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2} & \text{if } x \notin \mathbb{Z} \\ 0 & \text{if } x \in \mathbb{Z}. \end{cases}$$

4.9.1 $d'(m; a_1, \dots, a_n)$

Let $m, a_1, \dots, a_n$ be integers such that $m \geq a_i > 0$ for $i = 1, \dots, n$. Let $d'(m; a_1, \dots, a_n)$ be defined as the number of solutions to

$$x_1 a_1 + \cdots + x_n a_n \leq m \text{ with integers } x_i \geq 0.$$

Remark 4.9.1 *Let t be a positive integer. Let S be the set of all non-negative integer points in $x = (x_1, x_2, x_3)$ such that $\frac{x_1}{a_1 t} + \frac{x_2}{a_2 t} + \frac{x_3}{a_3 t} \leq 1$. In other words, S is the set of all integer points in the positive orthant lying 'below' the hyperplane H passing through the points $(a_1 t, 0, 0), (0, a_2 t, 0)$ and $(0, 0, a_3 t)$. Since the equation of H is given by $\frac{x}{a_1 t} + \frac{y}{a_2 t} + \frac{z}{a_3 t} = 1$ then we have*

$$i(\mathcal{T}(a, b, c), t) = d'(t a_1 a_2 a_3; a_2 a_3, a_1 a_3, a_2 a_3).$$

The value $d'(m; a_1, \dots, a_n)$ has been extensively studied. Beged-Dov [36] has investigated the function $d'(m; a_1, \dots, a_n)$, in relation with a knapsack-type problem called the *cutting stock* problem[3] and found the following bounds.

Theorem 4.9.2 *Let $a_1, \dots, a_n$ positive integers with $(a_1, \dots, a_n) = 1$ and let $P_n = \prod_{j=1}^{n} a_j$. Then,*

$$\frac{m^n}{n! P_n} \leq d'(m; a_1, \dots, a_n) \leq \frac{\left(m + \sum\limits_{i=1}^{n} a_i\right)^n}{n! P_n}.$$

Proof. Let $B(b_1, \dots, b_n)$ denote the set of points $\mathbf{x} = (x_1, \dots, x_n)$ satisfying the following $2n$ inequalities

$$b_i a_i \leq x_i < (b_i + 1) a_i \tag{4.22}$$

for each $i = 1, \dots, n$. $B(b_1, \dots, b_n)$ is a n-dimensional rectangular box with volume P_n. Let $P(r)$ denote the set of points $\mathbf{x}$ satisfying $x_1, x_2, \dots, x_n \geq 0$ and

$$x_1 + \cdots + x_n \leq r. \tag{4.23}$$

$P(r)$ is a pyramid of volume $\frac{r^n}{n!}$. Now, each $\mathbf{x} \in \mathbb{R}^n$ belongs to the unique box $B(b_1, \dots, b_n)$, where $b_i = \lfloor \frac{x_i}{a_i} \rfloor$ for each $i = 1, \dots, n$. Thus, if $\mathbf{x}$ is in $P(m)$ then, by eqn (4.23) we have that

$$\sum_{i=1}^{n} \left\lfloor \frac{x_i}{a_i} \right\rfloor a_i \leq \sum_{i=1}^{n} \left(\frac{x_i}{a_i} \right) a_i = \sum_{i=1}^{n} x_i \leq m,$$

[3] The *cutting stock* problem is the problem of filling an order at minimum cost for specified numbers of lengths of material to be cut from given stock lengths of given cost; see [156].

and so,

$$b_i a_i + \cdots + b_n a_n \leq m. \tag{4.24}$$

Therefore, the union of the $d'(m; a_1, \ldots, a_n)$ boxes $B(b_1, \ldots, b_n)$ where the $(b_1, \ldots, b_n)$ satisfy inequality (4.24) contains $P(m)$. We obtain the lower bound by comparing the volume of this union with the volume of $P(m)$, that is

$$\frac{m^n}{n!} \leq d'(m; a_1, \ldots, a_n) P_n.$$

Conversely, consider any point $\mathbf{x}$ in any of the $d'(m; a_1, \ldots, a_n)$ boxes $B(b_1, \ldots, b_n)$ with $(b_1, \ldots, b_n)$ satisfying (4.24). From eqn (4.22) we have

$$x_i \leq \sum_{i=1}^{n} (b_i + 1) a_i \leq m + \sum_{i=1}^{n} a_i,$$

which shows that $\mathbf{x}$ is in $P(m + \sum_{i=1}^{n} a_i)$. We now obtain the upper bound by comparing the volume of the union of the $d'(m; a_1, \ldots, a_n)$ boxes with the (larger) volume of $P(m + \sum_{i=1}^{n} a_i)$, that is

$$P_n d'(m; a_1, \ldots, a_n) \leq \frac{\left(m + \sum_{i=1}^{n} a_i\right)^n}{n!}.$$

□

Padberg [321] showed that the lower bound can be sharpened, obtaining

$$\frac{(m+1)^n}{n! P_n} \leq d'(m; a_1, \ldots, a_n). \tag{4.25}$$

In [321], Padberg also derived alternative upper and lower bounds for $d'(m; a_1, \ldots, a_n)$.

It is clear that

$$d'(m; a_1, \ldots, a_n) = \sum_{i=0}^{m} d(i; a_1, \ldots, a_n),$$

thus the $d(m; a_1, \ldots, a_n)$ is the coefficient of z^m in the development of

$$f'(z) = \frac{1}{1-z} f(z),$$

where $f(z)$ is the generating function of $d(m; a_1, \ldots, a_n)$. Achou [4] studied the generating function $f'(z)$ and derived an expression to compute $d'(m; a_1, \ldots, a_n)$ when the integers $a_1, \ldots, a_n$ are pairwise relatively prime. However, because of the presence of complex roots of unity, is awkward to calculate $d'(m; a_1, \ldots, a_n)$ numerically. In [329], Piehler transformed Achou's formula so that the calculation can be done by using only rational numbers.

Hujter [212] improved the above upper and lower bounds of $d'(m; a_1, \ldots, a_n)$ by using geometrical methods.

Theorem 4.9.3 *[212] Let $d = (a_1, \ldots, a_n)$ and $V = d\lfloor \frac{m}{d} \rfloor$ (i.e. V is the largest integer that is not larger than m and a multiple of d). Then,*

$$\frac{(V+d)^n}{n! \prod\limits_{j=1}^{n} a_j} \leq d'(m; a_1, \ldots, a_n) \leq \frac{2\left(V + \frac{1}{2}\sum\limits_{j=1}^{n} a_j\right)^2 - V^n}{n! \prod\limits_{j=1}^{n} a_j}.$$

The proof of the above upper bound is based on the so-called *Brunn–Minkowski* inequality (see [177] for details of this inequality).

4.9.2 $d''(m; a_1, \ldots, a_n)$

In [343], we have investigated the boundary between easy and hard variations of the denumerant. Let $m, a_1, \ldots, a_n, r_1, \ldots, r_n$ be integers such that $0 \leq a_i \leq r_i$ for $i = 1, \ldots, n$ and let $d''(m; a_1, \ldots, a_n)$ be the number of solutions to

$$x_1 a_1 + \cdots + x_n a_n = m \qquad \text{with integers } 0 \leq x_i \leq r_i.$$

A sequence $a_1, \ldots, a_n$ is called a *chain-divisible* if $a_j | a_{j+1}$ for $j = 1, \ldots, n-1$ and *superincreasing* if $\sum_{i=1}^{j} a_i \leq a_{j+1}$ for $j = 1, \ldots, n-1$.

Theorem 4.9.4 *[343] There exists a polynomial time algorithm that decides whether $d''(m; a_1, \ldots, a_n) \geq 1$ if either*

(a) *$a_1, \ldots, a_n$ is superincreasing and $r_i = 1$ for all i or*
(b) *$a_1, \ldots, a_n$ is an arithmetic progression and $r_i = 1$ for all i or*
(c) *$a_1, \ldots, a_n$ is a chain.*

Proof. (a) $d''(m; a_1, \ldots, a_n) \geq 1$ if and only if there exists $s \subseteq \{1, \ldots, n\}$ such that $m = \sum_{i \in s} a_i$. Let r be the greatest integer such that $m \geq a_r$. Since the sequence is superincreasing then $m = a_r + t$ where we now need to find a representation of t as the sum of the superincreasing sequence $a_1, \ldots, a_{r-1}$. repeating this procedure gives a representation of m (if there exists one). (b) We shall use the following observation.

Observation: *Let a, n, k be integers with $1 \leq k \leq n$. Then, if there exists $s \subseteq T = \{a, a+j, \ldots, a+(n-1)j\}$ with $|s| = k$, $s \neq \{a+(n-k)j, \ldots, a+(n-1)j\}$ such that $\sum_{i \in s} i = t$ then there exists $s' \subseteq T$ with $|s'| = k$, such that $\sum_{i \in s'} i = t + j$.*

Let a, n, k be integers with $1 \leq k \leq n$. Let $S_k = \{s \mid s \subseteq \{a, a+j, \ldots, a+(n-1)j\} \textit{ and } |s| = k\}$, and let

$$c_k = c_k(a,n,j) = \min_{s \in S_k} \sum_{i \in s} i = \left(\frac{k(k-1)}{2}\right) j + ka,$$

and

$$d_k = d_k(a,n,j) = \max_{s \in S_k} \sum_{i \in s} i = \left(\frac{n(n-1) - (n-1-k)(n-k)}{2}\right) j + ka$$
$$= \left(\frac{k(2n-k-1)}{2}\right) j + ka.$$

Observe that c_k and d_k are increasing functions of k. First note that for all s in S_k we have $\sum_{i \in s} i \equiv c_k \equiv ka \bmod j$. Let $g = (a, j)$. Suppose that $g|t$ (otherwise there can be no solution, since we would have $t = pa + qj$ for some $p, q \in \mathbb{N}$). There is a solution in SSP with triple (a_1, n, j) and integer t if and only if the there is a solution in SSP with triple $(\hat{a}_1 = \frac{a_1}{g}, n, \hat{j} = \frac{j}{g})$ and integer $\hat{t} = \frac{t}{g}$. Thus we may assume that a and j are coprime, and so a has an inverse $a^{-1} \bmod j$, (easily computed by Euclidean algorithm).

We are interested only in the sizes k such that $ka \equiv t \bmod j$, *i.e.*, such that $k \equiv a^{-1}t \bmod j$. Let k_1 be the least $k \equiv a^{-1}t \bmod j$ such that $d_k \geq t$. We may find k_1 in polynomial time by binary search (or find if there is no such k). Hence, by the above observation $d''(m; a_1, \ldots, a_n) \geq 1$ if and only if $c_{k_1} \leq t$.

(c) Let e and f be non-negative integers with $e \leq f$. Let $S(P) = S(a_1, r_1, \ldots, a_n, r_n; e, f)$ be the set of vectors $\mathbf{x} = (x_1, \ldots, x_n)$ of non-negative integers such that $0 \leq x_i \leq r_i$ for $i = 1, \ldots, n$ and $\sum_{i=1}^n a_i x_i \in [e, f]$. We may find (if there exist) vectors $\mathbf{x} = (x_1, \ldots, x_n)$ such that $S(P) \neq \emptyset$ (*i.e.,* such that $d''(m; a_1, \ldots, a_n) \geq 1$) by repeating the following subroutine. Let $S(P_1) = S(a_1, r_1, \ldots, a_n, r_n; t_1, t_2)$, and let $S(P_2) = S(\bar{a}_1, r_1, \ldots, \bar{a}_n, r_n; \bar{t}_1, \bar{t}_2)$ with $\bar{a}_i = \frac{a_i}{a_1}$ for $i = 1, \ldots, n$, $\bar{t}_1 = \lceil \frac{t_1}{a_1} \rceil$ and $\bar{t}_2 = \lfloor \frac{t_2}{a_1} \rfloor$. Then, $S(P_1) = S(P_2)$ since $\sum_{i=1}^n a_i x_i = a_1 \sum_{i=1}^n \bar{a}_i x_i$. Further, $S(P_2) \neq \emptyset$ if and only if $S(P_3) = S(\bar{a}_2, r_2, \ldots, \bar{a}_n, r_n; \bar{t}_1 - r_1, \bar{t}_2) \neq \emptyset$. □

However, in general, to decide whether $d''(m; a_1, \ldots, a_n) \geq 1$ is a difficult probem.

Theorem 4.9.5 *[343] Decide whether $d''(m; a_1, \ldots, a_n) \geq 1$ is a $\mathcal{NP}$-complete problem even if the sequence $a_1, \ldots, a_n$ is superincreasing and $r_i \leq 2$ for all i.*

In [343], we also proved that some more general problems can be solved in polynomial time for particular sequences; see also [341] for further related results.

4.10 Supplemetary notes

Hofmeister [203] studied **FP** via the *partition* theory; see also the paper [491] by Zöllner for further results on this direction. Another proof of Theorem 4.2.1 was also given by Wright [482]. Fergola[4] and Sardi[5] gave a more complicated determinant expression of $d(m; a_1, \ldots, a_n)$ than Theorem 4.3.5. Kuriki [259, 260] found a recursive formula for $d(m; a_1, \ldots, a_n)$ based on Theorem 4.3.5 and Del Vigna [110] gave a combinatorial proof of Theorem 4.3.3. By investigating $d(m; a_1, \ldots, a_n)$ and variants of it, Badra [22] obtained formulas for the Frobenius number, improving Chrząstowski-Wachtel's result (Theorem 3.2.1) and generalizing Rødseth's formula (Theorem 5.3.9).

The form that the function $d(m; p, q)$ takes is well known; see [481, page 90] and [96, pages 113–114]. In [23], Barbosa obtained the following explicit formulas: $d(m; 1, 3, 4) = m(m + 8)/24 + 1$, $d(m; 1, 3, 5) = m(m + 9)/30 + 1$ and $d(m; 1, 4, 5) = m(m + 10)/40 + a$ where $a = 2$ if $m \equiv 5 \bmod 20$ and $a = 1$ otherwise. Israilov [216] found a 'long' but general formula for $d(m; a_1, \ldots, a_n)$ in the case when $a_1, \ldots, a_n$ are pairwise relatively primes. Israilov also discussed a method to calculate denumerants. Ehrhart [125, 126] has also developed an algorithm for the computation of $d(m; a_1, \ldots, a_n)$ in the general case and Komatsu [249] gave a general form that is well computable practically to find $d(m; a_1, \ldots, a_n)$ when $(a_i, a_j) = 1$ for all $i \neq j$ and $m \geq 2$.

In [330], Piehler investigated $d(m; a_1, \ldots, a_n)$ through examples by using results due to Csorba [101]. Investigations on $d(m; p, q)$ have also been done by Catalan and de Polignac among others (see [114, pages 64–71] for an historical review of $d(m; p, q)$ and related problems).

Blakley [45, 46, 47] has developed the denumerant partition theory to *multi-indexes* as follows. For vectors $\mathbf{m} = (m_1, \ldots, m_k)$, let $\mathcal{L}$ be the

[4] *Giornali di Matematiche* **1** (1863), 63–64.

[5] *ibid.* **3** (1865), 94–99.

system of k equations,

$$a_{i,1}x_1 + a_{i,2}x_2 + a_{i,3}x_3 + \cdots = m_i,$$

where $a_{i,j}$ are integers. Blakley showed that the generating function of number $d_{(a_{i,j})}(\mathbf{m})$ of solutions of system $\mathcal{L}$ in integers $x_i \geq 0$ is given by

$$\sum_{m_1,m_2,\ldots,m_k \geq 0} d_{(a_{i,j})}(\mathbf{m}) t_1^{m_1} \cdots t_k^{m_k} = \prod_{j \geq 1} \left(1 - \prod_{i=1}^{k} t_i^{a_{i,j}} \right)^{-1}.$$

Sertöz and Özlük applied their results in [408] to the theory of *Hilbert–Samuel* polynomials (a basic reference for definitions on the Hilbert–Samuel polynomials is [20]).

Lisoněk [277] presented an arithmetic procedure to compute $d(m; a, b, c)$ in time $O(ab)$ for any m when a, b, c are pairwise relatively prime positive integers. A nice MAPLE package for computing denumerants has been implemented by Lisoněk [278].

A closed formula for the Ehrhart polynomial of a lattice of a 4-simplex was announced by Kantor and Khovanskii [230] and more recently by Cappell and Shaneson [84] for n-simpleces. Diaz and Robins [111, 112] computed the Ehrhart polynomial using Fourier integrals; see also the work by Brion and Vergne [71, 72]. A fuller review of problems concerning lattice points can be found in [133] and [181]. In [385], Sardo Infirri studied the problem of lattice point enumeration using ideas in relation with *toric varieties*. We refer the reader to [26] and [27] for a detailed discussion of this and related topics and in which a vast literature can be found.

An optimization version of the value $d''_m(n)$ is considered by Campillo and Revilla [83]. They showed how the availability of the *greedy* algorithm for finding the minimum number of coins $l(b)$ in a coin system, $1 = a_1 < \cdots < a_n$ needed to achieve the value $b > 0$ is related to the *Cohen–Macaulay* property of the toric projective curves given by the integers $a_1, \ldots, a_n$.

This page intentionally left blank

5

Integers without representation

5.1 Sylvester's classical result

Let $N(a_1, \ldots, a_n)$ be the number of positive integers with no non-negative integer representation by $a_1, \ldots, a_n$ (we still assume that $(a_1, \ldots, a_n) = 1$ unless stated otherwise). The study of $N(a_1, \ldots, a_n)$ dates back at least to 1882 in a paper by Sylvester [439] in which the partition function and the denumerant are studied; see Chapter 4. In [439] an explicit formula for $N(a_1, a_2)$ is given.

Theorem 5.1.1 *[439, page 134] Let p, q be positive integers such that $(p, q) = 1$. Then,*

$$N(p, q) = \frac{1}{2}(p-1)(q-1).$$

In 1909, Glaisher [157] simplified Sylvester's proof to obtain the same formula; see also [158]. In [437, Problem 7382], Sylvester posed, (as a recreational problem) the question of finding such a formula. We reproduce below the page of this so many referenced manuscript[1] where Curran Sharp [413] answered Sylvester's question.

We may give two other proofs of Theorem 5.1.1. Let $N^*(p, q)$ be the set of positive integers without non-negative integer representation by p and q and let $\bar{N}^*(p, q) = \mathbb{N} \setminus N^*(p, q)$.

Second proof of Theorem 5.1.1. Suppose that $c \notin N^*(p, q)$, *i.e.*, $c = px+qy$ with $x, y \geq 0$. We claim that $(p-1)(q-1)-c-1 \in N^*(p, q)$. Assume the contrary, that is, there exist integers $z, t \geq 0$ such that $pz + qt = (p-1)(q-1) - c - 1$. Then,

$$\begin{aligned} pz + qt = (p-1)(q-1) - c - 1 &= p(q-1-x) + q(-1-y) \\ &= p(-1-x) + q(p-1-y). \end{aligned}$$

[1] With the kind permission of *The Educational Times*. We keep the same style and format as the original manuscript.

MATHEMATICS

FROM

THE EDUCATIONAL TIMES,

WITH ADDITIONAL PAPERS AND SOLUTIONS.

7382. (By Professor Sylvester, F.R.S.)-If p and q are relative primes, prove that the number of integers inferior to pq which cannot be resolved into parts (zeros admissible), multiples respectively of p and q, is

$$\tfrac{1}{2}(p-1)(q-1).$$

[If $p=4$, $q=7$, we have $\frac{1}{2}(p-1)(q-1)=9$; and $1,2,3,5,6,9,10,13,17$ are the only integers inferior to 28, which are neither multiples of 4 or 7, nor can be made up by adding together multiples of 4 and 7.]

Solution by W.J. Curran Sharp, M.A.

If the product $(1+x^p+x^{2p}+\cdots+x^{pq})(1+x^q+x^{2q}+\cdots+x^{pq})$ be considered, each term between 1 and x^{pq} corresponds to a number less than pq, and of the form $mp+nq$; also $2x^{pq}$ is the middle term, and the coefficients from each end are the same. Hence twice the number of integers of the form $mp+nq$, and less then pq, is the value of the above product when $x=1$ with four deducted, since the terms involving x^1, x^{pq}, x^{2pq} are not included; and therefore the number of these integers is

$$\tfrac{1}{2}(p+1)(q+1)-2$$

and the number of those which cannot be put into this form $=pq-1-\left[\frac{1}{2}(p+1)(q+1)-2\right]=\frac{1}{2}\left[pq-p-q+1\right]=\frac{1}{2}(p-1)(q-1)$.

Since $(p,q)=1$ then it is impossible to have $(p-1)(q-1)-c-1 = pz+qt$ with $-1-x<z<q-1-x$. Hence, we have either $z \leq -1-x < 0$ (which is a contradiction since $z \geq 0$) or $z \geq q-1-y$ but then $t \leq -1-y < 0$ (which is also a contradiction since $y \geq 0$).

Now suppose that $c \in N^*(p,q)$. We can write $c = xp+yq$ with $0 \leq x < q$ and $y < 0$. We also have that $(p-1)(q-1)-c-1 = p(q-1-x)+q(-1-y)$, where $(-1-y) \geq 0$ and $q-1-x \geq 0$.

Thus, we have that the symmetry, regarding the middle of the interval $[0,\ldots,pq-p-q]$, interchanges the elements of $N(p,q)^*$ and its complement. Therefore, each class, in this interval, has $\frac{1}{2}(p-1)(q-1)$ elements. □

Third proof of Theorem 5.1.1. Consider the map $\phi : [1,\ldots,q-1]\times[1,\ldots,p-1] \longrightarrow \bar{N}^*(p,q)$ defined by $\phi(x,y)=px+qy$.

Remark 5.1.2 *There is a central symmetry with center* $(\frac{q}{2},\frac{p}{2})$ *(which is a point on the line with at least one non-integer co-ordinate) between the points in* $(z_1,z_2)\in[1,\ldots,q-1]\times[1,\ldots,p-1]$ *lying below the line* $px+qy=pq$ *that is, points such that* $pz_1+qz_2<pq$ *and the points in* $(z_1,z_2)\in[1,\ldots,q-1]\times[1,\ldots,p-1]$ *lying above this line that is, points such that* $pz_1+qz_2>pq$.

Since there are no points $\phi(x,y)$ lying on $px+qy=pq$ in $[1,\ldots,q-1]\times[1,\ldots,p-1]$ then, by the above remark, there are $(p-1)(q-1)/2$ points lying in the region $[1,\ldots,q-1]\times[1,\ldots,p-1]$. By adding points ip, $1\leq i\leq q-1$ and jq, $1\leq j\leq p-1$ and 0, we find that there are $(p-1)(q-1)/2+(p-1)+(q-1)+1$ elements in $[0,\ldots,pq-1]$ of the form $p\mathbb{N}+q\mathbb{N}$. Therefore, there are $pq-((p-1)(q-1)/2+(p-1)+(q-1)+1) = (p-1)(q-1)/2$ elements not of the form $p\mathbb{N}+q\mathbb{N}$. in $[0,\ldots,pq-1]$.

It is easy to verify that if $c\geq pq$ then we can write $c=px+qy$ with $0\leq x<q$; and thus $y>0$ (see proof of Theorem 2.1.1). Therefore, $|N^*(p,q)|=(p-1)(q-1)/2$. □

We invite the reader to see Chapter 7 (*cf.* Proposition 3.2.3) for a generalization of Theorem 5.1.1 in terms of symmetric semigroups.

5.2 Nijenhuis' and Wilf's results

Nijenhuis and Wilf [310] studied $N(a_1,\ldots,a_n)$. Let $d_1=a_1$ and $d_i=(a_1,\ldots,a_i)$, $1<i\leq n$. We say that the sequence $a_1,\ldots,a_n$ satisfy condition

[**I**] if $\frac{a_j}{d_j}=\frac{1}{\mathrm{d}_{j-1}}\sum_{i=1}^{j-1} y_{ji}a_i$ with integer $y_{ji}\geq 0$ for each $j=2,\ldots,n$, and condition

$$\textbf{[II]} \qquad \text{if } g(a_1, \dots, a_n) = \sum_{i=1}^{n-1} a_{i+1}d_i/d_{i+1} - \sum_{i=1}^{n} a_i.$$

Theorem 5.2.1 *[310] Suppose that $a_1, \dots, a_n$ satisfy condition* [**I**] *then*

$$\textbf{[III]} \qquad N(a_1, \dots, a_n) = \tfrac{1}{2}\left\{\sum_{i=1}^{n-1} a_{i+1}d_i/d_{i+1} - \sum_{i=1}^{n} a_i\right\}.$$

Moreover, the right side of [**III**] *is always an upper bound for $N(a_1, \dots, a_n)$.*

Rødseth [373] found the following easy proof of Theorem 5.2.1.

Proof of Theorem 5.2.1. Let $\gamma = \frac{1}{2}\left\{\sum_{i=1}^{n-1} a_{i+1}d_i/d_{i+1} - \sum_{i=1}^{n} a_i\right\}$. It is clear that

$$N\left(\frac{a_1}{d_i}, \dots, \frac{a_i}{d_i}, \frac{a_{i+1}}{d_{i+1}}\right) \geq N\left(\frac{a_1}{d_i}, \dots, \frac{a_i}{d_i}\right),$$

where equality holds if and only if $\frac{a_{i+1}}{d_{i+1}}$ is dependent on $\frac{a_1}{d_i}, \dots, \frac{a_i}{d_i}$. By Lemma 5.3.2 we have that $N(a_1, \dots, a_n) \leq \gamma$, and also that $N(a_1, \dots, a_n) = \gamma$ if and only if $a_1, \dots, a_n$ satisfy condition [**I**]. □

The proof of Theorem 5.2.1 given in [310] yields that the conditions [**I**], [**II**] and [**III**] are actually equivalent[2].

Theorem 5.2.2 *[310] Under condition* [**I**] *(or equivalently* [**II**] *or* [**III**]*) we have*

$$\textbf{[IV]} \qquad N(a_1, \dots, a_n) = \tfrac{g(a_1, \dots, a_n)+1}{2}.$$

In [310], Nijenhuis and Wilf compared the values $N(a_1, \dots, a_n)$ and $g(a_1, \dots, a_n)$.

Theorem 5.2.3 *[310]*

$$\frac{g(a_1, \dots, a_n)+1}{2} \leq N(a_1, \dots, a_n).$$

Proof. Let $\rho(x) = g(a_1, \dots, a_n) - x$; so $\rho(x) + x = g(a_1, \dots, a_n)$. The right side is not representable as a non-negative linear combination of $a_1, \dots, a_n$. Hence, both terms on the left side cannot be representable as a non-negative linear combination of $a_1, \dots, a_n$ (semigroup property, see Chapter 7). So, if x is representable then $\rho(x)$ is not. The set of the non-representable values among $0, \dots, g(a_1, \dots, a_n)$ contains therefore

[2] The equivalence of conditions [**I**] and [**II**] was shown by Brauer and Seelbinder [58] (*cf.* Theorem 3.1.4).

a subset of the cardinality of that of representable values, so at least half of the numbers $0, \ldots, g(a_1, \ldots, a_n)$ are non-representable. □

Notice that the same argument as that used in the above proof shows that if m is a non-representable value then at least half of the numbers $0, \ldots, m$ are non-representable. Nijenhuis and Wilf [310] investigated the relationship between the above conditions and the following property arising from the theory of *Gorenstein rings*. Suppose S is a set of integers m that are expressible by $\sum_{i=1}^{n} x_i a_i$ and in which $x_n = 0$ for every representation. Let $T = \{m \in S | m + a_i \notin S \text{ for all } i\}$. The *Gorenstein condition* [167] is the property

$$\textbf{[V]} \qquad\qquad |T| = 1.$$

Nijenhuis and Wilf [310] showed[3] that

Theorem 5.2.4 *Let $T = \{m \in S | m + a_i \notin S$ for all $i\}$.*

$$|T| = 1 \textit{ if and only if } N(a_1, \ldots, a_n) = \frac{1}{2}\left(g(a_1, \ldots, a_n) + 1\right).$$

Nijenhuis and Wilf used the following Lemma (see Theorem 7.2.11) to prove Theorem 5.2.4.

Lemma 5.2.5 *Let $T = \{m \in S | m + a_i \notin S$ for all $i\}$ and let $W = \{x | x - a_n \in T\}$. Then*

$$W = \{x | x \textit{ is not representable and } x + a_i \textit{ is representable for all } i\}.$$

Moreover, $g(a_1, \ldots, a_n)$ belongs to W.

Proof of Theorem 5.2.4. Suppose that $|T| = 1$, we shall show that $\rho(x) = g(a_1, \ldots, a_n) - x$ is representable if x is not (and so, exactly half of the numbers $0, \ldots, g(a_1, \ldots, a_n)$ are not representable). Suppose that x is not representable and let y be the largest representable value for which $x + y$ is not representable. As $y + a_i$ is representable, which exceeds y, it follows that $x + y + a_i$ is representable; so, $x + y$ is in W and thus $x + y = g(a_1, \ldots, a_n)$, that is, $y = \rho(x)$ is representable.

Conversely, suppose that (**IV**) holds, then $\rho(x)$ is representable if and only if x is not. Let w be such that $w \in W$, then w is not representable and hence $g(a_1, \ldots, a_n) - w$ is representable. Suppose that $g(a_1, \ldots, a_n) - w > 0$, so it is of the form $\sum_{i=1}^{n} \psi_i a_i$ with $\psi_i > 0$ for at least one i. Then, there exists i such that $w' = g(a_1, \ldots, a_n) - w - a_i$ is

[3] In [310], it is remarked that Kunz [256] has also proved independently such a characterization; see Chapter 7.

representable implying that $\rho(w') = w - a_i$ is not representable, contrary to one of the properties of the elements in $w \in W$ (Lemma 5.2.5). Hence, $w = g(a_1, \ldots, a_n)$, and that is the only element of W. □

In fact, the proof of Theorem 5.2.4 implies that if $w \in W$, $w < g(a_1, \ldots, a_n)$ then $\rho(w)$ is not representable, obtaining the following inequality

$$2N(a_1, \ldots, a_n) - g(a_1, \ldots, a_n) \geq |W|.$$

In [310] were noted the following interrelationships among the above conditions

$$[\mathbf{I}] \Leftrightarrow [\mathbf{II}] \Leftrightarrow [\mathbf{III}] \Rightarrow [\mathbf{IV}] \Leftrightarrow [\mathbf{V}],$$

and it was also observed that the example $(a_1, a_2, a_3) = (6, 7, 8)$ shows that the missing implication cannot be included in general.

5.3 Formulas for $N(a_1, \ldots, a_n)$

In this section, we state some formulas for $N(a_1, \ldots, a_n)$. We start with a result due to Selmer [392].

Theorem 5.3.1 *[392] Let* $L = \{1, \ldots, a_1 - 1\}$. *Then,*

$$N(a_1, \ldots, a_n) = \frac{1}{a_1} \sum_{l \in L} t_l - \frac{a_1 - 1}{2},$$

with t_l *is the smallest positive integer congruent to* l *modulo* a_1, *that is expressible as a non-negative integer combination of* $a_2, \ldots, a_n$.

Proof. The number of $M \equiv l \not\equiv 0 \bmod a_1$ with $0 < M < t_l$ is given by $\lfloor \frac{t_l}{a_1} \rfloor$. By assuming that $0 < l < a_1$, we have $\lfloor \frac{t_l}{a_1} \rfloor = \frac{t_l - l}{a_1}$. The result follows by summing over $l \in L$. □

The following analogue formula to that given in Theorem 3.1.7 was proved by Rødseth [373]; see also [198, 374].

Theorem 5.3.2 *[373] Let* $d = (a_1, \ldots, a_{n-1})$. *Then,*

$$N(a_1, \ldots, a_n) = dN\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n\right) + \frac{1}{2}(a_n - 1)(d - 1).$$

Proof. Let $t_l = t_l(a_1, \ldots, a_n)$ be the smallest integer that is dependent on $a_1, \ldots, a_n$ and $t_l \equiv l \bmod a_n$. Then there are no non-negative integers x_i such that $t_l = a_1x_1 + \cdots + a_nx_n$ where, by definition of t_l, $x_n = 0$. Let $a_i = da'_i$ for each $i = 1, \ldots, n-1$. Since $(a_1, \ldots, a_n) = 1$ then $(a_n, d) = 1$. We put $t'_l = t_l(a'_1, \ldots, a'_{n-1}, a_n)$. There are non-negative integers y_i such that

$$dt'_l = d \sum_{i=1}^{n-1} a'_i y_i = \sum_{i=1}^{n-1} a_i y_i. \tag{5.1}$$

By definition of t'_l, the sum on the right-hand-side of eqn (5.1) is the smallest integer dependent on $a_1, \ldots, a_n$ and $t'_l \equiv dl \bmod a_n$. Hence,

$$t_{dl} = dt'_l. \tag{5.2}$$

By Theorem 5.3.1 we have

$$N(a'_1, \ldots, a'_{n-1}, a_n) = \frac{1}{a_n} \sum_{l \in L} t'_l - \left(\frac{a_n - 1}{2} \right). \tag{5.3}$$

As l runs through a complete residue system modulo a_n, so does dl. Hence,

$$N(a_1, \ldots, a_n) = \frac{1}{a_n} \sum_{l \in L} t_{dl} - \left(\frac{a_n - 1}{2} \right). \tag{5.4}$$

By eqns (5.2)–(5.4) we have

$$\begin{aligned} N(a_1, \ldots, a_n) &= \frac{1}{a_n} \sum_{l \in L} t'_{dl} - \left(\frac{a_n - 1}{2} \right) \\ &= dN(a'_1, \ldots, a'_{n-1}, a_n) + \left(\frac{a_n - 1}{2} \right) (d-1). \end{aligned}$$

□

Mastrander [287] used Theorem 3.4.1 to show that

Theorem 5.3.3 *[287] Following the notation of Section 3.4 we have*

$$N(a_0, \ldots, a_n) = N(a_1, a_2) - \sum_{l=1}^{a_1 - 1} R(l) \text{ if and only if the sequence } a_0, \ldots, a_n \text{ is regular.}$$

The results of Krawczyk and Paz [255] (*cf.* Theorem 3.1.22) provide the following bound (computable in polynomial time). Recall that α_i, $1 \le i \le n$ is defined as the minimal integer α such that there exists a solution over the non-negative integers to the equation $\sum_{\substack{j=1 \\ j \ne i}}^{n} x_j a_j = \alpha a_i$ and let $B = \sum_{i=1}^{n} \alpha_i a_i$. Then,

$$\frac{B}{2n} \le N(a_1, \ldots, a_n) \le B.$$

Killingbergtrø [236] have used the cube-figure method (see Section 1.1.3) to obtain the following lower bound

$$\left\lfloor \left(\frac{n-1}{n}\right)((n-1)!a_1a_2\cdots a_n)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i - 1 \right\rfloor \leq N(a_1,\ldots,a_n).$$

We finally mention two formulas for the case $n = 3$. The first one is given by Tinaglia [446] and the other one is due to Rødseth [373] obtained via the negative division remainder approach (see Section 1.1.1).

Theorem 5.3.4 *[446] Let p, q, r be the minimum positive integers satisfying $a_1x_p + a_2y_p = qa_3$, $a_1x_q + a_3y_q = qa_2$ and $a_2x_r + a_3y_r = ra_1$ with integers $x_p, x_q, x_r, y_p, y_q, y_r \geq 0$. Then,*

$$N(a_1,a_2,a_3) = \frac{1}{2}(a_1r + a_2q + a_3p - pqr - a_1 - a_2 - a_3 + 1).$$

Theorem 5.3.5 *[373] Let $p_0 = 1$, $p_1 = q_1$, $p_2 = q_1q_2 - 1$ and $p_{i+1} = q_{i+1}p_i - p_{i-1}$. If $\frac{s_{v+1}}{p_{v+1}} \leq \frac{a_3}{a_2} < \frac{s_v}{p_v}$ where q_i and s_i are defined in Rødseth's Algorithm (see Section 1.1.1). Then,*

$$N(a_1,a_2,a_3) = \frac{1}{2}\Bigg(1 - a_1 + a_2(s_v - s_{v+1} - 1) + a_3(p_{v+1} - 1) + s_{v+1}(p_{v+1} - p_v)\frac{a_2s - v - a_3p_v}{a_1}\Bigg).$$

5.4 Arithmetic sequences

The results of Nijenhuis and Wilf in [310] lead to

$$N(m, m+1, \ldots, m+k-1) = \frac{mJ}{2}\left(\frac{(m-1)+\theta(k-1)}{m}\right),$$

where J is the least integer greater or equal to $\frac{m-1}{k-1}$, and $\theta = \frac{m-1}{k-1} - J + 1$ $(0 < \theta \leq 1)$.

By using Theorem 3.3.1, it can be checked that Theorem 5.2.3 is always verified in this case. Moreover, Theorem 5.2.2 is satisfied in this case if and only if $k-1$ divides $m-2$. Lewin [271] investigated some particular arithmetic sequences.

Theorem 5.4.1 *[271] Let a, d, k be positive integers with $(a, d) = 1$ and $1 \leq k \leq 7$. Then,*

$$N(a, a+d, \ldots, a+kd) = \left\lfloor \frac{(a-1)(a-1+kd)}{2k} \right\rfloor.$$

Grant [170] has found the exact number of $N(a, a+d, \ldots, a+kd)$ for any k.

Theorem 5.4.2 *[170] Let* a, d, k *be positive integers with* $(a,d) = 1$ *and let* $a-1 = r(k-1)+q$ *with* $0 \le q < k-1$*. Then,*

$$N(a, a+d, \ldots, a+(k-1)d) = \frac{1}{2}\left((a-1)(r+d)+q(r+1)\right).$$

Selmer [392] generalized Grant's result by giving a formula for almost arithmetic sequences.

Theorem 5.4.3 *[392] Let* a, h, d, k *be positive integers with* $(a,d) = 1$ *and let* $a-1 = r(k-1)+q$ *with* $0 \le q < k-1$*. Then,*

$$\begin{aligned}N(a, ha+d, ha+2d, \ldots, ha+(k-1)d) = \frac{1}{2}&((a-1)(hr+d+h-1)\\ &+hq(r+1)).\end{aligned}$$

5.5 The sum of integers in $N(p,q)$

Although we know that $N(p,q) = \frac{1}{2}(p-1)(q-1)$ (*cf.* Theorem 5.1.1), additional information about the non-representable numbers would be provided by estimating their sum

$$S(p,q) = \sum\{m | m \in N(p,q)\}.$$

An easy upper (respectively lower) bound is obtained by taking the sum of the $\frac{1}{2}(p-1)(q-1)$ largest (respectively smallest) integers in the interval $[0, \ldots, pq-p-q]$, giving

$$\frac{1}{8}(p-1)^2(q-1)^2 - \frac{1}{4}(p-1)(q-1) \le S(p,q) \le \frac{3}{8}(p-1)^2(q-1)^2 - \frac{1}{4}(p-1)(q-1).$$

Ho *et al.* [197] improved the latter upper bound. They found that if A is any finite set of non-negative integers such that the complement of A (in the set of non-negative integers) is closed under addition, then $\sum\{n | n \in A\} \le A^2$. Since the sum of two representable numbers is certainly a representable number, then by setting $A = N(p,q)$ we have

$$S(p,q) = \sum\{n | n \in N(p,q)\} \le |N(p,q)|^2 = \frac{1}{4}(p-1)^2(q-1)^2,$$

obtaining an upper bound for $S(p,q)$ of order $\frac{1}{4}(pq)^2$. Brown and Shiue [75] found the exact value of $S(p,q)$.

Theorem 5.5.1 *[75] Let* p, q *be positive integers with* $(p,q) = 1$*. Then,*

$$S(p,q) = \frac{1}{12}(p-1)(q-1)(2pq-pq-1).$$

Therefore the exact order of $S(p,q)$ is $\frac{1}{6}(pq)^2$. Brown and Shiue proof uses the following nice idea (see the fourth proof of Theorem 2.1.1). Define

$$f(x) = \sum_{m=0}^{pq-p-q} (1 - r_2(m))x^m.$$

Since $r_2(m) = 0$ or $r_2(m) = 1$ for $0 \leq m \leq pq - 1$ then

$$f'(1) = \sum_{m=1}^{pq-p-q} m(1 - r_2(m)) = \sum\{m|1 \leq m \leq pq \text{ and } r_2(m) = 0\}$$

$$= \sum\{m|m \in N(p,q)\} = S(p,q).$$

Thus, the problem of finding $S(p,q)$ was reduced to calculating $f'(1)$ that was achieved in [75] by using the following simple formula discovered by Özlük (and appearing in a more general setting in [408, equation (23)]; see proof of Theorem 4.2.2).

$$g(x) = \frac{P(x) - 1}{x - 1} \text{ where } P(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

Rødseth [375] generalized Brown and Shiue's result by giving a closed form for

$$S_m(p,q) = \sum_{n \in N(p,q)} n^m.$$

Notice that Sylvester's result and Brown and Shiue's result are special cases of Rødseth's equality when $m = 0$ and $m = 1$, respectively.

Theorem 5.5.2 *[375] Let p, q, m be positive integers with $(p,q) = 1$ and $m \geq 1$. Then,*

$$S_{m-1}(p,q) = \frac{1}{m(m+1)} \sum_{i=0}^{m} \sum_{j=0}^{m-i} \binom{m+1}{i} \binom{m+1-i}{j} B_i B_j p^{m-j} q^{m-i}$$
$$- \frac{1}{m} B_m,$$

where the B_is are the Bernoulli numbers[4].

[4] *Bernoulli numbers* are the coefficients of the power series

$$\frac{z}{e^z - 1} = \sum_{j \geq 0} B_j \frac{z^j}{j!}.$$

Bernoulli numbers can also be defined by an implicit recurrence relation, $\sum_{j=0}^{m} \binom{m+1}{j} B_j = 0$ for all $m \geq 0$; see Appendix B.5 for further details.

Theorem 5.5.2 implies the following rather simple formula for $S_2(p,q)$

$$S_2(p,q) = \frac{1}{12}(p-1)(q-1)pq(pq-p-q).$$

Recently, Tuenter [460] has rediscovered the above Rødseth's equality by characterizing, in an elegant manner, the set of integers that have no representation of the form $px+qy$ in non-negative integers x and y.

5.6 Related games

In this section we discuss two games closely related to integer representations.

5.6.1 Sylver coinage

> **Sylver coinage[5]:** *In this game the players alternatively name different numbers, but are not allowed to name 'any' number that is a sum of previously named ones. The 'winner' is the player who names the last number. Of course, as soon as 1 has been played, every other number is illegal (i.e. representable as a sum of ones) and the game ends. Because the player who names 1 is declared the 'loser'. Is there a winning strategy?*

In [40, Chapter 18], it was remarked that the game cannot go on forever due to Sylvester's result[6]. For, at any time after the first move, if g is the greatest common divisor of the moves made then, by Theorem 1.0.1, only finitely many multiples of g are *not* expressible as sums of numbers already played. In fact, one may use Theorem 5.1.1 from the second move to guarantee the existence of only $\frac{1}{2}(a-1)(b-1)$ playable numbers where a and b are the numbers named by the first and second player, respectively.

A position S in sylver coinage is determined by a set of previous moves $\{x_1,\ldots,x_j\}$. The expression $S+n$ denotes the position obtained by adjoining n to the set S. Notice that different sets of moves may be equal as sylver coinage position; for example, the position $\{3,5,10,11\}$ equals the position $\{3,5\}$ since the moves 10 and 11 can be expressed as sums of 3s an 5s, so they do not affect play in the position. A position is said to be *N-position* if the player 'next' to play can win.

[5] Game invented by J.C. Conway.

[6] It is because of this result that the game was called *sylver* coinage.

Every position partitions the set of numbers into *legal* and *illegal* moves; for exemple in the position $\{3, 5\}$ the moves 1,2,4 and 7 are legal (they are not expressed as a sum of 3s an 5s), all other numbers are illegal. Note that in any position S, all moves that lower the value of $(x_1, \ldots, x_j)$ are legal, so the set of legal moves is infinite if and only if $(x_1, \ldots, x_j) > 1$. In a position S with $(x_1, \ldots, x_j) = 1$, a legal move is called an *end* if it does not eliminate any other legal move. In particular, $g(x_1, \ldots, x_j)$ is always an end. A position S where $g(S)$ is the only end is called and *ender*. Thus, in an ender position, every legal move other than $g(S)$ eliminates $g(S)$. Suppose that $g(S) > 1$, the player on the move, say player A, in an ender S must be able to win. Suppose player A plays $g(S)$ if the second player has a winning reply u player A can play u instead of $g(S)$ and reach the same winning position as the second player because $S + g(S) + u = S + u$. Thus every ender with $g(S) > 1$ is N-position.

The most important general result in sylver coinage is due to Hutchings [40, 174].

Theorem 5.6.1 *[174] If $(m, n) = 1$ and $m, n > 3$ then $\{m, n\}$ is a N-position.*

At the moment, there is no way of working out a winning strategy from an arbitrarily given position. In [40, Chapter 18] some winning openings have been studied. We refer the reader to [421] where a variety of results about sylver coinage are presented.

5.6.2 The jugs problem

The jugs problem[7]**:**

> *There are three jugs with integral capacities B, M, and S, respectively, where $B = M + S$ and $M \geq S \geq 1$. Any jug may be poured into any other jug until either the first one is empty or the second is full. Initially jug B is full and the other two are empty (we use B as the name of the jug with capacity B, etc.).*
>
> *We want to divide the wine equally, so that $\frac{1}{2}B$ gallons are in jugs B and M and jug S is empty, and we want to do*

[7] This game is a generalization of the original puzzle with measures $B = 8$, $M = 5$, and $S = 3$ the roots of which can be traced back at least as far as Tartaglia, an Italian mathematician of the sixteenth century; see [316] and [442] for an historical review. We also refer the reader to [341] for closed related results.

so with as few pourings as possible. We ask three questions. Can we share equally? If so, what is the least number of pourings possible; and how do we achieve this least number?

In [289], it is shown that it is possible to share equally if and only if B is divisible by $2r$, where $r = gcd(M, S)$. If this is the case, then the least number of pourings is $\frac{1}{r}B-1$, and the unique optimal sequence of pourings is given by the first $\frac{1}{r}B-1$ steps (pourings) of the algorithm below.

Let us use b, m, s to denote the quantities of wine at any stage in jugs B, M, S, respectively.

```
Jug Algorithm

Pour jug $B$ into jug $M$
Repeat
Pour jug $M$ into jug $S$
Pour jug $S$ into jug $B$
If $m < S$ Then
    Pour jug $M$ into jug $S$
    Pour jug $B$ into jug $M$
```

Note that for simplicity a stopping condition is not included in this algorithm since it is interested only in the first $\frac{1}{r}B-1$ steps; see Example 5.6.2.

In the movie *Die Hard: With a Vegeance*[8] the main characters have to defuse a bomb by measuring four gallons of water using jugs of capacities three and five. The 'good boy' succeeded to defuse the bomb. The way to proceed is the same as first interations of the jug algorithm for the case $B = 8, M = 5$ and $S = 3$; see Example 5.6.2.

Example 5.6.2 Let $B = 8, M = 5$ and $S = 3$. We denote by (b, m, s) the quantities of wine at any stage in jugs B, M, and S, respectively. Thus, the quickest way to reach state $(4, 4, 0)$ form state $(8, 0, 0)$ is given by the following sequence of states: $(8, 0, 0), (5, 0, 3), (5, 3, 0), (2, 3, 3), (2, 5, 1), (7, 0, 1), (7, 1, 0), (4, 1, 3), (4, 4, 0)$ (this sequence is illustrated in Fig. 5.1).

The main result in [289] is based in the following lemmas.

[8] Copyright ©1995 Twenty-Century Fox.

Lemma 5.6.3 *Let M and S be coprime, let $B = M + S$ and let $0 < b < B$. Then there is a unique solution i, j to*

$$B - b = iS - jM \ ,\ 1 \leq i \leq M \ ,\ 0 \leq j \leq S - 1,$$

and it is given by setting

$$iS \equiv B - b \bmod M \textit{ and } jM \equiv b - B \bmod S. \tag{5.5}$$

Proof. Any solution must be given by eqn (5.5). Let i, j be as in eqn (5.5). Then, $iS - jM \equiv B - b \bmod M$ and $\bmod S$, and hence also $\bmod MS$. But $iS - jM \leq MS < B - b + MS$ and $iS - jM \geq S - (S-1) M = M + S - MS > B - b - MS$. Hence indeed $iS - jM = B - b$, as required. □

Lemma 5.6.4 *Let M and S be coprime integers and let $B = M + S$. The jug algorithm starts at vertex $(B, 0, 0)$, makes exactly $2B - 1$ non-trivial moves arriving exatly once at each vertex other than $(0, M, S)$, then makes one 'dummy' move, and terminates back at $(B, 0, 0)$. The*

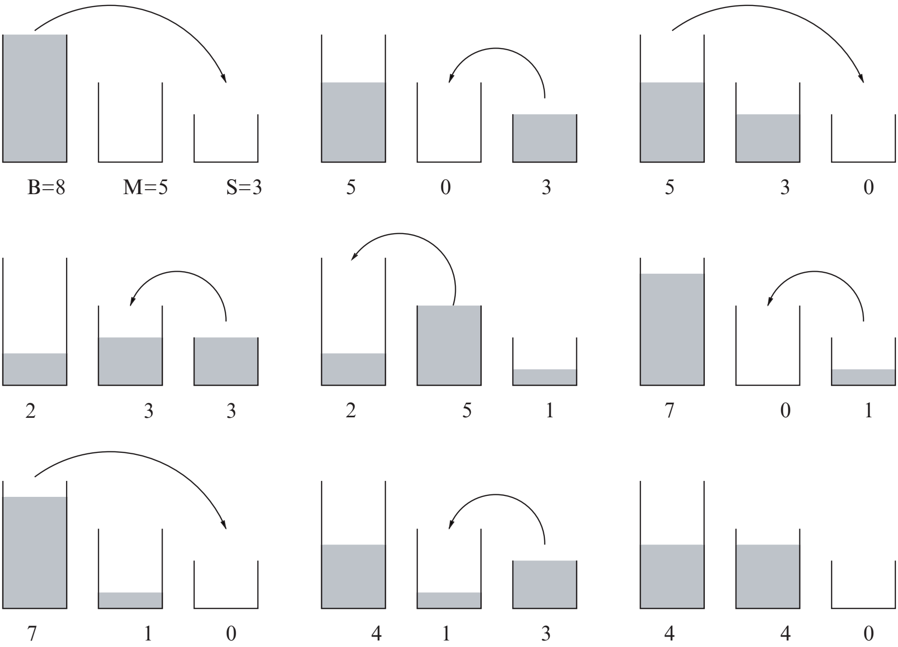

Figure 5.1: Sequence of pourings.

jug algorithm does not visit the vertex (O, M, S)*, and for each vertex* $x = (b, m, s)$ *other than* $(B, 0, 0)$ *and* $(0, M, S)$ *it arrives at* x *after exactly* $t(x)$ *steps, with*

$$t(x) = \begin{cases} 2i + 2j - 1 & \textit{if } s = S \textit{ or } m = 0 \textit{ and } s < S, \\ 2i + 2j & \textit{if } s = 0 \textit{ and } m > 0 \textit{ or } s > 0 \textit{ and } m = M, \end{cases}$$

where i *and* j *are defined as in Lemma 5.6.3.*

5.7 Supplemetary notes

Piehler [328] has also found Theorem 5.2.1 and Rødseth [379] also gave a simpler proof for Theorem 5.2.3. In [374], Rødseth has rediscovered Theorem 5.4.2 as well as Theorem 5.4.1.

In [450], Tinaglia was interested in finding the smallest m_i for which the equation $\sum_{j=1}^{n} a_j x_j = m_i$ has at least i solutions in non-negative integers. Tinaglia determined m_i in the case $n = 3$; see also [448].

We refer the reader to the following web pointer for an enourmous amount of information (results, references, software, etc.) about sylver coinage

`http://www.monmouth.com/~colonel/sylver.`

In [53] Boldi *et al.* studied the jug problem in a more general form (for any set of $n \geq 3$ jugs).

This page intentionally left blank

6

Generalizations and related problems

6.1 Special functions

Let $f = (a_1, \ldots, a_n, t) = f(n, t)$ be the maximum of the Frobenius numbers when $a_1 < \cdots < a_n \leq t$. Let us start with a result of Erdős and Graham [131].

Corollary 6.1.1 *[131] Let $a_1 < \cdots < a_n \leq t$ be integers with $(a_1, \ldots, a_n) = 1$. Then,*

$$2t^2/n > f(n,t) \geq \frac{t^2}{n-1} - 5t.$$

Proof. The upper bound is a consequence of Theorem 3.1.12. The lower bound is obtained by remarking that $f(n,t) \geq g(x, 2x, \ldots, (n-1)x, x^*) \geq \frac{t^2}{n-1} - 5t$, where $x = \left\lfloor \frac{t}{n-1} \right\rfloor$ and $x^* = (n-1)x + 1$, $n \geq 2$. □

Note that by Sylvester's result (*cf.* Theorem 5.1.1) one could actually get $f(2,t) = t^2 - 3t + 1$. Erdős and Graham [131] conjectured that

$$f(3,t) \leq \left\lfloor \frac{(t-2)^2}{2} \right\rfloor - 1,$$

with equality for $\{\frac{t}{2}, t-1, t\}$, $\{t-2, t-1, t\}$ if t is even, and $\{\frac{(t-1)}{2}, t-1, t\}$ if t is odd. This conjecture was proved by Lewin [272] for any $n \geq 3$

$$f(n,t) \leq \left\lfloor \frac{(t-2)^2}{2} \right\rfloor - 1. \tag{6.1}$$

It was showed in [272] that the above upper bound is sharp for $n = 3$. In [273], Lewin improved the upper bound of eqn (6.1) when $n = 3$.

Theorem 6.1.2 *[273] Let $a_1 < a_2 < a_3 = t$. Then,*

$$f(3,t) \le \left\lfloor \frac{1}{2}(a_2-1)(t-2) \right\rfloor - 1.$$

In [272], Lewin conjectured that in general for fixed n and for t large enough

$$f(n,t) \le \left\lfloor \frac{(t-2)(t-n)}{n} \right\rfloor - 1. \tag{6.2}$$

If true in general, then it is best possible, as for every n the bound is attained for infinitely many integers t. Vitek [467] proved Lewin's conjecture for $n = 4$ and showed that for any $n \ge 5$ if $t \ge n(n-3)$ then

$$f(n,t) \le t^2/n. \tag{6.3}$$

Vitek remarked that the restriction $t \ge n(n-3)$ is probably not essential (although in Lewin's conjecture n must be large enough with respect to t).

As an application of a generalization of Vosper's theorem, Hamidoune [179] proved that either $a_1 < \ldots < a_n \le t$ has a very 'special' structure or $f(n,t) \le (k-1)(t-r)-1$ where $t = kn+r$ and $1 \le r \le n$. Hamidoune used the latter bound to prove the uniqueness of sets attaining the bound in this case (the proof depends on a tedious density theorem). From density considerations, Nagata and Matsumura [303] proved that

$$f(n, 2n+k) = 2n+2k-1 \text{ for } 1-n \le k \le -1.$$

They obtained, as a corollary, a result that has to do with the gaps of a point on a closed *Riemann surface*. Erdős [129] proved that

Theorem 6.1.3 *[129] $f(n,2n) = 2n+1$, $f(n,2n+1) = 2n+3$, and for k fixed $f(n,2n+k) = 2n+p(k)$ for some function $p(k)$ provided n is sufficiently large.*

Erdős and Graham found the exact value of $p(k)$ of Theorem 6.1.3.

Theorem 6.1.4 *[131] For fixed k, if n is sufficiently large then*

$$f(n,k) = \begin{cases} 2n+2k-1 & \textit{for } k \le -1, \\ 2n+1 & \textit{for } k = 0, \\ 2n+4k-1 & \textit{for } k \ge 1 \textit{ and } n-k \equiv 1 \bmod 3, \\ 2n+4k+1 & \textit{for } k \ge 1 \textit{ and } n-k \not\equiv 1 \bmod 3. \end{cases}$$

Lev [267] also studied the function $f(n,k)$ for certain values of k, finding that if $2n < k < 3n-2$, then

$$f(n,k) = \begin{cases} 2(2k-3n)+1 & \text{if } k \not\equiv 2 \bmod 3, \\ 2(2k-3n)-1 & \text{if } k \equiv 2 \bmod 3. \end{cases}$$

Dixmier [113] settled a conjecture by Erdős and Graham [132, page 86] stating that

$$f(n,t) \le \frac{t^2}{(n-1)}\cdot$$

Theorem 6.1.5 *[113]*

$$\left\lfloor \frac{t-2}{k-1} \right\rfloor (t-n+1) - 1 \le f(n,t) \le \left\lceil \frac{t-2}{n-1} \right\rceil t - 1\cdot$$

Notice that Lewin's conjectured upper bound (eqn (6.2)) follows from Theorem 6.1.5 if $t \equiv 0$ or 2 mod $(n-1)$. We present a nice simple proof for the upper bound of Theorem 6.1.5 due to Hamidoune [180]. Hamidoune's proof uses the notion of *saturate* sets as well as three well-known additive results (see below). Let us introduce some standard terminology and notation.

Let G be an abelian group. Let $A_1, \ldots, A_j \subset G$. We write

$$A_1 + \cdots + A_j = \{x_1 + \cdots + x_j |\ x_i \in A_i\}.$$

If $A_1 = \cdots = A_j = A$ we write $jA = A_1 + \cdots + A_j$ (with the convention that $0A = \{0\}$).

Let $A \subset \mathbb{N}^*$ be such that $\max(A) = t$ and assume that $\gcd(A) = 1$. We write

$$\psi(A) = \bigcup_{j \ge 0} jA_j \text{ and } \psi_k(A) = \psi(A) \cap [(k-1)t+1, kt].$$

The Frobenius number of A is, by definition,

$$g(A) = \max\{\mathbb{Z} \setminus \psi(A)\}.$$

Lemma 6.1.6 (folklore) *Let G be a finite group and let $A, B \subset G$. If $|A+B| > G$ then $A + B = G$.*

Lemma 6.1.7 *(*Mann Theorem *[286]) Let B be a generating subset of a finite abelian group G such that $0 \in B$. Let A be a subset of G such that $|A+B| \le \min\{|G|-1, |A|+|B|-2\}$. Then, there is a subgroup H of G such that $|H+B| \le \min\{|G|-1, |H|+|B|-2\}$.*

Lemma 6.1.8 (folklore *[113, Lemma 2.3]) Let* $A \subset \mathbb{N}^*$ *be such that* $|A| > \max\{A\}/2$. *Then,*

$$g(A) \leq 2\max\{A\} - 2|A| - 1.$$

We denote by $\bar{A}$ the congruence class, modulo $t = \max\{A\}$, of each element in A and by $\mathbb{Z}_m$ the set of integers modulo m. A subset A of $\mathbb{N}$ is called *saturated* if for all $x, y \in A$ either $x+y \in A$ or $x+y > \max\{A\}$.

Lemma 6.1.9 *[180, Lemma 9.3] Let* $A \subset \mathbb{N}^* = \mathbb{N} \setminus 0$ *be a saturated subset such that* $gcd(A) = 1$, $|A| = n$ *and* $\max\{A\} = t$. *Also assume that* $|A| \leq t/2$. *Let* H *be a proper subgroup of* $\mathbb{Z}_t$ *such that* $|\bar{A} + H| \leq |H| + |\bar{A}| - 2$. *For* $i \in \{0, 1\}$ *put* $t - 1 + i = k_i(n + i - 1) - r_i$ *where* $1 \leq r_i \leq n + i - 1$. *Then,*

$$g(A) \leq (k_0 - 1)(t - r_0 - 1) - 1.$$

Proof for the upper bound in Theorem 6.1.5. Let $A \subset \mathbb{N}^*$ be such that $\max\{A\} = t$, $n = |A|$ and with $gcd(A) = 1$. Now, set $t - 1 = k(n-1) - r$ where $1 \leq r \leq n-1$. We claim that

$$g(A) \leq (k-1)(t - r - 1) - 1. \tag{6.4}$$

Note that eqn (6.4) implies Dixmer's upper bound when $r = 1$. In order to prove inequality (6.4) we assume without loss of generality that A is saturated (since A is contained in some saturated set X such that $g(X) = g(A)$). We have two cases.

Case a) Suppose that for all $j \leq k-1$, $|j\bar{A}| \geq \min\{t, 1 + j(n-1)\}$. By definition of k, we have $1+j(n-1) = \min\{t, 1+j(n-1)\}$. Hence,

$$\begin{aligned}|\psi(A) \cap [1, (k-1)t]| &= \sum_{j=1}^{k-1} |\psi_j| \geq \sum_{j=1}^{k-1} (1 + j(n-1)) \\ &= (k-1)(2 + k(n-1))/2 = (k-1)(t+r+1)/2.\end{aligned}$$

Recall that $A \subset \psi(A) \cap [1, (k-1)t] \subset \psi(A)$, obtaining that $g(A) = g(\psi(A) \cap [1, (k-1)t])$. By Lemma 6.1.8, $g(A) = g(\psi(A) \cap [1, (k-1)t]) \leq (k-1)(t - r - 1) - 1$.

Case b) Suppose that there exists $j \leq k-1$, $|j\bar{A}| < \min\{t, 1 + j(n-1)\}$. Note that $j \geq 2$. By Lemma 6.1.6, $2n \leq t$. Take a maximal $i \leq j-1$ such that $|i\bar{A}| \geq 1 + i(n-1)$. By putting $B = i\bar{A}$ we have $|B + \bar{A}| < \min\{t, |B| + |\bar{A}| - 1\}$ and by Mann's Theorem (Lemma 6.1.7), there is a proper subgroup H such that $|H+\bar{A}| \leq |H|+|\bar{A}|-2$. Finally, by Lemma 6.1.9, $g(A) \leq (k-1)(t-r-1)-1$. □

In [113], Dixmier also improved the upper bound of Theorem 6.1.5 and gave the exact value of $f(n,t)$ for some special cases.

Theorem 6.1.10 *[113]*

(i) $f(n,t) \leq 2vt - v(v+1)n + v^2 - v - 1$ *where* $v = \left\lfloor \frac{t-2}{n-1} \right\rfloor$.

(ii) if $n-1$ *divides* t *or* $t-2$ *then*

$$f(n,t) = \frac{t(t-2)}{n-1} - t + 1.$$

(iii) if $n-1$ *divides* $t-1$ *then*

$$f(n,t) = \frac{(t-1)^2}{n-1} - t.$$

Lev [266, 268] gave an independent proof of Theorem 6.1.10 (i) and remarked that equality holds if $t \equiv 0 \bmod (v+1)$. Kiss [242] extended the validity of Erdős and Graham formula (*cf.* Theorem 6.1.4) for any $n \geq k+2$ using the upper bound of Theorem 6.1.10.

Theorem 6.1.11 *[242] Let* d, n, k *be integers such that* $2 \leq d < n$, $0 \leq k \leq n-d$. *If* $n-k \equiv 0 \bmod d+1$ *or* $n-k \equiv -1 \bmod d+1$ *then*

$$f(n, dn+k) = d(d-1)n + 2dk + d^2 - d - 1.$$

The function $f(n,t)$ for sets that are the union of two arithmetic progressions with the same difference has been investigated by Janz [218].

Theorem 6.1.12 *[218] Let* $\mathcal{F}$ *be the set of all saturated subsets* A *of* $\mathbb{N}^*$ *such that* $A \cup \{0\}$ *is the union of two arithmetic progressions with the same difference. Let* $a_1, \ldots, a_n \leq t \in \mathcal{F}$ *where* $t \geq (9n^3 - 30n^2 + 4n - 22)/4$ *non-congruent to 0 or 1 modulo* $(n-1)$. *Then,*

$$f(n,t) \leq f(t, t-1, \ldots, t-n+1).$$

By using the *critical pair* method introduced in [180], Hamidoune obtained a different proof of a sharper (and more involved) result than that presented in Theorem 6.1.12.

Let $h(a_1, \ldots, a_n, t) = h(n,t)$ be the minimum of the Frobenius numbers when $t \leq a_1 < \cdots < a_n$. Hujter [207] proved that the following inequalities hold for some absolute positive constants c_1 and c_2

$$c_1 \leq \frac{h(n,t)}{(n-1)t + \frac{1}{n-1}} \leq c_2. \qquad (6.5)$$

6.2 The modular generalization

Skupień [427] formulated and studied a generalization of **FP** on numerical semigroups, namely, the *modular change* problem that is defined as follows. Let $a_1, \ldots, a_n$ and m be natural numbers. For $j \in \{0, \ldots, m-1\}$ a given non-negative natural number p is called *j-omitted* if it has no representation $p = \sum_{i=1}^{n} x_i a_i$ with non-negative naturals x's such that $\sum_{i=1}^{n} x_i \equiv j \bmod m$. The largest of the j-omitted numbers is denoted by $N_j(m; a_1, \ldots, a_n)$ (if there is not one we write $N_j(m; a_1, \ldots, a_n) = -1$). Let $\Omega_j(m; a_1, \ldots, a_n)$ be the number of j-omitted natural non-negative numbers and let $k(m; a_1, \ldots, a_n) = \max\{N_j(m; a_1, \ldots, a_n) | j \in \{0, \ldots, m-1\}\}$. We have that $k(1; a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$.

Skupień [427] characterized the existence of $k(m; a_1, \ldots, a_n)$ for arbitrary m and found the exact values of $k(m; a_1, a_2)$ and $\Omega_j(m; a_1, a_2)$.

Theorem 6.2.1 *[427] Let $a_1, \ldots, a_n$ and m be natural numbers. Then, $k(m; a_1, \ldots, a_n)$ is finite if and only if $(a_1, \ldots, a_n) = 1$ and $(m, a_2 - a_1, a_3 - a_2, \ldots, a_n - a_{n-1}) = 1$.*

Theorem 6.2.2 *[427] Let a_1 and a_2 be positive integers with $(a_1, a_2) = 1$.*

(i) $k(m; a_1, a_2) = ma_1a_2 - a_1 - a_2$,

(ii) $N_j(m; a_1, a_2) = k(m; a_1, a_2) - (m-2-j)a_1$ *for each* $-1 \leq j \leq m-2$, *where* N_{-1} *denotes* N_{q-1}.

(iii) $\Omega_j(m; a_1, a_2) = \frac{j(m; a_1, a_2)+1}{2}$.

Hence the interval $[0, k(m; a_1, a_2)]$ contains as many j-representable integers as j-omitted ones (keeping the same property as for the case $m = 1$; see Theorem 5.1.1). Hofmeister [201] found a formula for $k(m; a_1, \ldots, a_n)$ for arithmetic progression sequences.

Theorem 6.2.3 *[201] Let $a, d,$ and m be natural numbers with $(am, d) = 1$. Then,*

$$k(m; a, a+d, \ldots, a+jd) = \left\lfloor \frac{ma-2}{j} \right\rfloor a + (ma-1)d.$$

Note that Theorem 6.2.3 implies Theorem 6.2.2 part (i) by setting $j = 1$ and $a + d = b$.

An integer is called *omitted* if it is j-omitted for some $j \in \{0, \ldots, m-1\}$. Let $\omega(m; a_1, \ldots, a_n)$ be the number of omitted numbers. Hofmeister [201] also found a formula for $\omega(m; a_1, \ldots, a_n)$ for arithmetic sequences.

Theorem 6.2.4 *[201] Let a, d and m be natural numbers with $(am, d) = 1$ and let $(m-1)a = q_1 j - r_1$, $0 \leq r_1 < j$ and $a - 1 - r_1 = q_2 j + r_2$, $0 \leq r_2 < j$. Then,*

$$\begin{aligned}\omega(m; a, a+d, \ldots, a+jd) = &\frac{1}{2}\left((a-1)(q_2+d) + (r_2 - r_1)(q_2+1)\right) \\ &+ \left((m-1)d + q_1\right) a.\end{aligned}$$

Theorem 6.2.4 covers the general case of two basis elements by setting $j = 1$ and $a + d = b$, that is,

$$\omega(m; a, b) = \frac{(a-1)(b-1)}{2} + (m-1)ab. \tag{6.6}$$

We close this section by stating the following upper bound given by Skupień [427] that implies Erdős and Graham's upper bound given in Theorem 6.1.1 when $m = 1$.

$$k(m; a_1, \ldots, a_n) \leq 2ma_{n-1} \left\lfloor \frac{a_n}{n - 1 + \frac{1}{m}} \right\rfloor (m-1)(a_{n-1} - a_1) - a_n.$$

Thus $k(m; a_1, \ldots, a_n)$ is of order $O\left(\frac{ma_n^2}{n}\right)$.

Skupień [427] used the modular change problem to extend Wilf's algorithm (*cf.* Section 1.2.5).

Skipień's algorithm

Processes consecutive integers $n \in \mathbb{N}$ using the following simple rule:

r is $(j+1)$-representable
if and only if
$r - a_i$ is j-representable

for some $i = 1, \ldots, n$ with $j \in \{0, \ldots, m-1\}$.

Store the corresponding information in the lattice with $m - 1$ columns and 'large' number of rows, that is, entry (light) (n, j) is 1 (light is on) if and only if n is j-representable or 0 (light is off) otherwise.

During the process we keep updating $R[j]$, the number of j-representable integers. Let $N[j]$ be the largest integer such that it is the a_1-th of consecutive j-representable integers.

The process stops at the first s which is the a_1-th of consecutive *fully representable numbers* (a number is *fully representable* if it is j-representable for each $j = 0, \dots, m-1$). Then,

$$\Omega_j(m; a_1, \dots, a_n) = s + 1 - R[j], \quad N_j = N[j] - a_1$$

and

$$k(m; a_1, \dots, a_n) = \max\{N_j(m; a_1, \dots, a_n) | j \in \{0, \dots, m-1\}\}.$$

Example 6.2.5 Let $m = 3$, $a_1 = 4$ and $a_2 = 5$. Figure 6.1 shows the corresponding lattice of lights with entry (n, j) filled circle if n is j-representable and empty circle otherwise. We have that $s = 55$, $N_0(3; 4, 5) = N[2] - 4 = 51 - 4 = 47$, $N_1(3; 4, 5) = N[1] - 4 = 55 - 4 = 51$, $N_2(3; 4, 5) = N[2] - 4 = 47 - 4 = 43$ and $R[0] = R[1] =$

n \ k	0	1	2
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	●	○	○
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	●	●	●

Figure 6.1: Lattice of lights.

$R[2] = 30$. So, $\Omega_j(3;4,5) = 55 - 30 + 1 = 26$ for each $j = 0,1,2$ and $k(3;4,5) = \max\{43,47,51\} = 51$. Notice that $\omega(3;4,5) = 56 - 10 = 46$ which can also be obtained by eqn (6.6).

6.3 The postage stamp problem

The (local) *postage stamp* problem is defined as follows. Given an integral basis (the stamp denominations) $A_n = \{a_1, \ldots, a_n\}$, $1 = a_1 < a_2 < \ldots < a_n$. For a positive integer h (the size of the envelope, that is, the envelope has room for at most h different stamps) we form all the combinations

$$x_1a_1 + \cdots + x_na_n, x_i \geq 0 \text{ with } x_1 + \cdots + x_n = h,$$

and ask for the smallest integer $S_h(A_n)$ that is not represented as the above combination (the smallest amount of postage that cannot fit on the envelope).

Let $s_h(A_n) = S_h(A_n) - 1$. $s_h(A_n)$ is called the *h-range* and is defined as the largest integer such that each integer between 0 and $s_h(A_n)$ can be represented as sums of at most h elements of $a_1, \ldots, a_n$ (allowing repetitions). The postage stamp problem was apparently introduced by Rohrbach [359, 360] in 1937, and since then a number of papers have been written about it and a variant, namely, the *global postage stamp problem* (see below). We refer the reader to [396–401] for results concerning h-range and [403] for a comprehensive summary on the problem.

The connection of the **FP** with the postage stamp problem was found by Meures [294] (independent proofs were also given by Rødseth [377] and Hofmeister [199]; see also [399]).

Theorem 6.3.1 *[294] There exists a positive integer h_1 such that*

$$s_h(A_n) = ha_n - g(\bar{A}_n) - 1 \text{ for any } h \geq h_1,$$

where $\bar{A}_n = \{a_n - a_{n-1}, a_n - a_{n-2}, \ldots, a_n - a_1, a_n\}$.

Notice that $g(a_n - a_{n-1}, a_n - a_{n-2}, \ldots, a_n - a_1, a_n)$ is well defined since $a_n - a_1 = a_n - 1$ and thus $(a_n - a_1, a_n) = 1$. The value h_1 in Theorem 6.3.1 is usually dificult to determine. Several upper bounds for h_1 are given by Kirfel [238, 239] and in [403, page 8.2]. It turns out that if A_n is *pleasant*[1] then both h and $s_h(A_n)$ are known and thus

[1] $A_n = \{a_0, \ldots, a_n\}$, $1 = a_0 < a_1 < \cdots < a_n$ is *pleasant* if and only if the regular representation $n = \sum_{i=0}^{n} e_ia_i$ has a minimal coefficient sum among all possible representations $n = \sum_{i=0}^{n} x_ia_i$ for all natural numbers n.

$g(A_n)$ can be determined. Hence, it is natural to ask when $\bar{A}_n$ can be organized as a regular basis (see Section 3.4 for the definition of regular basis). Selmer [395] has studied the latter in some cases; see also [115, 241, 492].

Alter and Barnett [7, Problem 8] asked if there exists a polynomial time algorithm that solves the postage stamp problem. Shallit [410] observed that the following corollary of Theorem 6.3.1 together with the $\mathcal{NP}$-hardness result of **FP** (*i.e.* Theorem 1.3.1) answer the latter negatively (unless $\mathcal{P} = \mathcal{NP}$).

Corollary 6.3.2 *[410] Let $a_1, \ldots, a_n$ be positive integers such that $(a_1, \ldots, a_n) = 1$. Then, there exist positive integers $b_1, \ldots, b_n$ and h_1 such that*

$$g(a_1, \ldots, a_n) = hb_n - s_h(b_1, \ldots, b_n) \text{ for any } h \geq h_1.$$

Proof. Take $b_i = a_n - a_{n-i}$ for each $i = 1, \ldots, n$ with $a_0 = 0$. □

6.4 $(a_1, \ldots, a_n)$-trees

A *tree* T is a connected acyclic directed graph with a distinguished vertex called the *root*. We assume that the direction of the edges is downward. The *height* of a vertex in T is the length of the (unique) path from the root to the vertex. A vertex v is called a *leaf* if its outdegree is zero and all other vertices are called *internal*. The *level* m of T is the set of vertices of height m. A $(a_1, \ldots, a_n)$*-tree* is a tree with internal vertices having outdegrees in $\{a_1, \ldots, a_n\}$ and leaves of the same height.

An integer N is said to be $(a_1, \ldots, a_n)$*-realizable* if there exists a $(a_1, \ldots, a_n)$-tree with N leaves. Figure 6.2 shows a $(3, 4)$-tree with 11 leaves implying that 11 is $(3, 4)$-realizable.

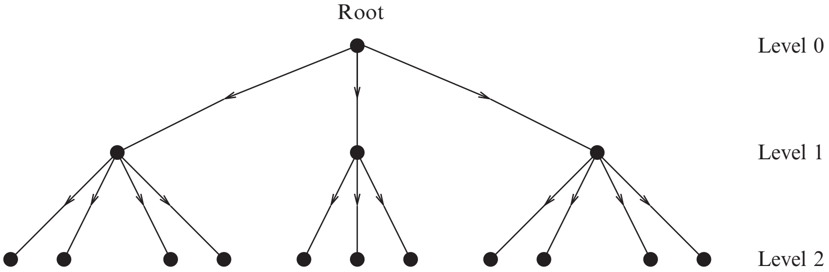

Figure 6.2: A $(3, 4)$-tree.

Let $b_i = a_i - a_1$ for all $i \geq 2$. In [319], Ottman *et al.* proved that all but finite set of positive integers are $(a_1, \ldots, a_n)$-realizable if and only if $(b_2, \ldots, b_n) = 1$ (this was also proved by Lee *et al.* in [262]).

Lemma 6.4.1 *Let N be a positive integer. If N is $(a_1, \ldots, a_n)$-realizable then $N - 1$ can be written of the form*

$$N - 1 = \sum_{i=1}^{n} x_i(a_i - 1) \text{ where } x_i \text{ is a non-negative integer for all } i.$$

Proof. Since N is $(a_1, \ldots, a_n)$-realizable then there exists a $(a_1, \ldots, a_n)$-tree T with N leaves. Let x_i be the number of vertices on T having outdegree a_i. Then,

$$\text{the number of leaves in } T = N = 1 + \sum_{i=1}^{n} x_i(a_i - 1),$$

and the result follows. □

The converse of Lemma 6.4.1 is not true. For instance, a result of Jones [221] implies that there is not a $(3, 4)$-tree having 80 leaves (see below). However, it turns out that all integers greater than 80 are $(3, 4)$-realizable. This naturally leads to the following definition. Let $\kappa(a_1, \ldots, a_n)$ be the least positive integer such that for all $N \geq \kappa$, N is $(a_1, \ldots, a_n)$-realizable. Lemma 6.4.1 implies that

$$g(a_1, \ldots, a_n) \leq \kappa(a_1 + 1, \ldots, a_n + 1).$$

If the property on the height of the leaves in a $(a_1, \ldots, a_n)$-tree were dropped (that is, if there were no restriction on the level location of the leaves) and the function κ were redefined accordingly, then, in this case, we would have that $\kappa(a_1 + 1, \ldots, a_n + 1) = g(a_1, \ldots, a_n)$.

In [221], Jones showed that if $a_1, \ldots, a_n$ form an interval, that is, if $a_{i+1} = a_i + 1$ for $i = 1, \ldots, n - 1$ then the number of integers that are $(a_1, \ldots, a_n)$-realizable is given by

$$\cup_{j=1}[a_1^j, a_n^j],$$

where $[a_1^j, a_n^j]$ denote the set of integers lying in the interval between a_1^j and a_n^j. So, the number of integers that are $(3, 4)$-realizable is

$$[3, 4] \cup [9, 16] \cup [27, 64] \cup [81, 256] \cup [243, 1024] \cup \ldots,$$

and thus, the largest integer that is not $(3, 4)$-realizable is 80.

6.5 Vector generalization of FP

A geometric interpretation of **FP** is as follows. If $(a_1, \ldots, a_n) = 1$ then the (1-dimensional) non-negative half-line cone (spanned by $a_1, \ldots, a_n$) can be shifted into its own inside in such a way that the shifted cone contains only integers representable by the integers $a_1, \ldots, a_n$.

Vizvári [468,470,474] has generalized **FP** to its m-dimensional analogue as follows. Let $\{\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}\}$ be m-dimensional integer vectors. Let $A = (\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$ be a $(m \times n)$ matrix containing a basis of $\mathbb{R}^m$. Let

$$\text{cone}(A) = \{Ax | x \in \mathbb{Q}_{\geq 0}\},$$

and

$$\text{mon}(A) = \{Ax | x \in \mathbb{Z}^n_+\}.$$

Then the *pseudo-conductor* of vectors $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$, denoted by $h = h(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$ is a vector in mon(A) such that every integral vector of the set $h + cone(A)$ is a non-negative integer combination of $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ (*i.e.* the cone A is shifted into its own inside in such a way that all integer points of the shifted cone are representable). Note that in the one-dimensional case $h(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$ is not an element of mon(A), *i.e.* in the one-dimensional case $h(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}) + 1 = g$ but in the general case $h \in \text{mon}(A)$.

Vizvári [468] gave a complete characterization for the existence of such a vector $h(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$; see also [383, 384] and [217] for an equivalent result.

Theorem 6.5.1 *[150, 217, 468, 474] Let $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ be m-dimensional integer vectors and assume that the set $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ contains a linear basis of the space $\mathbb{R}^m$. Let $\{\Omega_1, \ldots, \Omega_r\}$ be the set of all $(m \times m)$ matrices with the columns chosen from A and let $d_{\Omega_i} = |det\ \Omega_i|$, $1 \leq i \leq r$. Then,*

$$(d_{\Omega_1}, \ldots, d_{\Omega_r}) = 1, \tag{6.7}$$

if and only if a pseudo-conductor $h(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$ exists.

Remark 6.5.2 *The condition $(d_{\Omega_1}, \ldots, d_{\Omega_r}) = 1$ in Theorem 6.5.1 means that the lattice $L(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$ generated by the vectors $\mathbf{a_1}$, $\mathbf{a_2}, \ldots, \mathbf{a_n}$ is the standard lattice $\mathbb{Z}^m$, that is,*

$$L = L(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}) = \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{a_i} \quad \lambda_i \in \mathbb{Z}, i = 1, \ldots, n \right\}.$$

The proof of Theorem 6.5.1 can be obtained from the following two propositions given by Khovanskii in [234] where its relation with the *Newton* polyhedron is investigated; see also [235].

Proposition 6.5.3 *[234] Let D be a finite subset of $\mathbb{Z}^n$, $\mathbb{Z}^n \subset \mathbb{R}^n$ such that the subgroup generated by the elements of D coincides with the group $\mathbb{Z}^n$. Then, there exists a constant C with the following property: for every linear combination $\sum \alpha_i a_i$ of vectors $a_i \in D$ with real coefficients α_i such that $\sum \alpha_i a_i$ is an integral vector, there exists a linear combination $\sum_i n_i a_i$ of a_i with integer coefficients such that it is equal to $\sum \alpha_i a_i$ and $\sum |n_i - \alpha_i| < C$.*

Proof. For every x from the finite set X of integral vectors represented in the form $x = \sum \alpha_i a_i$ with $0 \leq \alpha_i \leq 1$, fix a representation of the form $x = \sum n_i(x) a_i$ with $n_i(x) \in \mathbb{Z}$. Such representation exists because the elements $a_i \in D$ generate the group $\mathbb{Z}^n$. Now, take $C = m + q$ where $m = |D|$ and $q = \max_{x \in X} \sum_{i=1}^{m} |n_i(x)|$. Thus, for any integral vector $z \in \mathbb{Z}^n$ of the form $\sum \alpha_i a_i$, the vector $x = z - \sum \lfloor \alpha_i \rfloor a_i$ belongs to X. Hence, $x = \sum n_i(x) a_i$ and $z = \sum n_i a_i$ where $n_i = \lfloor \alpha_i \rfloor + n_i(x) < C$. □

Proposition 6.5.4 *[234] Let D be a finite subset of $\mathbb{Z}^n$ such that it coincides with $\mathbb{Z}^n$. Then every integral point in $con(D) + x$ where $x = C \sum_{a_i \in A} a_i$ and C is the constant occurring in Proposition 6.5.3 is representable by the elements of D.*

Proof. If the vector $z - x$ lies in the $con(D)$, then this vector can be represented in the form $z - x = \sum \alpha_i a_i$, $\alpha_i \geq 0$. Therefore, each integral vector z can be represented in the form $z = \sum (\alpha_i + C) a_i$ where $\alpha_i \geq 0$. By Proposition 6.5.3, every integral vector z of this form can be represented as a linear combination of vectors of a_i with natural coefficients. □

Example 6.5.5 Let $A = \begin{pmatrix} 5 & 3 & 3 \\ 2 & 2 & 3 \end{pmatrix}$. We illustrate con$(A)$ in Fig. 6.3. We have

$$\Omega_1 = \begin{pmatrix} 5 & 3 \\ 2 & 2 \end{pmatrix} \qquad \Omega_2 = \begin{pmatrix} 5 & 3 \\ 2 & 3 \end{pmatrix} \qquad \Omega_3 = \begin{pmatrix} 3 & 2 \\ 3 & 3 \end{pmatrix},$$

and thus,

$$d_{\Omega_1} = \begin{vmatrix} 5 & 3 \\ 2 & 2 \end{vmatrix} = 4, \quad d_{\Omega_2} = \begin{vmatrix} 5 & 3 \\ 2 & 3 \end{vmatrix} = 9, \quad d_{\Omega_3} = \begin{vmatrix} 3 & 3 \\ 2 & 3 \end{vmatrix} = 3.$$

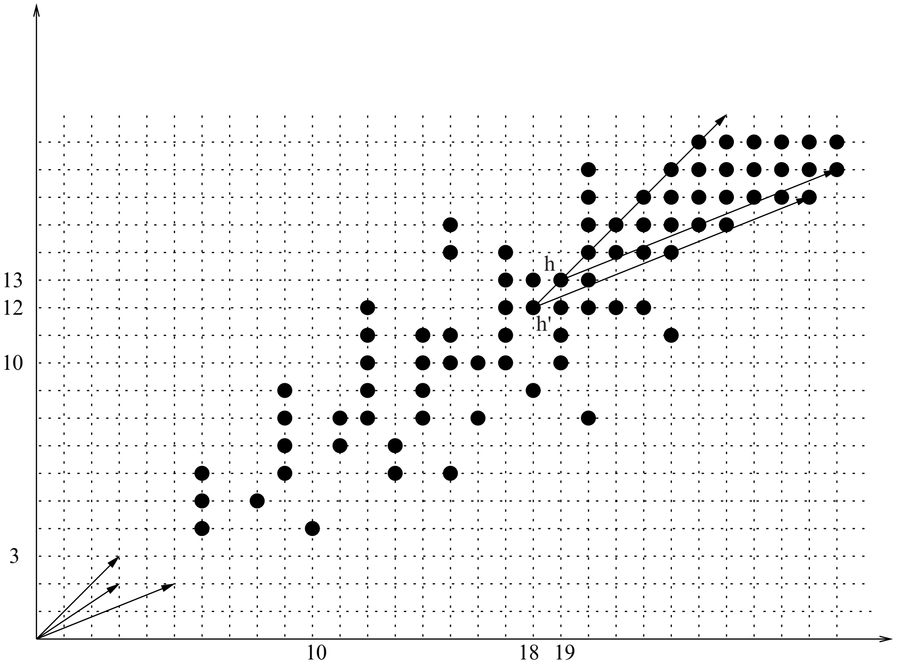

Figure 6.3: Lattice $\mathbb{Z}^2$ with points (filled circles) belonging to con(A) (A defined in Example 6.5.5) and translations of $(19, 13)$+con(A) and $(18, 12)$+con(A).

Therefore, $(d_{\Omega_1}, d_{\Omega_2}, d_{\Omega_3}) = (4, 9, 3) = 1$. By Theorem 6.5.1, the semi-conductor h of matrix A exists. For instance, with $h = (19, 13)$ then clearly all integer points inside h+con(A) are representable as a non-negative integer combination of vectors $(5, 2), (3, 2)$ and $(3, 3)$.

If the columns of A form a *Hilbert basis*[2], then, by Remark 6.5.2, every integral vector of the con(A) is the pseudo-conductor of the vectors $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$. The latter motivated Rycerz [382,384] to introduce and study the notion of an m-conductor. A pseudo-conductor is called

[2] A set of integral vectors $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ is called a *Hilbert basis* if every integral vector in the con(A) can be expressed as a non-negative integer combination of $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$.

an *m-conductor* of $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ if it has the smallest *Euclidean* distance from among all pseudo-conductors.

Example 6.5.6 In continuation of Example 6.5.5 we have that the 2-conductor of A is given by vector $h' = (18, 13)$; see Fig. 6.3.

The vector generalization was also obtained independently by Ivanov and Shevchenko [217], Halter-Koch [178] and more recently by Simpson and Tijdeman [424] subject to a geometric condition on the input set of vectors. In [332], Pleasants *et al.*, gave generalizations of both Theorem 5.1.1 and the notion of symmetry; see Section 7.2 in the case when $n = \dim L$ or $\dim L - 1$. This also has been done by Reid and Roberts in [349, Theorem 5.2].

6.6 Supplementary notes

In [314], Norman reports a *level conjecture* that appears to have important consequences for estimating $f(n,t)$. Norman proved the level conjecture for $n = 3$ and used it to prove Lewin's conjecture in the case $n = 3$. Hofmeister [202] gave an asymptotic formula for $f(n,t)$ for certain classes of sequences. In [117], Djawadi and Hofmeister introduced two functions and studied their connection with **FP**. Analogously to $f(n,t)$, Kiss [242] defined $\mu(n,t)$ as $\mu(n,t) = \max N(a_1, \ldots, a_n)$ where the max is taken over all sequences satisfying $1 < a_1 < \cdots < a_n \leq t$. Kiss proved that $\mu(n,t) = N(t-n+1, t_n+2, \ldots, t)$ for any $1 \leq n \leq t$; see also [243].

Rødseth [376–380] gave an upper bound of s_h and proposed to determine all sets $A = \{1, a_2, 2a_2, \ldots, (k-2)a_2, a_n\}$ with certain parameters; see the work by Selmer and Selvik [394]. A variant of the postage stamp problem is as follows: for arbitrary $h \geq 2$ and $n \geq 2$ one may generally ask for the extremal h-range $m_h(n)$ and the corresponding extremal base(s) A_n^* where $s_h(A_n^*) = m_h(n)$. In stamp terminology, the problem is as follows. Given the number of stamp denominations and the size of the envelope. How should the denominations be chosen to cover the largest possible block of consecutive postages that can be stamped? Selmer [402] denotes this as the (global) *postage stamp problem.* In contrast to this, the local stamp problem consists on determining the h-range $m_h(A_n)$ for given h and A_n; see also [409] for a closed related amusing problem.

Novikov [315] considered a multidimensional analogue of **FP**; see also [269, 270].

This page intentionally left blank

7
Numerical semigroups

Let S be a finitely generated commutative semigroup[1] with 0. We shall write $S(s_1, \ldots, s_n)$ or $< s_1, \ldots, s_n >$ to denote the semigroup generated by integers $s_1, \ldots, s_n$. In this chapter, S will always denotes a semigroup of integers such that $n + \mathbb{N} \cup \{0\} \subseteq S$ for some $n \in \mathbb{N}$ (such semigroups are called *numerical semigroups*). The latter is equivalent to the condition that $(s_1, \ldots, s_n) = 1$. The least positive integer belonging to S is called the *multiplicity* of S (denoted by $\mu(S)$). The cardinality of an irredundant set of generators of S is called the *embedding dimension* of S (denoted by $e(S)$). Notice that $g(s_1, \ldots, s_n) = g(S)$ is the largest integer not belonging to $< s_1, \ldots, s_n >$ ($g(S)$ is also known as the *conductor* of S).

7.1 Gaps and non-gaps

The *genus* of a numerical semigroup S is the number $N(S) = \#(\mathbb{N} \setminus S)$; see Chapter 5. Throughout this section will be assumed greater than zero. The positive elements of S (resp. $\mathbb{N} \setminus S$) are called the *non-gaps* (resp. *gaps*) of S. We denote by $\rho_i(S) = \rho_i$ the i-th non-gap of S. We also enumerate the gaps of S by increasing order $l_1, < \cdots < l_{N(S)}$. So $l_{N(S)} = g(S)$ is the largest gap of S. Finally, the number of gaps smaller than ρ_i will be denoted by $n(\rho_i)$.

One motivation to study gaps comes from the important role they play in the concept of *symmetry* (see next section) as well as in the investigations of *hyperelliptic* and *Weierstrass* semigroups (see Section 7.1.2). The following proposition gives some basic results on gaps (some parts of this proposition can be found in [205, 240, 252]).

[1] A semigroup $(S, *)$ consists of a non-empty set S and an associative binary operation $*$ on S.

Proposition 7.1.1 *Let S be a semigroup. Then,*

(i) $N(S) = 0$ *if and only if* $g(S) = 1$.

(ii) *If* $N(S) > 0$ *then* $N(S) \leq g(S)$.

(iii) $\rho_1 = 0$ *and* $\rho_2 = 1$ *if and only if* $N(S) = 0$.

(iv) S *has at least* $N(S)$ *non-gaps in* $[1, \ldots, 2N(S)]$.

(v) $g(S) < 2N(S)$.

(vi) *If* $l \in \mathbb{N}$ *then* $N(\rho_l) = \rho_l - l + 1$.

(vii) *If* $l \in \mathbb{N}$ *then* $\rho_l \leq l + N(S) - 1$ *and equality holds if and only if* $\rho_l + 1 \geq g(S)$.

(viii) *If* $l > g(S) - 1 - N(S)$ *then* $\rho_l = l + N(S) - 1$.

(ix) *If* $l \leq g(S) - 1 - N(S)$ *then* $\rho_l < g(S)$.

(x) *Let* $B \subset \mathbb{N} \cup \{0\}$ *and* $a \in \mathbb{N} \cup \{0\}$. *We write* $(a + B) = \{a + b | b \in B\}$. *Then,* $|S \setminus (s + S)| = s$ *for any* $s \in S$.

Proof. Parts $(i), (ii), (iii)$ and (iv) are clearly true.

(v) Let $[p, q]$ denotes the set of integers m with $p \leq m \leq q$. Let $r \geq 2N(S)$ and consider the following two subsets of $[0, r]$:

$$I = S \cap [0, r] \text{ and } J = \{r - i | i \in I\}.$$

Notice that each set contains at least $r + 1 - N(S)$ integers. Since $2(r + 1 - N(S)) \geq r + 2 > r + 1$ then I and J have a common element. Hence, there exists $i, j \in I$ such that $i = r - j$. This shows that $r = i + j \in S$ and then $g(S) < 2N(S)$.

(vi) The non-gap ρ_l is the $(\rho_l + 1)$-th element of $\mathbb{N} \cup \{0\}$. So ρ_l is the $(\rho_l + 1 - N(l))$-th element of S. Hence, $l = \rho_l + 1 - N(l)$.

(vii) $N(\rho_l) \leq g(S)$ and $N(\rho_l) = g(S)$ if and only if $\rho_l \geq g(S) + 1$.

(viii) $g(S) + 1$ is the $(g(S) + 1)$-th element of $\mathbb{N} \cup \{0\}$ and all gaps are strictly smaller than $g(S)$. So, $g(S) + 1$ is the $(g(S) + 1 - g)$-th element of S. Hence, $g(S) + 1 = \rho_{g(S)+1-N(S)}$. If $l > g(S) - 1 - N(S)$ then $\rho_l \geq \rho_{g(S)+1-N(S)} = g(S) + 1$. Therefore, by part (vii), $\rho_l = l + N(S) - 1$.

(ix) If $l \leq g(S) - 1 - N(S)$ then $\rho_l \leq l + N(S) - 1 \leq g(S)$, but, by definition of $g(S)$, $\rho_l < g(S)$.

(x) Let $T = \{t \in \mathbb{N} | t \geq s + g(S) + 1\}$. Then, T is contained in S and in $(s + S)$. Let $U = \{u \in S | u < s + g(S) + 1\}$ then the number of elements of U is equal to $s + g(S) + 1 - N(S)$ and S is the disjoint union of T and U. Let $V = \{v \in (s + S) | s \leq v < s + g(S) + 1\}$ then, the number of elements of V is equal to $g(S) + 1 - N(S)$ and $(s + S)$ is the disjoint union of V and T. Moreover, since $s \in S$ and S is a semigroup then $V \subseteq U$. Hence,

$$|S \backslash (s+S)| = |U| - |V| = (s+g(S)+1-N(S)) - (g(S)+1-N(S)) = s.$$

□

Lemma 7.1.2 *[240] Let $S =< p, q >$ and let $M \in S$ with $M < (p-1)q$. Let P_M be the number of pairs $m_1, m_2 \in S$ such that $M = m_1 + m_2$. Then, there is at least one gap in the interval $[M - P_M, M]$.*

Proof. Since $M \in S$ and $M \leq l_{N(S)}$ then $M = xp + yq$ with $x, y \geq 0$ and $y < p$ and thus

$$M = xp + yq = (x_1 p + y_1 q) + (x_2 p + y_2 q) = m_1 + m_2.$$

The system $x = x_1 + x_2$, $y = y_1 + y_2$ has exactly $P_M = (x+1)(y+1)$ pair of non-negative integers solutions that are pairwise since $0, y_1, y_2 \leq y < p$. Let $M - z$ be an element of $[M - P_M, M]$, then

$$M - z = s_z p + r_z q,\ 0 \leq r_z < p \text{ for } z = 0, \ldots, P_M. \tag{7.1}$$

We claim that $s_z < 0$ for some z (implying that there is at least one gap in the interval $[M - P_M, M]$). We have two cases.

Case A) If $P_M < p$ then the set of r_z, $0 \leq z \leq P_M$ takes $P_M + 1$ distinct non-negative integers. So, there is at least one $r_z \geq P_M = (x + 1)(y + 1)$ and, for the corresponding s_z, we have

$$s_z p = M - z - r_z q \leq xp + yq - z - (x+1)(y+1)q \leq x(p-q) - z - q < 0,$$

since $p < q$.

Case B) If $P_M \geq p$ then, since $M - z \equiv q r_z \bmod p$ and $(p, q) = 1$, there exists $0 \leq z \leq P_M$ such that $r_z = p - 1$. We have, for the corresponding s_z

$$s_z p = M - z - r_z q \leq M - (p - 1)q < 0,$$

since, by hypothesis, $M < (p - 1)q$. □

In [345], we have investigated the distribution of the gaps of $S = < p, q >$ in the interval $[0, \ldots, pq - (p+q)]$ by applying Pick's theorem (as used in the third proof of Theorem 2.1.1).

Theorem 7.1.3 *[345] Let p, q be relatively prime integers. Let $G(s)$ be the number of gaps of $S =< p, q >$ in the interval $[pq - (k+1)(p+q), \ldots, pq - k(p+q)]$ with $0 \le k \le \left\lfloor \frac{pq}{p+q} \right\rfloor - 1$. Then,*

$$G(S) = \begin{cases} 2(k+1) + \left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{kp}{q} \right\rfloor & \text{if } 1 \le k \le \left\lfloor \frac{pq}{p+q} \right\rfloor - 1 \\ 1 & \text{if } k = 0. \end{cases}$$

Proof. In the third proof of Theorem 2.1.1 we defined P as the lattice polygon with vertices $(q-1, -1), (-1, p-1), (q, 0)$ and $(0, p)$ and proved that line $px + qy = pq - p - q + i$ contains exactly one point in $I(P)$ for each $i = 1, \ldots, p+q-1$.

Let k^* be the largest integer such that $pq - k^*(p+q) \ge 0$. Let r_k (resp. r'_k) be the intersection of line $px + qy = pq - k(p-q)$ with the x-axis (resp. with the y-axis) for each $k = 0, \ldots, k^*$. Let Q_k (resp. Q'_k), $k = 0, \ldots, k^* - 1$ be the (not necessarily lattice) polygon formed by the points $(r_k, 0), (r_{k+1}, 0), (q-k, -k)$ and $(q-(k+1), -(k+1))$ (resp. formed by the points $(0, r'_k), (0, r'_{k+1}), (-k, p-k)$ and $(-(k+1), p-(k+1))$). By applying the same arguments as the claim proved in the third proof of Theorem 2.1.1, we have that the number of gaps of S in the interval $[pq - (k+1)(p+q), \ldots, pq - k(p+q)]$ is given by $I(Q_k) + I(Q'_k)$ for each $k = 0, \ldots, k^* - 1$. So, we calculate $I(Q_k)$ and $I(Q'_k)$ for each $k = 1, \ldots, k^* - 1$ (note that $I(Q_0) = I(Q'_0) = 0$). To this end, we first observe that the number of integers points lying on the interval $[(\lceil r_k \rceil, 0), \ldots, (q, 0)[= [(q - k - \lfloor \frac{kq}{p} \rfloor, 0), \ldots, (q, 0)[$ (resp. lying on the interval $[(0, p), \ldots, (0, \lceil r'_k \rceil)[= [(0, p), \ldots, (0, p - k - \lfloor \frac{kp}{q} \rfloor)[$) is equal to $k + \left\lfloor \frac{kq}{p} \right\rfloor$ (resp. equal to $k + \left\lfloor \frac{kp}{q} \right\rfloor$). Now, if for each $k = 0, \ldots, k^* - 1$ we denote by Δ_k and Δ'_k the number of integers points lying on the intervals $[(r_{k+1}, 0), \ldots, (r_k, 0)[$ and $[(0, r'_{k+1}), \ldots, (0, r'_k)[$ respectively, then for each $k = 0, \ldots, k^* - 1$

$$\begin{aligned} I(Q_k) &= \sum_{i=0}^{k-1} \Delta_i = \sum_{i=0}^{k-1} (i+1) + \left\lfloor \frac{(i+1)q}{p} \right\rfloor - i - \left\lfloor \frac{iq}{p} \right\rfloor \\ &= \sum_{i=0}^{k-1} 1 + \left\lfloor \frac{(i+1)q}{p} \right\rfloor - \left\lfloor \frac{iq}{p} \right\rfloor = k + \left\lfloor \frac{kq}{p} \right\rfloor . \end{aligned}$$

Similarly, $I(Q'_k) = k + \left\lfloor \frac{kp}{q} \right\rfloor$, $k = 1, \ldots, k^* - 1$ and the result follows.

□

7.1.1 Telescopic semigroups

Let $d_i = (s_1, \ldots, s_i)$ and set $A_i = \{s_1/d_1, \ldots, s_i/d_i\}$ for each $i = 1, \ldots, n$. Let S_i be the semigroup generated by A_i. The sequence $\{s_1, \ldots, s_n\}$ is called *telescopic* if $s_i/d_i \in S_{i-1}$ for $i = 2, \ldots, n$. We call a semigroup *telescopic* if it is generated by a telescopic sequence.

Remark 7.1.4 *If $\{s_1, \ldots, s_n\}$ is telescopic then $(s_1/d_1, \ldots, s_i/d_i) = 1$ and the sequence $\{s_1/d_1, \ldots, s_i/d_i\}$ is telescopic for $i = 2, \ldots, n$. If $d_i = 1$ for a telescopic sequence $\{s_1, \ldots, s_n\}$, then $\{s_1, \ldots, s_i\}$ is also telescopic and generates the same semigroup.*

Example 7.1.5 Semigroups generated by two elements are telescopic. The sequence $\{4, 6, 5\}$ is telescopic since $d_2 = 2$ and 5 is an element of the group generated by 4/2 and 6/2. The sequence $\{4, 5, 6\}$ is not telescopic.

Lemma 7.1.6 *[240] If $\{s_1, \ldots, s_n\}$ is telescopic and $M \in S_n$ then there exists uniquely determined non-negative integers $0 \le x_i < d_{i-1}/d_i$ for $i = 2, \ldots, n$ such that*

$$M = \sum_{i=1}^{n} x_i s_i.$$

Proof. It follows by induction on n and by using Remark 7.1.4. □

The following lemma shows that telescopic semigroups are symmetric.

Lemma 7.1.7 *[240] For a semigroup generated by the telescopic sequence $\{s_1, \ldots, s_n\}$ we have*

$$l_{N(S)}(S_n) = d_{n-1} l_{N(S)}(S_{n-1}) + (d_{n-1} - 1)s_n = \sum_{i=1}^{n} \left(\frac{d_{i-1}}{d_i} - 1 \right) s_i, \quad (7.2)$$

and

$$N(S_n) = d_{n-1} N(S_{n-1}) + (d_{n-1} - 1)(s_n - 1)/2 = \frac{l_{N(S)}(S_n) + 1}{2}, \quad (7.3)$$

where $d_0 = 0$.

Proof. Since $(s_n, d_{n-1}) = 1$ then every integer $m \in \mathbb{N}$ can be uniquely represented as $m = v s_n + w d_{n-1}$ with $0 \le v \le d_{n-1}$ (w may be negative). By Lemma 7.1.6 the gaps of S_n are exactly the numbers m, where the corresponding w is either a gap of S_{n-1} or w is negative. Thus, the first equality in (7.2) follows. The second equality follows by induction on n.

We shall now prove the first equality of (7.3) (the second equality follows by induction on n). For every value of $0 \leq v < d_{n-1}$ we get $N(S_{n-1})$ gaps of S_n from those of S_{n-1}. Moreover, integers of the form $m = vs_n + wd_{n-1}$ where $w < 0$ are also gaps in S_n. But these gaps are exactly the gaps of the semigroup $< s_n, d_{n-1} >$ that, by Theorem 2.1.1, there are $(d_{n-1}-1)(s_n-1)/2$. Thus the total number of gaps in S_n is

$$d_{n-1}N(S_{n-1}) + (d_{n-1}-1)(s_n-1)/2.$$

□

It is not true that symmetric semigroups need to be telescopic. For instance, consider the semigroup $\bar{S}$ generated by $\{g, g+1, \ldots, 2g-2\}$. Then, it is clear that $1, 2, \ldots, g-1$ and $2g-1$ are the gaps of $\bar{S}$. Thus, $\bar{S}$ has g gaps and the largest gap is $2g-1$, so $\bar{S}$ is symmetric. It can be shown by induction that $\bar{S}$ is not telescopic. Semigroups with the property mentioned in Lemma 7.1.6 are called 'semi-groupe libre'(*free semigroups*) by Bertin and Carbonne in [41, 42]. In these papers it is proved that a sequence is telescopic if and only if it is free if and only if the formula for the largest gap in Lemma 7.1.7 holds.

7.1.2 Hyperelliptic semigroups

A semigroup $S =< s_1, \ldots, s_n >$ with $s_1 < \cdots < s_n$ is called *hyperelliptic* if $s_1 = \rho_2(S) = 2$. Oliveira [317] gave a characterization of hyperelliptic and non-hyperelliptic semigroups with respect to gaps. The corresponding characterization in terms of non-gaps was obtained by Buchwitz [78].

Theorem 7.1.8 *[317] Let $S =< s_1, \ldots, s_n >$ with $s_1 < \cdots < s_n$ be a semigroup with genus $N(S)$. Then,*

(i) S is hyperelliptic if and only if $l_i = 2i-1$ for each $i = 2, \ldots, N(S)$.

(ii) S is nonhyperelliptic if and only if $l_i \leq 2i-2$ for each $i = 2, \ldots, N(S)-1$ and $l_{N(S)} \leq 2N(S)-1$ (here we assume that $\rho_2 \geq 3$ since the case $\rho_2 = 1$ is irrelevant).

Sketch of the proof. (i) If S is hyperelliptic then all even positive integers belongs to S and thus all gaps are odd integers. Now, let i be the smallest integer such that s_i is odd (there is at least one since $(s_1, \ldots, s_n) = 1$). Since $g(S) = g(2, s_i) = 2s_i - s_i - 2 = s_i - 2$ then $N(S) = \frac{s_i-2+1}{2}$ (*i.e.* all odd integers smaller than or equal to $s_i - 2$). For the converse, if all gaps are odd integers then any positive even integer belongs to S, in particular $2 \in S$.

(*ii*) This part follows from the following observation: Let j be an integer where $2 \leq j \leq N(S)$. Notice that at least one of the integers in the pair $\{r, l_r - r\}$ with $1 \leq r \leq \lfloor l_j/2 \rfloor$ is a gap of S (otherwise, if both were non-gaps then $r + l_j - r = l_j$ would be a non-gap, which is a contradiction). Thus, we have $\lfloor l_j/2 \rfloor \leq j - 1$ (since l_j is the j-th gap) that is, $l_j \leq 2j - 1$. □

The following result shows the importance of studying the sum of gaps in semigroups.

Theorem 7.1.9 *[317] If S is a non-hyperelliptic semigroup then each integer $2 \leq r \leq 2N(S)$ is the sum of two gaps of S with the exception only of $l_{N(S)}$ if S is symmetric.*

Proof. Let $r \geq 2$ be an integer such that r is not the sum of two gaps of S. Then, at least one of the integers in the pair $\{i, r - i\}$ with $1 \leq i \leq \lfloor r/2 \rfloor$ is a non-gap of S (otherwise, if both were gaps then $r = i + r - i$ would be a sum of two gaps), therefore the number of non-gaps between 1 and $r - 1$ is at least $\lfloor r/2 \rfloor$. Thus, if $N'(r)$ denotes the number of gaps smaller then r we have $N'(r) \leq r - 1 - \lfloor r/2 \rfloor$, so $2N'(r) + 1 \leq r$. Since $r \leq 2N(S)$ then $N'(r) < N(S)$ and

$$2N'(r) + 1 \leq r \leq l_{N'(r)+1}. \tag{7.4}$$

We claim that $N'(r) + 1 = N(S)$. Indeed, if $N'(r) + 1 < N(S)$ then by Theorem 7.1.9 part (*ii*) and by eqn (7.4) we have

$$2N'(r) + 1 \leq r \leq l_{N'(r)+1} \leq 2(N'(r) + 1) - 2 = 2N'(r), \tag{7.5}$$

which is a contradiction. So, if $N'(r) + 1 = N(S)$ then again by Theorem 7.1.9 part (*ii*) we have that $r \leq l_{N(S)} \leq 2N(S) - 1$ and by the the left-hand inequality of (7.4) we have $r \geq 2N'(r) + 1 = 2$ $(N(S) - 1) + 1 = 2N(S) - 1$. Thus, $r = 2N(S) - 1 = l_{N(S)}$ Therefore, if r is an integer that is not the sum of two gaps of S we obtain that r must be $l_N(S) = g(S)$. □

7.2 Symmetric semigroups

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$. Notice that S and g_S are disjoint sets (otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$, which is a contradiction). A semigroup S is called *symmetric*[2] if $S \cup g_S = \mathbb{Z}$.

[2] Herzog [192] called these semigroups ‘Sylvester-semigroups’.

The interest in symmetric numerical semigroups started from their role in the classification of *plane algebraic branches* (see Section 7.2.2). Later, the result of Herzog [191] that

> *a* monomial curve[3] *is* ideal theoretically a complete intersection *if and only if its associated semigroup is symmetric*

together with a result by Bresinsky [62] that

> *a monomial curve in the affine space* A^4 *is set theoretically complete intersection if its associated semigroup is symmetric*

along with the appealing theorem of Herzog and Kunz [193] (see also [256]) that

> *a* Noetherian local ring *of dimension one and analiytically irrreducible is a Gorenstein ring if and only if its associates value semigroup is symmetric*

have certainly contributed to increase even more the interest in symmetric semigroups.

For a semigroup S, let $T_S = \{z \in \mathbb{Z} \setminus S | z + s \in S$ for every positive $s \in S\}$. The number of elements in T_S is called the *type* of S.

Proposition 7.2.1

$$T_S \cap g_S = \{g(S)\}.$$

Proof. It is clear that $g(S)$ belong to g_S and T_S. Suppose that there exists $x = g(S) - s \in g_S$ with $s > 0$, then $x + s = g(S) \notin S$ and thus $x \notin T_S$. □

A first characterization of symmetric groups was given by Kunz [256] (*cf.* Theorem 5.2.6)

Theorem 7.2.2 *[256]* $T_S = g(S)$ *if and only if* S *is symmetric.*

Proof. Suppose that S is symmetric and assume that $x \in T_S$ with $x \leq g(S)$. Then, $0 < g(S) - x \in S$ and $x + (g(S) - x) = g(S)$ is in S, which is a contradiction, So, $x = g(S)$.

[3] Let $a_1, \ldots, a_n$ be relatively prime positive integers. A *monomial curve* Γ in the affine space A^n_k over a field k is given parametrically by

$$x_i = t^{a_i}$$

that is, we have

$$\Gamma = \{(t^{a_1}, \ldots, t^{a_n}) \in A^n_k | t \in k\}.$$

Now, assume that $T_S = g(S)$. Let $z \in S$, $z > 0$, we must show that $g(S) - z \in S$. Suppose the contrary, $g(S) - z \notin S$ and assume that z is the least positive integer such that $g(S) - z \notin S$. Since $g(S) - z \neq g(S)$ then, there exists $s \in S$, $s \neq z$ such that $(g(S) - z) + s \notin S$ (otherwise, $g(S) - z \in T_S$, which is not possible since $T_S = g(S)$). Thus, it must be the case that $z - s > 0$ (if not, then $g(S) - z + s = g(S) + r$ with $r > 0$ and then $g(S) + r \in S$ by definition of $g(S)$) that contradicts the choice of z. □

Thus, by Theorem 7.2.2 and Sylvester's result (*cf.* Theorem 2.1.1) any semigroup $S =< p, q >$ is symmetric in the interval $[0, \dots, pq - p - q]$. Frőberg *et al.* [149] gave alternative descriptions of the concept of symmetry in semigroups.

Lemma 7.2.3 *[149] The following conditions are equivalent for a semigroup $S =< s_1, \dots, s_n >$.*

(i) *S is symmetric.*

(ii) *For each $z \in \mathbb{Z}$ we have that either $z \in S$ or $g(S) - z \in S$.*

(iii) *If $x + y = g(S)$ then exactly one of x and y belongs to S.*

(iv) *There is $a \notin S$ such that $x + y = a$ implies that exactly one of x and y belongs to S.*

(v) *Among the numbers $0, 1, \dots, g(S)$ there are just as many elements in S as there are elements outside S.*

Proof. Since S and g_S are always disjoint then (ii) and (iii) are just reformulations of (i). Clearly (ii) implies (iv) and since non-negative numbers belong to S then we must have that a is the largest number not belonging to S and hence (iv) implies (ii). Finally, since condition (iii) is always true for $z < 0$ then we have that (iii) is equivalent to (v). □

Notice that Lemma 7.2.3 part (v) shows that $g(S)$ must be an odd number if S is symmetric. One may also study S when $g(S)$ is even (and thus S not symmetric). Let $S_r = \{S | S$ be a semigroup with $g(S) = r\}$. S_r is partially ordered under set-theoretic inclusion. It is easy to see, by *Zorn's Lemma*[4], that S_r has at least one maximal element. Lemma 7.2.3 can be reformulated as follows.

[4] *Zorn's Lemma* states that every non-empty inductive system possesses at least one maximal element. If the reader has not encountered Zorn's Lemma before, it is suggested to be treated as an axiom. It is in fact, equivalent to be the *Well Ordering Principle*.

Lemma 7.2.4 *[149] Let $r \in \mathbb{N}$ be odd. Then, for any semigroup $S \in S_r$, the following are equivalent:*

(i) *S is symmetric.*

(ii) *The map*

$$S \cap \{0, 1, \ldots, r\} \rightarrow (\mathbb{N} \setminus S) \cap \{0, 1, \ldots, r\}$$
$$s \rightarrow r - s$$

is a bijection.

(iii) $|S \cap \{0, 1, \ldots, r\}| = (r + 1)/2$.

(iv) $T_S = \{r\}$.

(v) *S is maximal in S_r.*

The proof for the equivalence between $(i), (ii), (iii)$ and (iv) are just as in Lemma 7.2.3 so we may just prove the equivalence between condition (ii) and condition (v). To this end, we need the following proposition.

Proposition 7.2.5 *Let $H_S = \{z \in \mathbb{Z} | z \notin S$ and $g(S) - z \notin S\}$. Then,*

(i) $T_S \setminus H_S = \{g(S)\}$.

(ii) *Let h_S be the largest element of H_S. Then, h_S is the second largest element of T_S.*

(iii) $2h_S \geq g(S)$.

Proof. (i) It is clear that $g(S) \in T_S \setminus H_S$ (by the definitions of T_S and H_S). Let $\rho \in T_S \setminus \{g(S)\}$ and suppose $g(S) - \rho \in S$. Then, $g(S) - \rho = s$ for some $s \in S$, $s > 0$ and so $g(S) = \rho + s \in S$, which is impossible. Therefore, $g(S) - \rho \notin S$; hence $\rho \in H_S$ and so $T_S \setminus H_S = \{g(S)\}$.

(ii) Assume that $h_S + s \notin S$ for some $s \in S$, $s > 0$. By the maximality of h_s, we have that $h_S + s \notin H_S$ and thus $g(S) - (h_S + s) \in S$. We rewrite the latter as $g(S) - h_S - s = t$ for some $t \in S$. Therefore, $g(S) - h_S \in S$ that is contradictory to the fact that $h_S \in H_S$. So, $h_S + s \in S$ for all $s \in S$, $s > 0$ implying that $h_S \in T_S$. Finally, from (i) we can see that there are no elements in T_S strictly between h_S and $g(S)$.

(iii) This part follows by observing that if $h \in H_S$ then $g(S) - h \in H_S$ and that either h_S or $g(S) - h_S$ is greater than or equal to $g(S)/2$ (since their sum is $g(S)$). □

Proof of the equivalence between (ii) **and** (v) **of Lemma 7.2.4.** If S is symmetric and $a \notin S$ then we have that $a = g(S) - s$ for some $s \in S$. Thus, $g(S) = a + s \in < S, a >$ so $g(S, a) < g(S)$ and hence S is maximal in S_r. Now, suppose that (ii) does not hold then we claim that $g(S) \notin < S, h_S >$. Indeed, if $g(S) = s + nh_S$ for some $s \in S$ and some $n \in \mathbb{N}$ we must have, by Proposition 7.2.5 (iii) that $n = 1$ and thus $h_S = g(S) - s$, which is impossible by definition of H_S. Thus $g(S, h_S) = g(S)$ and S is not maximal in S_r. □

The following lemma gives some (analogous) information of S when the conductor of S is even.

Lemma 7.2.6 *[149] Let $r \in \mathbb{N}$ be even. Then, for any semigroup $S \in S_r$, the following are equivalent:*

(i) $S \cup g_S = \mathbb{Z} \setminus \{r/2\}$,

(ii) The map

$$S \cap \{0, 1, \ldots, r-1\} \to (\mathbb{N} \setminus S) \cap \{0, 1, \ldots, r-1\}$$
$$s \to r - s$$

is a bijection.

(iii) For each $z \in \mathbb{Z}$ we have either $z \in S$ or $z \in g_S$ or $z = r/2$.

(iv) $T_S = \{r/2, r\}$.

(v) S is maximal in S_r.

Proof of Lemma 7.2.6. Condition (iii) is just a reformulation of condition (i) and their equivalence to condition (ii) follows as in Lemma 7.2.3. We show the equivalence between (i) and (iv). Suppose tha (i) holds. Since $T_S \cap g_S = \{g(S) = r\}$ and $T_S \cap S = \emptyset$ then $T_S \subseteq \{r/2, r\}$. But S is not symmetric (since $r = g(S)$ is even) then $T_S = \{r/2, r\}$ implying condition (iv). Now, suppose that (iv) holds then, by Proposition 7.2.5 (ii), h_S is the second largest element in T_S (and thus $n_S = r/2$) and also h_S is the largest element such that $h_S \in H_S$ and thus, by definition of H_S, $g(S) - h_S = r - \frac{r}{2} = \frac{r}{2} \notin S$. Thus condition (iv) implies condition (i).

We now prove the equivalence between (iv) and (v). Suppose that $T_S = \{r/2, r\}$. If $a \notin S$ then we have either $a \in r - s$ for some $s \in S$ or $a = r/2$. In both cases we have that $r \in < S, a >$ and thus $g(S, a) < g(S) = r$ implying the maximality of S in S_r. The other direction follows by using the same argument as in the proof of the equivalence between (ii) and (v) of Lemma 7.2.4. □

A numerical semigroup satisfying conditions of Lemma 7.2.6 is called *pseudo-symmetric*. A simple example of a pseudo-symmetric semigroup is given by $< 3, 4, 5 >$.

Frőberg, *et al.* [149] used Lemmas 7.2.4 and 7.2.6 not only to give an answer to the extending bases problem (see Section 3.5) but also to show that the number of symmetric semigroups grows exponentially with $g(S)$.

Proposition 7.2.7 *[149] Let r be a fixed odd number. The number of symmetric semigroups S with $g(S) = r$ is at least $2^{\lfloor \frac{r}{8} \rfloor}$.*

Proof. Let $T =< g(S)+1, \ldots, 2g(S)+1 >$. It is clear that $g(T) = g(S)$. We extend T to a semigroup T_1 by adding an even number of generators form the set $E = \left\{ \left\lfloor \frac{g(S)}{4} \right\rfloor + 1, \ldots, \left\lfloor \frac{g(S)}{2} \right\rfloor \right\}$. If T_1 is not symmetric then we set $T_2 =< T_1, h_{T_1} >$ and check if T_2 is symmetric, if not then we set $T_3 =< T_2, h_{T_2} >$ and so on. It is clear that we eventually reach a symmetric semigroup (by Lemmas 7.2.4 (v) and 7.2.6 (v)). The result follows since there are at least $2^{\lfloor \frac{r}{8} \rfloor}$ ways to choose an even number of generators from the set E each yielding different semigroups such that $g(T_i)$ remains the same throughout the process. □

Backelin [21] improved this proposition in some cases.

Theorem 7.2.8 *[21] Let $S_r = \{S | S$ is a semigroup with $g(S) = r\}$. Then,*

$$0 < \liminf_{r \to \infty} 2^{-r/2} |\mathcal{S}_r| < \limsup_{r \to \infty} 2^{-r/2} |\mathcal{S}_r| < \infty.$$

Moreover,

$$2^{\lfloor (r-1)/2 \rfloor} \leq |\mathcal{S}_r| \leq 42^{\lfloor (r-1)/2 \rfloor}$$

for all positive integers r.

The proof of Theorem 7.2.8 is based in an upper bound of $K(n, q) = |\{X \subseteq \{1, \ldots, n\} : |2X| \leq q\}|$, where $2X$ denotes $X + X = \{a + b | a, b \in X\}$ and n, q are positive integers.

In [149], Frőberg *et al.* established an easy criteria for deciding whether a semigroup with three elements is symmetric.

Let $S =< s_1, \ldots, s_n >$ and let $d_i = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{s_1 / \prod_{j \neq 1} d_j, \ldots, s_n / \prod_{j \neq n} d_j\}$.

Theorem 7.2.9 *[149] $S =< s_1, s_2, s_3 >$ is symmetric if and only if its derived semigroup is generated by two elements.*

Instead of proving Theorem 7.2.9 (that requires a number of technical lemmas), we rather expose an algorithm that uses Theorem 7.2.9, for detecting symmetry on semigroups on three elements.

```
Frőberg, Gottlieb and Hăggkvist Algorithm

Determine the derived semigroup of $S$, say $< \bar{s}_1, \bar{s}_2, \bar{s}_3 >$
(suppose that $\bar{s}_3$ is the largest of these three elements)
If $\bar{s}_3 > \bar{s}_1\bar{s}_2 - \bar{s}_1 - \bar{s}_2$ Then $S$ is symmetric
Else
    If $\bar{s}_1$ divides $\bar{s}_3 - i\bar{s}_2$ for some $i = 1, \ldots, \left\lfloor \frac{\bar{s}_3}{\bar{s}_2} \right\rfloor$ Then $S$ is symmetric
    Else $S$ is not symmetric.
```

Delorme [106] found a recursive characterization for symmetric semigroups.

Theorem 7.2.10 *[106] Let $S =< s_1, \ldots, s_n >$ and $S' =< s'_1, \ldots, s'_n >$ and let s and s' be positive integers such that $s \in S$, $s' \in S'$ and $(s, s') = 1$. Let $T =< s'S + sS' >= \{t | t = ss_0 + s's'_0,\ s_0 \in S,\ s'_0 \in S'\}$. Then,*

(i) $g(T) = s'g(S) + sg(S') + ss'$.

(ii) T is symmetric if and only if S and S' are symmetric.

Proof. (i) Since $g(s, s') = ss' - s - s'$ is the conductor of $s\mathbb{N} + s'\mathbb{N}$ then

$$s'g(S) + sg(S') + ss' + \mathbb{N} \subset s'g(S) + s'\mathbb{N} + sg(S') + s\mathbb{N} \subset s'S + sS'.$$

Now, suppose that $s'g(S) + sg(S') + ss' \in T$. Hence,

$$s'b + sb' = s'g(S) + sg(S') + ss', \tag{7.6}$$

with $b \in S$ and $b' \in S'$. By taking equality (7.6) modulo s and s', we obtain the following equalities

$$b = g(S) + su \text{ and } b' = g(S') + s'u', \tag{7.7}$$

where u and u' are integers. By combining eqns (7.6) and (7.7) we have that $u + u' = 1$. Moreover, $u, v \neq 0$, otherwise $b = g(S)$ (respectively $b' = g(S')$), which is impossible since $b \in S$ and $g(S) \notin S$ (respectively, $b' \in S'$ and $g(S') \notin S'$).

(ii) Suppose that S and S' are symmetric. Let $us' + u's \notin T$. By modifying the decompostion of $us' + u's$, we can actually assume that

$u \notin S$ and $u + s' \in S$. Thus, $u' - s\ {}_{i}/nS'$ (otherwise, if $u' - s \in S'$ then $us' + u's = s'(u + s') + s(u' - s) \in T$ contradicting the choice of $us' + u's$) and, by part (i), we have

$$\begin{aligned} g(T) - (us' + u's) = s'g(S) + sg(S') + ss' - (us' + u's) = s'(g(S) - u) \\ + s(g(S') + s' - u'), \end{aligned}$$

but $s'(g(S) - u) + s(g(S') + s' - u') \in T$ since $g(S) - u \in S$ (as S is symmetric) and $g(S') + s - u' \in S'$ (as S' is symmetric). So, T is symmetric. □

7.2.1 Intersection of semigroups

A numerical semigroup S is called *irreducible* if it cannot be expressed as an intersection of two numerical semigroups properly containing it; see [366] for results on irreducibility. From [149], it can be deduced that the set of irreducible numerical semigroups with odd (even) Frobenius number coincides with the set of symmetric (pseudo-symmetric) numerical semigroups. Hence, every numerical semigroup can be expressed as an intersection of numerical semigroups that are either symmetric or pseudo-symmetric. In [365], Rosales and Branco characterize those numerical semigroups that can be expressed as a finite intersection of symmetric numerical semigroups.

Theorem 7.2.11 *[365] Let S be a semigroup. Then, S can be expressed as a finite intersection of symmetric semigroups if and only if for every even positive integer $x \notin S$, there exists an odd positive integer y such that $x + y \notin < S, y >$.*

In fact, they improved the above theorem for *pseudo-Frobenius* numbers. Let S be a semigroup. An element $x \in S$ is called a *pseudo-Frobenius* number of S if $x \notin S$ but $x + s \in S$ for all $s \in S \setminus \{0\}$, that is, $x \in T_S$.

Theorem 7.2.12 *[365] Let S be a semigroup and let $g_1, \ldots, g_t$ be its pseudo-Frobenius numbers. Then, S can be expressed as a finite intersection of symmetric semigroups if and only if for all g_i even, there exists an odd positive integer y_i such that $g_i + y_i \notin < S, y_i >$.*

We close this section by proving a nice characterization of symmetry for a special sequence due to Estrada and López [135] generalizing a result due to Juan [222].

Theorem 7.2.13 *[135] Let $S =< s, hs+d, hs+2d, \ldots, hs+kd >$ with $(s, d) = 1$ and $k \leq s-1$. Then, S is symmetric if and only if either $k = 1$ or $k \geq 2$ and $s \equiv 2 \bmod k$.*

Proof. From Theorems 3.3.4 and 5.4.15 we have that

$$g(s, hs+d, hs+2d, \ldots, hs+kd) = hs \left\lfloor \frac{s-2}{k} \right\rfloor + s(h-1) + d(s-1),$$

and

$$N(s, hs+d, hs+2d, \ldots, hs+kd) = \frac{(s-1)(hq+d+h-1+hr(q+1))}{2},$$

where $s - 1 = qk + r$ with $0 \leq r < k$, respectively. Now, by Lemma 7.2.3 part (v), S is symmetric if and only if

$$N(s, hs+d, hs+2d, \ldots, hs+kd) = \frac{g(s, hs+d, hs+2d, \ldots, hs+kd)+1}{2}.$$

In this case such a condition is equivalent to

$$\left\lfloor \frac{s-2}{k} \right\rfloor = sq - q - 1 + rq + r. \tag{7.8}$$

We have two cases.

Case a) If $r = 0$ then $\lfloor \frac{s-2}{k} \rfloor = q - 1$ so condition (7.8) means that $q - 1 = sq - q - 1$ if and only if $2q = sq$ that is, $s = 2$ implying that $k = 1$.

Case b) If $r \neq 0$ then $\lfloor \frac{s-2}{k} \rfloor = q$ so condition (7.8) is the same as

$$\begin{aligned} q &= sq - q - 1 + rq + r \\ &= sq - q - 1 + r(q+1) \\ &= sq + (q+1)(r-1). \end{aligned}$$

So, $q(s-1) = (q+1)(r-1)$ implying that $q|(r-1)$ but since $r < q$ then $r = 1$. Thus, $s - 1 = qk + 1$ implying that $s \equiv 2 \bmod k$ with $k \geq 2$. □

7.2.2 Apéry sets

The *Apéry set* of element n, $n \in S \setminus \{0\}$ is defined as $Ap(S, n) = \{s \in S | s - n \notin S\}$.

Proposition 7.2.14 *The set $Ap(S, n)$ is a complete system modulo n.*

Proof. Let $w(i) = \min\{s \in S | s \equiv i \bmod n\}$ for every $i = 0, \ldots, n-1$. The element $w(i)$ exists since for every $n \in \mathbb{N}$, $n > g(S)$, we have that

$n \in S$ that implies that the set $\{s \in S | s \equiv i \bmod n\}$ is not empty. It is easy to check that

$$Ap(S, n) = \{w(0), \ldots, w(n-1)\}.$$

□

From the above proposition we have that $|Ap(S, n)| = n$. Moreover,

Proposition 7.2.15

$$g(S) = \max\{Ap(S, n)\} - n.$$

Proof. Let $n \in S \setminus \{0\}$. By definition, $\max\{Ap(S, n)\} - n \notin S$. Let $s \in \mathbb{N}$ be an element greater than $\max\{Ap(S, n)\} - n$ and suppose that $w \in Ap(S, n)$ is such that $s \equiv w \bmod n$. Since, $s + n > \max\{Ap(S, n)\}$ then $s + n > w$ and thus $s + n = w + qn$ for some $q \in \mathbb{N} \setminus \{0\}$. Hence, $s = w + (q-1)n \in S$. □

Apéry [13] showed the following result.

Lemma 7.2.16 *[13] Let $n \in S \setminus \{0\}$ and $0 = w(0) < w(1) < \cdots < w(n-1)$ the smallest elements of S in the respective congruence class modulo n. Then, S is symmetric if and only if $w(i) + w(n-(i+1)) = w(n-1)$ for all $i \in \{0, \ldots, n-1\}$.*

Proof. By Proposition 7.2.15 that $g(S) = w(n-1) - n$. Now, suppose S is symmetric then there exists a permutation $j_0, \ldots, j_{n-1}$ of the set $\{0, \ldots, n-1\}$ such that $w(i) + w(j_i) = g(S) + n = w(n-1)$ and since $w(i) < w(i+1)$ then $j_i = n - (i+1)$. Contrarily, suppose that $w(i) + w(n-(i+1)) = w(n-1)$ for all $i \in \{1, \ldots, n\}$. Then for any two integers a and b such that $a + b = w(n-1) - n = g(S)$ we must have that $a = w(i) + \lambda n$ and $b = w(n-(i+1)) + \lambda' n$ with $\lambda, \lambda' \in \mathbb{N}$ and $\lambda + \lambda' = -1$. Then, necesarily either $\lambda < 0$ or $\lambda' < 0$ and the result follows since clearly every integer g is of the form $w(i) + \lambda n$ where $\lambda \geq 0$ if $g \in S$ ($\lambda < 0$ otherwise). □

7.3 Related concepts

7.3.1 Type sequences

In [24, 25], Barucci *et al.* remarked that, although symmetric semigroups are characterized by having type less than or equal to one (*cf.* Lemma 7.2.4), the pseudo-symmetric semigroups are only one particular kind of semigroups having type two. For instance, the semigroup $S =< 3, 10, 11 >$ is of type two (since $T_S = \{7, 8\}$) but it is not pseudo-symmetric (since $g(S)/2 = 4 \neq 3 = \{3, 10, 11\} \cap \{0, 1, \ldots, 8\}$). Barucci *et al.* sharpened the notion of type in order to characterize the maximal elements of the set S_r.

Let $S = \{0 = s_0, s_1, \ldots, s_n = g(S)-1, \rightarrow\}$ be a numerical semigroup where $s_i < s_{i+1}$, $n = n(S) = |S \cap \{0, 1, \ldots, g(S)\}|$ and the arrow means that every integer greater than $g(S) + 1$ belongs to S. Let $S_i = \{x \in S | x \geq s_i\}$ and define $S(i) := (S - S_i) = \{x \in \mathbb{N} | x + S_i \subseteq S\}$. It is obvious that every $S(i)$ is itself a numerical semigroup and that

$$S_n \subset S_{n-1} \subset \cdots \subset S_1 \subset S \subset S(1) \subset \cdots \subset S(n-1) \subset S(n) = \mathbb{N}.$$

The number $t_S := |S(1) \setminus S|$ is the type of S. Likewise, it is defined $t_i(S) := |S(i) \setminus S(i-1)|$, $i \geq 1$. Obviously, $t_1(S) = T_S$, but, in general case, $t_i(S) \neq t(S(i))$ (*cf.* [24, Theorem 8]). In this way, it is possible to associate with every numerical semigroup S a numerical sequence $\{t_1, \ldots, t_{n(S)}\}$ that is called the *type sequence* of S. Since $\mathbb{N} \setminus S$ is the disjoint union of the sets $S(i) \setminus S(i-1)$, the integer

$$g(S) + 1 - n(S) = \sum_{i=1}^{n(S)} t_i(S) \tag{7.9}$$

counts the elements in $\mathbb{N} \setminus S$.

Proposition 7.3.1 *[24] Let $S = \{0 = s_0, s_1, \ldots, s_n = g(S) - 1, \rightarrow\}$ be a numerical semigroup, $S \neq \mathbb{N}$. Then, for each $i = 1, \ldots, n(S)$*

(i) $g(S(i)) = g(S) - s_i$,

(ii) $1 \leq t_i(S) \leq t_1(S)$,

(iii) $2n(S) \leq g(S) + 1 \leq n(S)[t(S) + 1]$ *and*

(iv) $t(S) \leq g(S) + 2 - 2n(S)$.

Proof. (i) Since $g(S) = g(S) + s_i - s_i \notin S$ then $g(S) - s_i \notin S(i)$. Moreover, if $x > g(S) - s_i$ then for each $s_i \in S_i$, $x + s_i > g(S)$ and so $x + s \in S$. Hence, $x \in S(i)$ and $g(S(i)) = g(S) - s_i$.

(ii) If $s \in S_i$ then $g(S) - s_{i-1} + s \geq g(S) - s_{i-1} + s_i \geq g(S) + 1$ and thus $g(S) - s_{i-1} \in (S \setminus S_i) = S(i)$ but $g(S) - s_{i-1} \notin S(i-1)$; hence, $1 \leq t_i(S)$. Now, consider the injection

$$\begin{aligned} S(i) \setminus S(i-1) &\rightarrow S(1) \setminus S \\ x &\mapsto x + s_{i-1}. \end{aligned}$$

By definition $s_{i-1} + s \geq s_i$ for each $s \in S \setminus \{0\}$; thus, if $x \in S(i)$ then $x + s_{i-1} + s \in S$ and $x + s_{i-1} \in S(1)$. Therefore, the above injection is an immersion of $S(i) \setminus S(i-1)$ into $S(1) \setminus S$; thus $t_i(S) \leq t_1(S)$.

(iii) and (iv) follow from part (ii) and eqn (7.9). □

Corollary 7.3.2 *[24] Let $r \geq 1$ and let $S \in S_r = \{S | S$ is a semigroup with $g(S) = r\}$. Then, S is maximal in S_r if and only if its type sequence is $(t_1(S), 1, \ldots, 1)$ and $t_1(S) \leq 2$.*

Proof. Suppose that r is odd. Then, by Lemma 7.2.4, S is maximal in S_r if and only if $t(S) = 1$ and, by Propostition 7.3.1 (ii), if and only if the type sequence of S is $(1, \ldots, 1)$. Moreover, by eqn (7.9) if S has type sequence $(2, 1, \ldots, 1)$ then $r = 2n(S)$ is even.

Now, suppose that r is odd. By eqn (7.9), S cannot have type sequence of the form $(1, \ldots, 1)$ and if the type sequence of S is of the form $(2, 1, \ldots, 1)$ then $n(S) = r/2$ and thus, by Lemma 7.2.6 S is maximal in S_r. Conversely, if S is maximal in S_r then $n(S) = r/2$ and $t_1(S) = 2$. Therefore, by eqn (7.9) and Propostition 7.3.1 (ii) the type sequence of S is $(2, \ldots, 1)$. □

Given integers $n \geq 2$ and $f \geq 3$, an interesting problem is to characterize the type sequences arising from S such that $n(S) = n$ and $g(S) = f$. The case $n = 2$ is answered in the following result.

Proposition 7.3.3 *[24] If $n = 2$ and $f \geq 3$ then an ordered pair (t, τ) of natural numbers is the type sequence of some semigroup S such that $n(S) = 2$ and $g(S) = f$ if and only if we have that*

$$1 \leq \tau \leq t, \ \ (f-1)/2 \leq t \leq f-2 \ \textit{and}\ t + \tau = f - 1. \tag{7.10}$$

Proof. If $n(S) = 2$ and $g(S) = f$ then eqn (7.10) follows by eqn (7.9) and Proposition 7.3.1 (ii), (iii) and (iv). Conversely, suppose that (t, τ) verifies eqn (7.10) then there exists a semigroup $S' = \{0, s, f+1, \rightarrow\}$ with type sequence (t, τ) with $2 \leq s \leq f-1$ and $f+1 \leq 2s$. Indeed, any such s implies that $n(S') = 2$ and $g(S') = f$; moreover, $t(S') = s - 1$ (since $T(S') = \{x \in \mathbb{N} \setminus S | f + 1 \leq x + s\}$). By setting $s = t + 1$, we have, by eqns (7.9) and (7.10), that S' has type sequence (t, τ) with $2 \leq s \leq f - 1$ and $f + 1 \leq 2s$. □

7.3.2 Complete intersection

A semigroup $S =< s_1, \ldots, s_n >$ is called *complete intersection* if the cardinality of a minimal presentation plus one equals the cardinality of a minimal system of generators of the given semigroup. Equivalently, S is a *complete intersection* if the semigroup ring $k[S] = k[t^{s_1}, \ldots, t^{s_n}]$

is a complete intersection[5]. Complete intersection semigroups are important because they can be presented by the least possible number of relators.

Delorme [106] found a recursive characterization of complete intersection semigroups.

Theorem 7.3.4 *[106] Let $S =< s_1, \ldots, s_n >$ and $S' =< s'_1, \ldots, s'_n >$ be two semigroups and let s and s' be positive integers such that $s \in S$, $s' \in S'$ and $(s, s') = 1$. Let $T =< sS + s'S' >= \{t | t = ss_0 + s's'_0,\ s_0 \in S,\ s'_0 \in S'\}$. Then, T is a complete intersection if and only if S and S' are a complete intersection.*

Let $S =< s_1, \ldots, s_n >$ and let $d_i = (s_1, \ldots, s_i)$ for $i = 1, \ldots, n$ with $d_n = 1$. In [191], Herzog showed that if (after suitable reordering) S verifies that

$$[d_i, s_{i+1}] \in < s_1, \ldots, s_i > \text{ for } i = 1, \ldots, n-1, \tag{7.11}$$

where $[x, y]$ denotes the least common multiple of integers x and y then S is complete intersection (see Lemma 3.2.3). Further, Herzog proved that condition (7.11) is not only sufficient but also necessary in the case $n = 3$. In [143], Fischer and Shapiro showed that this is not the case in general by considering the semigroup $S' =< 20, 30, 33, 44 >$ (one can check that S' does not satisfy condition (7.11) by observing that no matter how the elements are ordered $[s_1, (s_2, s_3, s_4)]$ is never in $< s_2, s_3, s_4 >$, while S' is complete intersection). However, they showed that condition (7.11) is equivalent to the concept of *principally dominating* for matrices.

7.3.3 The Möbius function

Let P be a finite partially ordered set (or *poset*). The function $\mu : P \times P \longrightarrow \mathbb{Z}$ satisfying

$$\sum_{x \le y \le z} \mu(x, y) = \delta(x, z) \text{ if } x \le z, \tag{7.12}$$

where δ is the *Kronecker delta function*[6] together with ordering property $\mu(x, z) = 0$ if $x \not< z$ is called the *Möbius function* of P. μ exists

[5] If we consider the homomorphism $\Phi_S : k[X_1, \ldots, X_n] \to R[S],\ \Phi(X_i) = t^{s_i}$, S is a complete intersection if and only if $Ker(\Phi_S)$ is generated by $n-1$ elements.

[6] The Kronecker delta function is defined by

$$\delta(x, z) = \begin{cases} 1 & \text{if } x = z \\ 0 & \text{otherwise.} \end{cases}$$

and is uniquely recursively defined. Indeed, let us rewrite eqn (7.12)

$$\mu(x,x) = 1, \tag{7.13}$$

$$\mu(x,z) = -\sum_{x\leq y<z} \mu(x,y) \text{ if } x < z. \tag{7.14}$$

It can be first calculated $\mu(x,z)$ with $z = x$ from eqn (7.13) and then, recursively from eqn (7.14) for successively higher z by induction on the length of the longest chain from x to z. Thus μ depends only on the order structure of the interval $[x,z]$ and not on the rest of P.

Let $S =< s_1, s_2 >$ be the semigroup generated by s_1 and s_2. Notice that S can be given a natural partial order: for $g, h \in S,\ g < h \Leftrightarrow g + k = h$ for some $k \in S$. Deddens [105] determined the Möbius function[7] of S.

Theorem 7.3.5 *[105] Let μ be the Möbius function of the poset $S =< s_1, s_2 >$. Then,*

$$\mu(0,s) = \begin{cases} 1 & \textit{if } s \equiv 0 \textit{ or } s_1 + s_2 \bmod (s_1 s_2 n), \\ -1 & \textit{if } s \equiv s_1 \textit{ or } s_2 \bmod (s_1 s_2), \\ 0 & \textit{otherwise.} \end{cases}$$

Deddens actually calculated $\sum_{j=1}^{\infty}(-1)^j N(j,s)$, where $N(j,s)$ denote the number of (ordered) ways that s can be written as the sum of j non-zero elements of G (not necessarily distinct), that is, $N(j,s)$ is the number of chains of length j of the type $0 = g_0 \not< g_1 \not< \cdots \not< g_j = g$. We have that $\sum_{j=1}^{\infty}(-1)^j N(j,s) = \mu(0,s)$. Székely and Wormald [441] computed the *zeta* and the Möbius functions of $S =< s_1, s_2, s_3 >$. They also showed that a similar result does not extend to the case with $n \geq 4$ generators.

7.4 Supplementary notes

Let $\gamma \geq 0$ be an integer. A semigroup S is called *γ-hyperelliptic* if the following conditions hold: S has γ even elements in the interval $[2, 4\gamma]$ and the $(\gamma + 1)$-th positive element of S is $4\gamma + 2$. The motivation for studying γ-hyperelliptic semigroups comes from the investigations of *Weierstrass* semigroups[8]

[7] It is remarked in [105] that this result originally arose in connection with semigroups of operators on *Hilbert spaces.*

[8] A *Weierstrass semigroup* is a semigroup associated to a point on an algebraic curve (or on a *Riemann surface*) X. This semigroup can give important information about the curve X. We refer the reader to [15, 173, 432] for further details.

In [452], Torres investigated the γ-hyperelliptic semigroups and found some characterizations of such semigroups in terms of the genus and non-gaps and applied them in order to characterize double coverings of curves by means of *weights* of Weierstrass semigroups.

Consider the following interesting question: when a numerical semigroup occurs as a Weierstrass semigroup? In 1976, Buchweitz [77] gave the first example of a numerical semigroup that cannot occur as a Weierstrass semigroup. Buchweitz's proof is based on the fact that if S is a Weierstrass semigroup then $|L_m(S)| \leq (2m-1)(N(S)-1)$, where L_m denotes the set of all sums of m elements of $\mathbb{N} \setminus S$. Buchweitz [77] constructed numerical semigroups S satisfying $|L_m(S)| > (2m-1)(N(S)-1)$ (such semigroups are called *Buchweitz*).

Torres [453] also used his results on Weierstrass semigroups (on γ-hyperelliptic curves) and Buchweitz's examples to give the first examples of symmetric numerical semigroups that cannot occur as Weierstrass semigroups on non-singular curves.

Kraft [253] gave another characterization of symmetric semigroups in terms of the *Euler derivation*; see also [64] for closed related results. In [362], Rosales compared the cardinals of a *minimal relation* of S and $S \cup \{g(S)\}$ obtaining a recurrent method to build the set $S(m)$ of all numerical semigroups with multiplicity m. In [363], Rosales gave an upper bound for the cardinal of a minimal relation of a symmetric semigroup S (which depends on the multiplicity of S) and studied the set of numerical semigroups with given conductor and multiplicity. In [151], García-Sánchez and Rosales studied numerical semigroups generated by intervals and showed that $S = < s, s+1, \ldots, s+x >$ is symmetric if and only if $s \equiv 2 \bmod x$. Notice that this is a special case of Theorem 7.2.13 by taking $y = 1$ and $d = x$. Juan [222] gave a proof of a weaker version of Theorem 7.2.13. The concept of *fundamental gaps* in numerical semigroups and its Frobenius number is investigated in [369]. In [285] Manley, investigated the gaps of semigroups generated by arithmetic progressions.

In [149], Frőberg *et al.* proved that if S is a semigroup of type t with $n(S) < g(S)$ then

$$g(S) + 1 \leq (t+1)n(S). \tag{7.15}$$

In [73], Brown and Curtis, classified all semigroups with $g(S) = (t+1)$ $n(S)$ or $g(S)+1 = (t+1)n(S)$. Kunz [257] considered the classification of numerical semigroups in connection with the study of their invariants coming from the associated semigroup rings (*i.e.* Cohen–Macaulay type, Betti numbers, etc.).

In [363], Rosales studied questions related to Apéry sets and remarked that the characterization of Lemma 7.2.16 shows that there exist only a 'few' symmetric semigroups S fulfilling the condition that the elements of $Ap(S, n)$ have a unique expression. From results due to Rosales and García-Sánchez [153], it can be deduced that if the elements of $Ap(S, n)$ have a unique expression then S is a free semigroup; see also [371] and [370].

A numerical semigroup S is an *Arf numerical semigroup* if for every $x, y, z \in S$ such that $x \geq y \geq z$, we have that $x+y-z \in S$. Barucci *et al.* [25] have characterized the Arf semigroups that are either symmetric or pseudo-symmetric, studied their role in characterizing *Arf* rings[9] and investigated the *Lipman* semigroups[10]; see also [120] and [276]. In [82], Campillo and Marijuan studied complete intersection semigroups via the *Koszul complexes*. Zariski [487, 488] remarked on the importance of the conductor in semigroups in relation to *algebroid branches* and the *Newton–Puiseux* expansions; see also [41] and [42].

In [250], Komeda investigated whether a given numerical semigroup is Buchweitz and in [251] the *Schubert index* associated to numerical semigroups S, that is, the tuple $(l_1 - 1, l_2 - 2, \ldots, l_{N(S)} - N(S))$ where $l_1 < \cdots < l_{N(S)}$ are the gaps of S.

D'Anna [103] deduced some general results, which allowed complete characterization of the type sequences of semigroups S when $n(S)$ is 3 or 4. Moreover, D'Anna obtained upper and lower bounds for the elements of $t_i(S)$ and proved a result that connects the type sequence of S with the *standard bases* of the $S(i)$ (in the sense of [351]). The latter result yields an algorithm for computing the type sequence of a given numerical semigroup.

Delorme's complete intersection characterization (Theorem 7.3.4) generalized some results given by Watanabe [476]. García-Sánchez and Rosales [151] characterized complete intersection semigroups generated by intervals (sequences of consecutive integers).

Apéry used Lemma 7.2.16 to show that the symmetric semigroup $< 6, 7, 8 >$ does not correspond to an *algebroid planar branch*; a complete characterization of this type of symmetric semigroup for planar branches over any algebraically closed ground field K, has been given by Angermüller [9]. For the general case, a very elegant algebraic char-

[9] Arf rings are an important class of rings studied in algebraic geometry and commutative algebra. We refer the reader to [406] for a discussion on Arf rings and their relevance in geometry and also to [25] for the connection between the Arf property of a one-dimensional analytically irreducible domain and the Arf property of its value numerical semigroup; see also [16].

[10] In honour of [276].

acterization was given by Herzog and Kunz [193]. Unfortunately, this does not give an intrinsic characterization of symmetry in terms of generators of Thoma [445] presented a simple technique, based on the gluing concept, for finding *monomial varieties* that are *set theoretic complete intersection*. We refer the reader to [60, 61, 63] for further investigation related to Apéry sets and planar branches.

Theorem 7.3.4 was also proved by Fischer and Shapiro [143]. Their proof depends on a decomposition theorem for *mixed dominating* matrices[11]. García-Sánchez and Rosales [152] characterized simplicial complete intersection affine semigroups, with dimension less than four, by using the concept of *gluing* semigroups; see also the dissertation of Schäfer (1987). In [144], Fischer *et al.* generalized the latter to arbitrary dimensions. In [296], Micale studied monomial semigroups by using the concept of *critical number* (a natural number k is a *critical number* for s_i if $s_i + k \notin < s_1, \ldots, s_n >$).

[11] A matrix is said to be *mixed* if every row contains non-zeros of opposite sign real numbers and is *dominating* if it does not contain a non-empty square mixed submatrix; We refer the reader to [145] for a collection of many interesting properties of mixed dominating matrices.

This page intentionally left blank

8

Applications of the Frobenius number

The knowledge of the Frobenius number turned out to be very useful in many different areas. In this chapter we show a number of applications of **FP**.

8.1 Complexity analysis of the Shell-sort method

Shell-sort is a sorting algorithm proposed by Shell [414] in 1959. Shell-sort leads to a simple and compact sorting program that works well for small files and for files that are partially ordered.

Let us give a brief description of the Shell-sort (for a detailed explanation of the Shell-sort procedure see Appendix B.4). Given an increment sequence $h_1, h_2, \ldots$ a file is sorted by successively h_j*-sorting* it, for j from integer t down to 1. An array $a[1], \ldots, a[N]$ is defined to be h_j*-sorted* if $a[i - h_j] \leq a[i]$ for $i = h_j + 1, \ldots, N$. The method used for h_j-sorting is *insertion sort*: for $i = h_j + 1, \ldots, N$, we sort the sequence $\ldots, a[i - 2h_j], a[i - h_j], a[i]$ by taking advantage of the fact that the sequence $\ldots, a[i - 2h_j], a[i - h_j]$ is already sorted, so $a[i]$ can be inserted by moving larger elements one position to the right in the sequence, then putting $a[i]$ in the place vacated.

Example 8.1.1 The table shows how a sample file is sorted by Shell-sort with increments $h_3 = 7$, $h_2 = 3$ and $h_1 = 1$.

Input file	$3, 2, 7, 9, 8, 1, 1, 5, 2, 6$
7-sorted	$3, 2, 6, 9, 8, 1, 1, 5, 2, 7$
3-sorted	$1, 2, 1, 3, 5, 2, 7, 8, 6, 9$
1-sorted	$1, 1, 2, 2, 3, 5, 6, 7, 8, 9$

Shell-sort sorts properly whenever the increment sequence ends with $h_1 = 1$, but the running time of the algorithm clearly depends on the specific increment sequence used and little is known on how to pick the 'best' increment sequence.

Surprisingly, **FP** is very useful to obtain upper bounds for the running time of this fundamental sorting algorithm. Let $n_d(a_1, \ldots, a_n)$ be the number of multiples of d that cannot be represented as a linear combinations (with non-negative coefficients) of $a_1, \ldots, a_n$ (see Chapter 5 for further details on $n_d(a_1, \ldots, a_n)$ when $d = 1$).

Lemma 8.1.2 *[214] The number of steps required to h_j-sort an array $a[1], \ldots, a[N]$ that is already h_{j+1}-h_{j+2}-$, \ldots ,$-h_t-sorted is*

$$O\left(Nn_{h_j}(h_{j+1}, h_{j+2}, \ldots, h_t)\right).$$

Proof. The number of steps required to insert element $a[i]$ is the number of elements among $a[i - h_j], a[i - 2h_j], \ldots$, which are greater than $a[i]$. Any element $a[i - x]$ with x a linear combination of h_{j+1}, $h_{j+2}, \ldots, h_t$ must be less than $a[i]$ since the file is h_{j+1}-h_{j+2}-$, \ldots ,$-h_t-sorted (recall that if a k-sorted file is h-sorted, it remains k-sorted; see [246]). Thus, an upper bound on the number of steps to insert $a[i]$, for $1 \leq i \leq N$, is the number of multiples of h_j that are not expressible as linear combination of $h_{j+1}, h_{j+2}, \ldots, h_t$ or $n_{h_j}(h_{j+1}, h_{j+2}, \ldots, h_t)$. □

Lemma 8.1.3 *Suppose that $(a_1, \ldots, a_n) = 1$. Then*

$$n_d(a_1, \ldots, a_n) < \frac{g(a_1, \ldots, a_n)}{d}.$$

Proof. Every integer greater than $g(a_1, \ldots, a_n)$ can be represented as a linear combination of $a_1, \ldots, a_n$; in the worst case all multiples of d less than $g(a_1, \ldots, a_n)$ cannot. □

The complexity of Shell-sort is related to the Frobenius number in the following lemma due to Incerpi and Sedgewick [214]; see also [477].

Lemma 8.1.4 *[214] The number of steps required to h_j-sort an array $a[1], \ldots, a[N]$ that is already h_{j+1}-h_{j+2}-$, \ldots ,$-h_t-sorted is*

$$O\left(\frac{Ng(h_{j+1}, h_{j+2}, \ldots, h_t)}{h_j}\right).$$

Proof. The result follows from Lemmas 8.1.2 and 8.1.3. □

Specific bounds are obtained by solving **FP** for particular increment sequences. For example, Theorem 2.1.1 leads directly to an upper bound for h_j-sorting of $O(Nh_j)$ when $h_j = 2^j + 1$ since

$$N^{\frac{g(h_{j+1},h_{j+2},\ldots,h_t)}{h_j}} \le \frac{g(h_{j+1},h_{j+2})}{h_j} = O\left(N^{\frac{h_{j+1},h_{j+2}}{h_j}}\right) = O(Nh_j).$$

The above bound was given by Papernov and Stasevich [323] and was generalized by Pratt [336] to cover a large family of 'almost geometric' increment sequences.

From Lemma 8.1.4, other specific bounds can be obtained by solving **FP** for particular increment sequences. Sedgewick [391] used Selmer's results (*cf.* Theorem 2.3.6) for $n = 3$ to develop increment sequences obtaining a bound of order $O(N^{4/3})$. The increment sequences were rather complicated (of the form $4^{j+1} + 3(2^j) + 1$ and $2(4^j) + 9(2^j) + 9$).

Incerpi and Sedgewick [214] improved $O(N^{4/3})$ to $O(N^{1+\epsilon})$ and further to $O(N^{1+\epsilon/\sqrt{\log N}})$ by using the **FP** approach as well. Their proof of the bound $O(N^{1+\epsilon})$ resulted from a complicated increment sequence. Selmer [393] presented a simpler method to prove the latter, by using a classical result for the Frobenius number due to Brauer (*cf.* Theorem 3.1.2) and by Brauer and Seelbinder (*cf.* Theorem 3.1.4).

8.2 Petri Nets

Petri nets are one of the most sustained techniques to model and analyse non-sequential systems and have successfully been applied in many areas. Indeed, they are frequently used to model systems performing infinite processes like operating systems, real-time control devices, communication protocols or information systems. This model was introduced and studied by Petri [326].

8.2.1 P/T systems

Here, we consider *Place/Transition nets* that, among Petri nets, have become very popular.

A triple $\mathcal{N} = (P, T; F)$ is called a *net* if and only if

(a) $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$,

(b) $F \subseteq (P \times T) \cup (T \times P)$.

A fivetuple $\mathcal{N} = (P, T; F, K, W)$ is a *Place/Transition* net (we write P/T net) if and only if

(a) $(P, T; F)$ is a net where P and T are disjoint sets of *places* and *transitions* with $|P| = n, |T| = m$.

(b) $K : P \longrightarrow \mathbb{N}^+ \cup \{\infty\}$ is a *capacity* function.

(c) $W : F \longrightarrow \mathbb{N}^+$ is a *weight* function.

A P/T net $\mathcal{N}$ is called *pure* if and only if $(p,t) \in F$ then $(t,p) \notin F$ for all $(p,t) \in P \times T$ (*i.e.* $\mathcal{N}$ has no parallel edges forming a directed cycle). A function $M : P \to \mathbb{N}$ is called *marking.* A P/T *system* is a pair $(\mathcal{N}, M_0)$ where $\mathcal{N}$ is a P/T net and M_0 is the *initial* marking.

A transition $t \in T$ is *enabled* at M if and only if

(a) $M(s) \geq W(s,t)$ for all s such that $(s,t) \in F$, and

(b) $K(s) \geq M(s) + W(t,s)$ for all s such that $(t,s) \in F$.

If t is enabled at M then t may *fire*, yielding a new marking M' given by

$$M'(s) = \begin{cases} M(s) - W(s,t) & if\ (s,t) \in F, \\ M(s) - W(t,s) & if\ (t,s) \in F, \\ M(s) & otherwise. \end{cases}$$

We call M' *reachable* from M if and only if there exists a sequence of firings transforming M into M'.

Clearly, a P/T system $\mathcal{N}$ can be seen, and drawn, as weighted directed bipartite graphs where the partition sets are given by P and T and directions of edges are given by the relation F (*i.e.* one direct edge from x to y if and only if $(x,y) \in F$).

An $(\mathcal{N}, M_0)$ system is *live* if there exists an infinite sequence of enabled transitions starting from M_0 (otherwise the $(\mathcal{N}, M_0)$ system is called *dead*). The *liveness* problem (*i.e.* the problem of deciding liveness of a given markings) is one of the main problems studied in Petri nets.

Example 8.2.1 Let $(\mathcal{N}, M_0)$ be the P/T system given by

$$\begin{aligned} P &= \{a,b,c,d,e,f,g\}, \\ T &= \{1,2,3,4\}, \\ F &= \{(a,1),(c,1),(1,b),(1,d),(b,2),(e,2),(2,a),(2,d), \\ &\quad\ (d,3),(f,3),(3,c),(3,g),(d,4),(g,4),(4,e),(4,f)\}, \\ K &: P \to \{\infty\}, \\ W &: F \to \{1\}, \\ M_0 &: P \to \{0,1\} \text{ where } \{a,b,c,g\} \to \{1\} \text{ and } \{d,e,f\} \to \{0\}. \end{aligned}$$

The $(\mathcal{N}, M_0)$ system is represented in Fig. 8.1.

The only enabled transition is $1 \in T$ and the immediate follower marking of M_0 is M', where $M' : P \to \{0,1,2\}$ with $\{b\} \to \{2\}$,

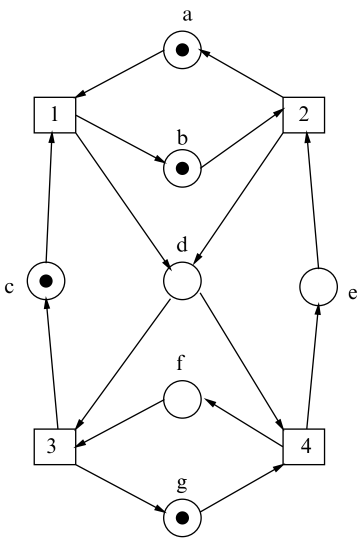

Figure 8.1: $(\mathcal{N}, M_0)$ system.

$\{d, g\} \to \{1\}$ and $\{a, c, e, f\} \to \{0\}$. In turn, under M' the only enabled transition is $4 \in T$ and the immediate follower marking of M' is M'', where $M'' : P \to \{0, 1, 2\}$ with $\{b\} \to \{2\}$, $\{e, f\} \to \{1\}$ and $\{a, c, d, g\} \to \{0\}$. It can be checked that under M'' there is not an enabled transition, and thus this P/T system is dead.

8.2.2 Weighted circuits systems

An $(\mathcal{N}, M_0)$ system is called a *weighted circuit* system[1] (denoted by $\mathcal{C}$) if and only if the bipartite graph associated to $(\mathcal{N}, M_0)$ is an even directed (say, anti-clockwise) circuit with vertex partitions $P = \{p_0, \ldots, p_{n-1}\}$ and $T = \{t_0, \ldots, t_{n-1}\}$ with the relation $F = \{(t_i, p_i) \text{ and } (p_i, t_{i+1})\}$, where $i + 1$ is taken modulo n. Moreover, if we let $W(t_i, p_i) = w_{i,i}$ and $W(p_i, t_{i+1}) = w_{i,i+1}$, where again $i + 1$ is taken modulo n then $C = (c_{i,j})$ denotes the *incidence matrix*, associated to $\mathcal{C}$, where $c_{i,i} = w_{i,i}$, $c_{i,i-1} = -w_{i,i+1}$ and zero otherwise.

We say that $\mathcal{C}$ is *consistent* (resp. *conservative*) if there exists a positive integer T-vector $X = (x_0, \ldots, x_{n-1})$ (resp. P-vector $Y = (y_0, \ldots, y_{n-1})^t$) such that $C \cdot X = \mathbf{0}$ (resp. $Y^t \cdot C = \mathbf{0}^t$). Such vectors

[1] One motivation to study weighted circuits systems is that some problems (like the liveness of T-graphs) can be reduced to the problem of liveness of circuits.

are up to a constant uniquely determined by the matrix C (thus, we may assume that $(x_0, \ldots, x_{n-1}) = 1$ and $(y_0, \ldots, y_{n-1}) = 1$). The least positive X and Y are called *T-invariant* and *P-invariant* (also called the *weight vector*). The *weight* of a marking M is the value of the scalar product $W(M) = Y^t \cdot M$. It is known that during firing transitions the weights of reachable markings are invariant. A marking M' is *potentially reachable* from marking M if and only if the equation $C \cdot \mathbf{z} = M' - M$ has an integer solution. Notice that if system $(\mathcal{N}, M_0)$ is live then the set of reachable markings from M_0 is equal to the set of potentially reachable markings. We say that number w is *live weight* (respectively. *dead weight*) if and only if all markings with weight w are live and there exists at least one (respectively, if and only if no live marking in $\mathcal{C}$ has a weight d). We denote by M_D the greatest dead marking of $\mathcal{C}$.

Example 8.2.2 Let $\mathcal{C}$ be the system represented in Fig. 8.2. We have that incident matrix associated to $\mathcal{C}$ is given by

$$C = \begin{pmatrix} 5 & 0 & 0 & -4 \\ -9 & 3 & 0 & 0 \\ 0 & -5 & 4 & 0 \\ 0 & 0 & -3 & 9 \end{pmatrix}.$$

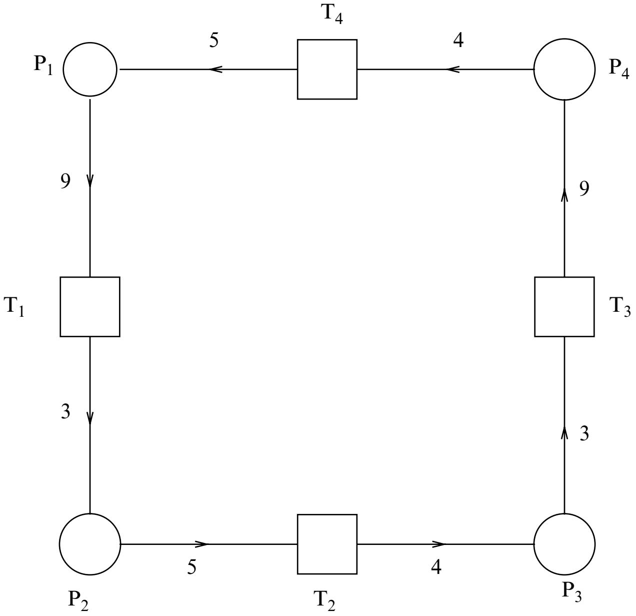

Figure 8.2: A conservative weighted circuit system.

System $\mathcal{C}$ is conservative since $Y = (4, 12, 15, 5)^t$. If $M = (8, 4, 2, 3)$ then the weight of $\mathcal{C}$ is given by $W(M) = (4, 12, 15, 5) \cdot (8, 4, 2, 3) = 125$.

Question *What is the least live weight in a conservative weighted circuit?*

Teruel *et al.* [444] answered this question by using **FP**.

Theorem 8.2.3 *[444] Let $\mathcal{C}$ be a consistent weighted circuit and let $Y^t = (y_1, \ldots, y_n)$ be a P-invariant. Then $W(M_D) - g(y_1, \ldots, y_n)$ is the value of the minimal live weight.*

The proof of Theorem 8.2.3 depends on a non-trivial intrisic result (see [93, Lemma 2.3]). It is clear that having a formula for the Frobenius number would give a simple method to determine the value of the least live weight. Chrząstowski-Wachtel and Raczunas [93] proved the following stronger result.

Theorem 8.2.4 *[93] The problem of finding a formula for the least live weight in conservative weighted circuits and* **FP** *are equivalent.*

Proof. Theorem 8.2.3 shows that the problem of finding the least live weight can be reduced to **FP**. For the other direction, it is enough to construct a circuit with the least live weight equal to $W(M_D) - g(y_1, \ldots, y_n)$. To this end, it suffices to construct a circuit with the weight vector equal to $Y = (y_1, \ldots, y_n)$. It can be easily checked that the circuit with input arcs defined as $c_{i,i} = \frac{[y_i, y_{i-1}]}{y_i}$ and with output arcs defined as $c_{i,i-1} = \frac{[y_i, y_{i-1}]}{y_{i-1}}$ has Y as its weight vector, where $[a, b]$ denotes the $lcm(a, b)$. □

Example 8.2.5 In continuation of Example 8.2.2, we can easily verify that $g(4, 5, 12, 15) = g(4, 5) = 11$ and by Theorem 8.2.3 we have that the weight $W(M) - g(4, 5, 12, 15) = 125 - 11 = 114$ is the least live weight.

8.3 Partition of a vector space

A collection $\{V_i\}_{i=1}^{k_1}$ of subspaces of $V = V_n(q)$ (the vector space of n-tuples over $GF[q]$ with q an arbitrary prime power) is called a *partition* of V if and only if $V = \cup_{i=1}^{k} V_i$ and $V_i \cap V_j = \{0\}$ when $1 \leq i \neq j \leq k$.

A group H is said to have a partition $H = G_1 \cup \cdots \cup G_n$ if H is the union of n of its subgroups that have pairwise only the zero element in common. Partitions groups have been studied by several authors. Young [485] proved that if an abelian group has a non-trivial partition, the group must be an elementary abelian p-group. Since such a group can be represented as the additive group of some $V_n(p)$ and U is a subgroup of $V_n(p)$ if and only if U is a subspace of $V_n(p)$ then partitions of $V_n(p)$ are a generalization of partitions of abelian groups.

Herzog and Schønheim [194] related the partition problem (existence, classification and enumeration of the partitions of $V_n(p)$) to coding theory. This motivated them to try to find sufficient and necessary conditions for the existence of partitions of abelian groups.

Beutelspacher [43] introduced the notion of *T-partition* of $V_n(q)$. Let $T = \{t_1, \ldots, t_k\}$ be a set of positive integers with $t_1 < \cdots < t_k$. If W is a subspace of $V_n(q)$, we denote by $\dim_q W$ the dimension of W. A partition π of $V_n(q)$ constitutes a *T-partition* if

(a) for any element W of π $\dim_q W \in T$,
and (b) for any $t \in T$ there is an element W of π with $\dim_q W = t$.

Remark 8.3.1 *[108, page 29] Let n, t be positive integers. Then a finite vector space $V_n(q)$ admits a partition of type $\{t\}$ if and only if t is a divisor of n.*

Beutelspacher proved the analoguous result for partitions of type $\{t_1, \ldots, t_k\}$.

Theorem 8.3.2 *[43] Let n be an integer. Suppose that $V_n(q)$ admits a partition π of type $T = \{t_1, \ldots, t_k\}$ with $t_1 < \cdots < t_k$ and $n > t_k$. Then,*

(i) $n \geq t_{k-1} + t_k$,

(ii) if $t_{k-1} + t_k \leq n < 2t_k$ then $(t_1, \ldots, t_{k-1}) | n - t_k$,

(iii) if $n \geq 2t_k$ then $(t_1, \ldots, t_k) | n$.

Proof. (i) The partition π must contain subspaces W and W' with $\dim_q W = t_k$ and $\dim_q W' = t_{k-1}$. Since W and W' have no point in common then $n \geq t_k + t_{k+1}$.

(ii) If $t_{k-1} + t_k \leq n < 2t_k$ then π contains a unique element, say W, with $\dim_q W = t_k$. Hence, the remaining elements of π cover exactly $q^n - q^{t_k}$ vectors. Since $d' = (t_1, \ldots, t_{k-1}) | t_i$ for each $i = 1, \ldots, k-1$ then $q^{d'} - 1 | q^{t_i} - 1$ for each $i = 1, \ldots, k-1$. And, since any subspace W' with $\dim_q W' = t_i$ in π contains exactly $q^{t_i} - 1$ of the $q^{t_k}(q^{n-t_k} - 1)$ vectors of $V_n \setminus W'$ then $q^{d'} - 1 | q^{t_k}(q^{n-t_k} - 1)$. Therefore, $q^{d'} - 1 | q^{n-t_k} - 1$ implying that $d' | n - t_k$.

(iii) If $d = (t_1, \ldots, t_k)$ then $q^d - 1 | q^{t_i} - 1$ for each $i = 1, \ldots, k$. So, by using the fact that π is a partition then $q^d - 1 | q^n - 1$, implying that $d | n$. □

Theorem 8.3.3 *[43] Let n be an integer such that $n > dg(t_1/d, \dots, t_k/d) + t_1 + \cdots + t_k$, where $d = (t_1, \dots, t_k)$. Then, $V_n(q)$ admits a partition of type $T = \{t_1, \dots, t_k\}$ if and only if $d|n$.*

Theorem 8.3.2 implies the necessity of Theorem 8.3.3. In order to prove the sufficiency we need the following two lemmas.

Lemma 8.3.4 *Let s, t be positive integers. Then $V_{s+t}(q)$ admits a partition of type $\{s, t\}$.*

Proof. By Remark 8.3.1, $V_{2s}(q)$ admits a partition π of type $\{s\}$. Let V' be a subspace of $V_{2s}(q)$ with $\dim_q V' = s + t$ containing an element, say W, of π. We shall show that any element W' of $\pi \setminus \{W\}$ intersects V' in a subspace of dimension t. To see the latter, first observe that $\dim_q(V' \cap W') \leq t$ otherwise the distinct elements W and W' of π would have a point in common. On the other hand, $\dim_q(V' \cap W') \geq t$ since both W and W' generate the whole vector space $V_{2s}(q)$ and $W \subseteq V'$. Hence,

$$\pi' = \{W\} \cup \{W' \cap V' | W' \in \pi \setminus \{W\}\}$$

is a partition of type $\{s, t\}$ in V'. □

Lemma 8.3.5 *Let $n \geq t$ be positive integers. If $V_n(q)$ admits a partition $\{t_1, \dots, t_k\}$ then $V_{n+t}(q)$ admits a partition of type $\{t_1, \dots, t_k, t\}$.*

Proof. By Lemma 8.3.4, $V_{n+t}(q)$ contains a partition π' of type $\{n, t\}$. Let W be the unique element in π' with $\dim_q W = n$. By hypothesis W admits a partition π'' of type $\{t_1, \dots, t_k\}$. Hence,

$$\pi := \pi'' \cup (\pi' \setminus \{W\})$$

is a partition of type $\{t_1, \dots, t_k, t\}$ in $V_{n+t}(q)$. □

Proof of Theorem 8.3.3. As we stated before, the necessity follows by Theorem 8.3.2. Suppose that $d|n$. By Lemma 8.3.4, $V_{t_k + t_{k-1}}(q)$ admits a partition of type $\{t_k, t_{k-1}\}$ and by Lemma 8.3.5 we have that $V_{t_1 + \cdots + t_k}(q)$ admits a partition of type $\{t_1, \dots, t_k\}$. Now, $n > dg(t_1/d, \dots, t_k/d) + t_1 + \cdots + t_k$ then a repeated application of Lemma 8.3.5 shows that $V_n(q)$ admits a partition of type $\{t_1, \dots, t_k\}$ if

$$n = \sum_{i=1}^{k} x_i t_i$$

for integers $x_i > 0$ (which is the case since $(t_1, \dots, t_k)|n$). □

Since the Frobenius number is finite then there is a least integer $N(T,q)$ such that if $n > N(T,q)$ and $(t_1,\ldots,t_k)$ divides n then $V_n(q)$ has a T-partition. Beutelspacher used the upper bound given in Theorem 3.1.11 to obtain that

$$N(T,q) \leq 2t_1 \left\lfloor \frac{t_k}{dk} \right\rfloor t_2 + \cdots + t_k. \tag{8.1}$$

In [190], Heden improved the latter by showing that if $t_1 \leq \frac{t_{k-1}}{2}$ or $k-2 \leq 2(q-1)$ then

$$N(T,q) \leq dg(t_1/d,\ldots,t_k/d) + t_{k-1} + t_k. \tag{8.2}$$

Moreover, Heden proved that in general

$$N(T,q) \leq dg(t_1/d,\ldots,t_k/d) + t_{k-2} + t_{k-1} + t_k. \tag{8.3}$$

8.4 Monomial curves

Let a, b, and c be positive integers such that $(a,b,c) = 1$. Let $R = k[X,Y,Z]$ be the polynomial ring graded by weight $deg(X) = a, deg(Y) = b$ and $deg(Z) = c$. Recall the result due to Herzog [191,258] stating that the monomial curve $k[t^a,t^b,t^c]$, denoted by C, considered as a R-module has the following resolution

$$0 \longrightarrow R^2 \xrightarrow{M} R^3 \xrightarrow{N} R \xrightarrow{I} k[t^a,t^b,t^c] \rightarrow 0,$$

where the map I is given by $X \rightarrow t^a$, $Y \rightarrow t^b$, $Z \rightarrow t^c$. Herzog determined explicitly matrix N (see eqn (4.7)) and gave an algorithm to find the matrix M but no explicit formula for the entries of M was given. In [299], Morales improved Herzog's result by giving the entries of M explicitely. To do this, Morales considered Rødseth's method (see Section 1.1.1) to find $g(a,b,c)$. Let s_0 be the unique integer such that $bs_0 \equiv c \bmod a$, $0 \leq s_0 < a$. If $s_0 = 0$ then M is trivially described. So, assume that $s_0 > 0$, write $s_{-1} := a$ and consider the continuous fraction

$$\begin{aligned} a &= q_1 s_0 - s_1,\ 0 \leq s_1 < s_0, \\ s_0 &= q_2 s_1 - s_2,\ 0 \leq s_2 < s_1, \\ s_1 &= q_3 s_2 - s_3,\ 0 \leq s_3 < s_2, \\ &\ \vdots \end{aligned}$$

$$s_{m-1} = q_{m+1}s_m,$$
$$s_{m+1} = 0,$$

where $q_i \geq 2$, $s_i \geq 0$ for all i (see Section 1.1.1). Set $p_{-1} = 0,\ p_0 = 1$, $p_{i+1} = q_{i+1}p_i - p_{i-1}$ and $r_i = (s_ib - p_ic)/a$ and recall that v is the unique integer number such that $r_{v+1} \leq 0 < r_v$, or equivalently, the unique integer such that

$$\frac{s_{v+1}}{p_{v+1}} \leq \frac{c}{b} < \frac{s_v}{p_v}.$$

Remark 8.4.1 *(a) $\{s_i\}$ and $\{r_i\}$ are strictly decreasing sequences and $\{p_i\}$ is a strictly increasing sequences.*

(b) r_{m+1} is a negative integer and $s_ip_{i+1} - s_{i+1}p_i = a$ for any i

Theorem 8.4.2 *[299] (i) If $a, b,$ and c are positive integers pairwise relatively prime then the matrix syzygies M of the curve C is given by*

$$M = \begin{pmatrix} Z^{p_v} & X^{-r_{v+1}} & Y^{s_v - s_{v+1}} \\ Y^{s_{v+1}} & Z^{p_{v+1}-p_v} & X^{r_v} \end{pmatrix}.$$

(ii) The curve C is a complete intersection if either $r_{v+1} = 0$ or $p_{v+1} = 0$ or $s_{v+1} = 0$.

By the results of Herzog in [191], part (i) of Theorem 8.4.2 follows if the following claim is true.

Claim 8.4.3

(i) $p_{v+1}c$ is the least multiple of c as a non-negative integer linear combination of a and b.

(ii) s_vb is the least multiple of b representable as a non-negative integer linear combination of a and c.

(iii) $(r_v - r_{v+1})a$ is the least multiple of a representable as a non-negative integer linear combination of b and c.

In Section 2.2, we defined the values L_1, L_2 and L_3 as the smallest positive integers such that there exist integers $x_{ij} \geq 0$, $1 \leq i, j \leq 3$, $i \neq j$ with

$$\begin{aligned} L_1a &= x_{12}b + x_{13}c, \\ L_2b &= x_{21}a + x_{23}c, \\ L_3c &= x_{31}a + x_{32}b. \end{aligned} \tag{8.4}$$

Claim 8.4.3 tells us that $L_1 = r_v - r_{v+1}$, $L_2 = s_v$ and $L_3 = p_{v+1}$. By the definition of s_i, p_i, and r_i, we have the following equalities

$$\begin{aligned} (r_v - r_{v+1})a =& (s_v - s_{v+1})b + (p_{v+1-p_v})c \\ s_v b =& \qquad r_v a \qquad + p_v c \\ p_{v+1} c =& \quad - r_{v+1} a \quad + s_{v+1} b. \end{aligned} \tag{8.5}$$

Note that the equations in the system (8.5) are consistent with the values of the L_is, given in Proposition 4.7.1.

Proof of Claim 8.4.3. Let $S =< a, b, c >$ and let $s \in S$, then the Apery set of s is defined as $Ap(S, s) = \{l \in S | l - s \notin S\}$ (see Section 7.2.2). Any element $s \in Ap(S, a)$ can be written of the form $s = yb + zc$ with integers $y, z \geq 0$. We suppose that z is the minimal with this property in which case the pair (y, z) is unique. Let

$$A = \{(y, z) | 0 \leq y < s_v - s_{v+1},\ 0 \leq z < p_{v+1}\}$$

and

$$B = \{(y, z) | s_v - s_{v+1} \leq y < s_v,\ 0 \leq z < p_{v+1} - p - v\}.$$

It can be checked that $Ap(a, S) = \{yb + zc | (y, z) \in A \cup B\}$ (by construction).

Part *(i)* By contradiction, suppose that there exists γ, $0 < \gamma < p_{v+1}$ such that $\gamma c \in< a, b >$. We have that $(0, \gamma) \in A \cup B$ and thus $\gamma c \in Ap(S, a)$. Now, since $\gamma c \in< a, b >$ then $\gamma c = \alpha a + \beta b$ for some non-negative integers α and β. We observe that in fact, $\alpha = 0$ (otherwise, $\gamma c - a = (\alpha - 1)a + \beta b \in S$, which is a contradiction since $\gamma c \in Ap(S, a)$). So, $\gamma c = \beta b$, which is a contradiction with the minimality condition on z.

Part *(ii)* By contradiction, suppose that there exists γ, $0 < \gamma < s_v$ such that $\gamma b \in< a, c >$ and γ is minimal with this property. We have that $(\gamma, 0) \in A \cup B$ and thus $\gamma b \in Ap(S, a)$. Now, since $\gamma b \in< a, b >$ then $\gamma b = \alpha a + \beta c$ for some non-negative integers α and β. We observe that in fact, $\alpha = 0$ (otherwise, $\gamma c - a = (\alpha - 1)a + \beta c \in S$, which is a contradiction since $\gamma c \in Ap(S, a)$). So, $\gamma c = \beta b$ and, by part (i), we have that $\lambda \geq p_{v+1}$. By using the third equation of system (8.5) we have

$$\gamma b = (\lambda - p_{v+1})c + b s_{v+1} + (-r_{v+1})a.$$

We observe that $r_{v+1} = 0$ otherwise, if $-r_{v+1} \geq 1$ then $\gamma b - a = (\lambda - p_{v+1})c + b s_{v+1} + (-r_{v+1} - 1)a \in S$, which is a contradiction since

$\gamma b \in Ap(S, a)$. So, we have

$$\gamma b = (\lambda - p_{v+1})c + bs_{v+1}.$$

By the minimality of γ, we have two cases: (a) $s_{v+1} = 0$ and $p_{v+1} = 0$ that is impossible since, by Remark 8.4.1, $s_v p_{v+1} - s_{v+1} p_v = 0 = a$ and (b) $\gamma = s_{v+1}$ and $\lambda = p_{v+1}$ in this case $s_{v+1} b = p_{v+1} c$. Since $(b, c) = 1$ then c divides s_{v+1} and combined with the fact that $(a, c) = 1$ we have, from the third equation of system (8.5), that c divides r_{v+1}. By the latter and since $r_{v+1} a = s_v b - p_v c$ (obtained by the recurrence of the r_is) then we have that c divides s_v. So, we deduce that if c divides s_{v+1} then c divides s_v, and, by carrying on this argument, we obtain that c divides $s_0 = a$, which is a contradiction.

Part *(iii)* By Proposition 4.7.1 we have that

$$\begin{aligned} L_1 &= x_{21} + x_{31} \\ L_2 &= x_{12} + x_{32} \\ L_3 &= x_{13} + x_{23}, \end{aligned}$$

where the x_{ij} are given as in the system (8.4). Now, by parts *(i)* and *(ii)* we have that $L_3 = p_{v+1}$ and $L_2 = s_v$ and by system (8.5) we deduce that $x_{31} = -r_{v+1}, x_{32} = s_{v+1}, x_{21} = r_v$ and $x_{23} = p_v$. From these, we obtain $L_1 = r_v - r_{v+1}$. □

In [300], Morales used Theorem 8.4.2 to construct a large class of monomial curves defined by an ideal P in $R = k[X, Y, Z]$ such that $R^{(P)}$ is *noetherian*.

8.5 Algebraic geometric codes

The idea of using methods from algebraic geometry to introduce *algebraic geometric* codes (AG codes) is one of the major developments in the theory of error-correcting codes. These codes are based on generalizations of Goppa's code and were inspired by ideas of the work of Goppa [164–166]. AG codes are known to be more efficient than the well-known *Reed–Solomon* codes in many parameter ranges and they also offer more flexibility in the choice of code parameters; see [461]. This series of results contributed significantly to advancing the decoding of algebraic geometric codes.

AG codes have played a more prominent role in the theory of error-correcting codes.

In 1982, Tsfasman *et al.* [459] obtained a very appealing result: they showed the existence of a sequence of AG codes that exceeds the

Gilbert–Varshamov bound[2]. Since then, many papers dealing with AG codes and decoding procedure have followed.

The Frobenius numbers are of particular interest for the study of the AG codes called *evaluation code* and its dual code. To see this, we need to introduce some definitions and terminology. The rest of this section is based on [205] where a detailed treatment can be found.

Let $R = \mathbb{F}[X_1, \ldots, X_m]$ be a $\mathbb{F}_q$-algebra and suppose that $\prec$ is a total order on the set of monomials in the variables $X_1, \ldots, X_m$ such that if $M \neq 1$ then $1 \prec M$ and if $M_1 \prec M_2$ then $MM_1 \prec MM_2$, where M, M_1 and M_2 are monomials. Let $f_1, f_2, \ldots$ be the enumeration of the set of monomials such that $f_i \prec f_{i+1}$ for all i. The monomials form a basis of R, so every monomial $f \neq 0$ can be written uniquely as

$$f = \sum_{i=1}^{j} \lambda_i f_i,$$

where $\lambda_i \in \mathbb{F}$ for all i and $\lambda_j \neq 0$. Let us define the function

$$\rho : \mathbb{F}[X_1, \ldots, X_m] \longrightarrow \mathbb{N} \cup \{-\infty\}$$

by $\rho(0) = -\infty$ and $\rho(f) = \min\{j | f = \sum_{i=1}^{j} \lambda_i f_i\} - 1$. One can check that the function ρ satisfies the following conditions

(a) $\rho(f) = -\infty$ if and only if $f = 0$,

(b) $\rho(\lambda f) = \rho(f)$ for all non-zero $\lambda \in \mathbb{F}$,

(c) $\rho(f+g) =\leq \max\{\rho(f), \rho(g)\}$ and equality holds when $\rho(f) < \rho(g)$,

(d) If $\rho(f) < \rho(g)$ and $h \neq 0$ then $\rho(fh) < \rho(gh)$,

(e) If $\rho(f) = \rho(g)$ then there exists a non-zero $\lambda \in \mathbb{F}$ such that $\rho(f - \lambda g) < \rho(g)$,

for all $f, g, h \in R$. Here $-\infty < n$ for all $n \in \mathbb{N}$. An *order function* on R is a map

$$\rho : R \longrightarrow \mathbb{N} \cup \{-\infty\}$$

satisfying the above conditions. A *weight function* on R is an order function on R that also satisfies the following condition

(f) $\rho(fg) = \rho(f) + \rho(g)$.

[2] Tsfasman, Vlăduţ and Zink received the IEEE Information Theory Group Paper Award in 1983 for this work.

Let $(f_i | i \in \mathbb{N})$ be a basis of R such that $\rho(f_i) < \rho(f_{i+1})$ (the existence of such a basis is always guaranteed [205, Proposition 3.12]) and let L_l be the vector space generated by $f_1, \ldots, f_l$. In this case, we have that $\rho(f) = \rho(f_l)$ if and only if l is the smallest integer such that $f \in L_l$ for all non-zero $f \in R$. The vector space $\mathbb{F}_q^n$ with the coordinatewise multiplication, denoted by $*$, becomes a commutative ring with the unit $(1, \ldots, 1)$. By identifying the unitary subring $\{(\lambda, \ldots, \lambda) | \lambda \in \mathbb{F}_q\}$ with $\mathbb{F}_q$ then $\mathbb{F}_q^n$ is an $\mathbb{F}_q$-algebra. We say that the map $\psi : R \to \mathbb{F}_q^n$ is a *morphism* of $\mathbb{F}_q^n$-algebras if ψ is $\mathbb{F}_q$-linear and $\psi(fg) = \psi(f) * \psi(g)$. Let $\mathbf{h}_i = \psi(f_i)$ and define the *evaluation code* E_l and its *dual* C_l by

$$E_l = \psi(L_l) =< \mathbf{h}_1, \ldots, \mathbf{h}_l > \text{ and } C_l = \{\mathbf{c} \in \mathbb{F}_q^n | \mathbf{c} \cdot \mathbf{h}_i = 0 \text{ for all } i \leq l\}.$$

We note that condition (f) above implies that the subset $\Gamma = \{\rho(f) | f \in R,\ f \neq 0\}$ of the non-negative integers has the property that $0 \in \Gamma$ and $x + y \in \Gamma$ for all $x, y \in \Gamma$. Thus, Γ is a semigroup (see Chapter 7). It is assumed that the greatest common divisor of the weights $\rho(f),\ 0 \neq f \in R$ is one. So, the number of gaps of Γ, denoted by $N(\Gamma)$ is finite. The elements of Γ will be enumerated by the sequence $(\rho_i | i \in \mathbb{N})$ such that $\rho_i < \rho_{i+1}$ for all i and the number of gaps smaller than ρ_i will be denoted by $n(\rho_i)$. Let $l(i,j)$ be the smallest positive integer l such that $f_i f_j \in L_l$ and define $N_l = \{(i,j) \in \mathbb{N}^2 | l(i,j) = l = 1\}$. Since the function $l(i,j)$ is determined by $\rho_{l(i,j)} = \rho_i + \rho_j$ then the set N_l can be redefined by $N_l = \{(i,j) \in \mathbb{N}^2 | \rho_i + \rho_j = \rho_{l+1}\}$. Let $\nu_l = |N_l|$ and $d(l) = \min\{\nu_m | m \geq l\}$. The number $l + 1 - N(\Gamma)$ is called the *Goppa designed minimum distance* of C_l and is denoted by $d_G(l)$. It is a lower bound on the minimum distance of C_l.

Theorem 8.5.1 *Let $g(\Gamma)$ be the conductor of Γ and let $D(l) = \{(x,y) \in \mathbb{N}^2 | x$ and y are gaps and $x + y = \rho_{l+1}\}$. Then,*

$$\nu_l = l + 1 - l + 1 - n(\rho_{l+1}) + |D(l)|,$$

where $n(\rho_{l+1}) = N(\Gamma)$ if $l \geq g(\Gamma) - N(\Gamma)$ and $|D(l)| = 0$ if $l > 2g(\Gamma) - N(\Gamma) - 2$. Furthermore, $d(l) \geq d_G(l) = l + 1 - N(\Gamma)$ and equality holds if $l > 2g(\Gamma) - N(\Gamma) - 2$.

In this case $d_G(l)$ is called the *order bound* or the *Feng–Rao designed minimum distance* of C_l. This distance is a good estimate for the minimum distance of one-point AG codes, the main interest of such a code is that they can be decoded efficiently by the majority scheme of the Feng and Rao algorithm [142].

8.6 Tilings

A *tiling* is a plane-filling arrangement of plane figures called *tiles* (another word for a tiling is a *tessalation*). The history of tessellations dates back to the early Greeks. The Greeks actually used small quadrilateral tiles as tokens in their games. These tiles then were taken and used to make mosaic pictures on walls, floors, and ceilings. Mathematicians tend to be very interested in tessellations because of their ties to symmetry of figures, angle divisions, rotation of objects, and various geometrical concepts. Here, we consider the problem of tiling a large rectangle using smaller rectangles.

> **Problem B-3 (from the 1991 William Mowell Putnam Examination)**
>
> *'Does there exist a natural number L, such that if m and n are integers greater than L, then an $m \times n$ rectangle may be expressed as a union of 4×6 and 5×7 rectangles any two of which intersect at most along their boundaries?'*

The rectagles 4×6 and 5×7 will be called tiles and will be denoted by T_1 and T_2. A rectangle is to be said *tiled* if it can be expressed as a union of T_1 and T_2 any two of which intersect at most along their boundaries. Since the areas of T_1 and T_2 are 24 and 35, respectively, then a rectangle of area A that is tiled must satisfy the equation

$$24x + 35y = A, \tag{8.6}$$

where x and y are non-negative integers. The solutions to this equation determine a list of the possible quantities of the two types of tiles used in a tiling. We note that the areas of T_1 and T_2 are relatively prime, otherwise if an integer $p > 1$ divides each area, tiling a rectangle whose sides are both congruent to 1 modulo p would not be possible.

In [244], Klosinski *et al.* gave one solution to the Putnam problem, with a guarantee that every rectangle whose sides are larger than 2213 can be tiled. Their proof uses Theorem 2.1.1 and it goes as follows.

A 20×6 and a 20×7 rectangle can be tiled (by joining 5 L_1 and by joining 4 L_2, respectively) then, by Theorem 2.1.1

$$\text{a } 20 \times n \text{ rectangle can be tiled for any } n > g(6,7) = 29. \tag{8.7}$$

Now, a 35×5 and a 35×7 rectangle can be tiled (by joining 5 L_2) then, by Theorem 2.1.1

$$\text{a } 35 \times n \text{ rectangle can be tiled for any } n > g(5,7) = 23, \tag{8.8}$$

and finally a 42×4 and a 42×5 rectangle can be tiled (by joining 7 L_1 and by joining 6 L_2, respectively) then, by Theorem 2.1.1

$$\text{a } 42 \times n \text{ rectangle can be tiled for any } n > g(4,5) = 11. \tag{8.9}$$

By combining eqns (8.7) and (8.8), we can tile a $55 \times n$ rectangle for any $n \geq 30$. Since $(42, 55) = 1$ then, from the latter and from eqn (8.9) we conclude that all $m \times n$ rectangles with $m \geq n > g(42, 55) = 2214$ can be tiled with rectangles T_1 and T_2.

In [304], Narayan and Schwenk established a lower bound for L by showing that a 33×33 square cannot be tiled and they proved that this bound is tight.

8.7 Applications of denumerants

8.7.1 Balls and cells

A classical use of generating functions is the calculation of the number of possible placements of n different balls into r distinct cells under certain restrictions. For instance, one may wish to know the number of n place sequences made up from an alphabet of As, Bs, and Cs so that the number of As is even, the number of Bs is odd and there are no restriction on the number of Cs. Many such problems are dealt with by Liu [279, Chapter 2] and by Riordan [352, Chapter 5].

Cornish [97] investigated the following generalization.

> Let h_j and k_j be integers such that $0 \leq h_j < k_j$ for each $j = 1, \ldots, r$. What is the number of ways of placing $n \geq 0$ different balls in r distinct cells so that the number of balls in the j-th cell is congruent to h_j modulo k_j?

Cornish [97] gave an expression for such a number, denoted by $p(n; h_1, \ldots, h_r, k_1, \ldots, k_r)$.

Theorem 8.7.1 *[97]*

$$p(n; h_1, \ldots, h_r, k_1, \ldots, k_r) = \left(\prod_{j=1}^{r} k_j\right)^{-1} \times \sum_{\substack{s_1, \ldots, s_r \\ 0 \leq s_j \leq k_j - 1}} \left(\prod_{j=1}^{r} \omega_i^{-h_j s_j}\right) \left(\sum_{j=1}^{r} \omega_j^{s_j}\right)^{n},$$

where $\omega_j = e^{\frac{2\pi}{k_j}}$.

Cornish's proof[3] is by means of the exponential enumerator and employs the generalized *cosh*: $C_k(x) = \sum_{i=0}^{\infty} \frac{x^{ki}}{(ki)!}$. The simpler alternative proof below was given by Pitman and Leske [331]. They also noted the following connection between conditions for $p(n; h_1, \dots, h_r, k_1, \dots, k_r)$ to be non-zero and the denumerant.

Proposition 8.7.2 *[331] Let* $n_j \equiv h_j \bmod k_j$ *(and thus* $n_j = h_j + y_j k_j$*). Then,*

$p(n; h_1, \dots, h_r, k_1, \dots, k_r) > 0$ *if and only if the equation*

$$y_1 k_1 + \cdots + y_r k_r = n - \sum_{j=1}^{r} h_j$$

is solvable in non-negative integers, $y_1, \dots, y_r$*, that is,*

$$p(n; h_1, \dots, h_r, k_1, \dots, k_r) > 0 \textit{ if and only if}$$
$$d\left(n - \sum_{j=1}^{r} h_j; k_1, \dots, k_r\right) > 0.$$

Sketch of the proof of Theorem 8.7.1. Let us write $e^{2\pi i y} = e(y)$ and let x, h and $k > 0$ be integers. Then,

$$\sum_{s=0}^{k-1} e^{\frac{2\pi i s(x-h)}{k}} = \begin{cases} k & \text{if } x \equiv h \bmod k, \\ 0 & \text{otherwise.} \end{cases}$$

Now, the number of ways of placing $n = n_1 + \cdots + n_r$ different balls into r distinct cells so that there are n_j balls in the j-th cell is $\frac{n!}{n_1! n_2! \cdots n_r!}$. Hence,

$$p(n; h_1, \dots, h_r, k_1, \dots, k_r) = \sum_{(n_1, \dots, n_r) \in P_n} \frac{n!}{n_1! n_2! \cdots n_r!},$$

where

$$P_n = \{(n_1, \dots, n_r) \in \mathbb{N}^r | n_1 + \cdots + n_r = n\} \text{ and } n_j \equiv h_j \bmod k_j.$$

Of course $p(n; h_1, \dots, h_r, k_1, \dots, k_r) = 0$ if $P_n = \emptyset$. We obtain

[3] As a consequence, Cornish was led to the rediscovery of the so-called *higher-order hyperbolic functions*; comments on these functions together with related bibliography can be found in [231].

$$\begin{aligned}
&p(n;h_1,\ldots,h_r,k_1,\ldots,k_r)\prod_{j=1}^{r}k_j\\
&\quad=\sum_{\substack{n_1,\ldots,n_r\geq 0\\ n_1+\cdots+n_r=n}}\frac{n!}{n_1!n_2!\cdots n_r!}\prod_{j=1}^{r}\left(\sum_{0\leq s_j\leq k_j-1}e^{\frac{2\pi i s_j(n_j-h_j)}{k_j}}\right)\\
&\quad=\sum_{\substack{s_1,\ldots,s_r\\ 0\leq s_j\leq k_j-1}}\prod_{j=1}^{r}\omega_j^{-h_js_j}\sum_{\substack{n_1,\ldots,n_r\geq 0\\ n_1+\cdots+n_r=n}}\frac{n!}{n_1!n_2!\cdots n_r!}\prod_{j=1}^{r}\omega_j^{n_js_j}.
\end{aligned}$$

And, by the multinomial theorem,

$$\sum_{\substack{n_1,\ldots,n_r\geq 0\\ n_1+\cdots+n_r=n}}\frac{n!}{n_1!n_2!\cdots n_r!}=\left(\sum_{j=1}^{r}\omega_j^{s_j}\right)^n,$$

from which the result follows. □

8.7.2 Conjugate power equations

Let $w_{ij},\ 1\leq i\leq k,\ \ 1\leq j\leq t$ and $n_1,\ldots,n_k$ be non-negative integers. Consider the linear diophantine problem

$$\begin{aligned}
n_1&=w_{11}y_1+w_{12}y_2+\cdots+w_{1t}y_t,\\
n_2&=w_{21}y_1+w_{22}y_2+\cdots+w_{2t}y_t,\\
&\ \ \vdots\\
n_k&=w_{k1}y_1+w_{k2}y_2+\cdots+w_{kt}y_t,
\end{aligned}\tag{8.10}$$

which can be written succintly as

$$N=WY,$$

where $N=(n_1,\ldots,n_k)^t$ and W denotes the matrix $W=(w_{ij})$, $1\leq i\leq k,\ \ 1\leq j\leq t$. Here, N and W are fixed and

$$Y=\begin{pmatrix} y_1\\ \vdots\\ y_t\end{pmatrix}$$

consists of non-negative variables.

In 1748, Euler [137,138] pointed out that the number of non-negative solutions of a system $Wx=N$ of linear equations is equal to the coefficient of $x_1^{n_1}\cdots x_k^{n_k}$ in the expansion of

$$R(x_1,\ldots,x_k)=\frac{1}{(1-(x_1^{w_{11}}\cdots x_t^{w_{k1}}))\cdots(1-(x_1^{w_{1t}}\cdots x_t^{w_{kt}}))}.$$

In the case when $k = 1$ and $n_1 = n$ we obtain Theorem 4.1.2. In [11], Anshel and Goldfeld studied the function $R(x_1, \ldots, x_k)$ and obtained the following bound for the length $\sum_{i=1}^{t} y_i$ of the solution Y for the equation $N = WY$

$$\sum_{i=1}^{t} y_i \le \left(\sum_{i=1}^{k} n_i\right) \cdot \left[\sum_{j=1}^{t}\left(\sum_{i=1}^{k} w_{ij}\right)^{-1}\right]^{\frac{1}{2}} \cdot \max_{1\le j\le t}\left(\sum_{i=1}^{k} w_{ij}\right)^{-\frac{1}{2}} = B(N, W). \tag{8.11}$$

They applied their results to the investigation of equations in groups. Let $G = G(q_1, \ldots, q_t)$ be a *HNN group*[4] given by the generators and relations

$$< a_1, \ldots, a_t, b; a_1^{-1} b a_1 = b^{q_1}, \ldots, a_t^{-1} b a_t = b^{q_t} >,$$

where the exponents $q_1, \ldots, q_t$ are distinct rational integers, $q_i \ge 2$. Let $p_1, \ldots, p_t$ denotes the distinct prime divisors of the exponent q_i, so

$$q_i = p_1^{w_{i1}} \cdots p_k^{w_{ik}}, \tag{8.12}$$

with non-negative integer exponents $w_{i1}, \ldots, w_{ik}$. A positive *conjugate power equation* for G is given by

$$b^n = x^{-1} b x, \tag{8.13}$$

where n is a positive integer and x is a positive word (*i.e.* one containing no negative exponents in the generating symbols $a_1, \ldots, a_t, b$. It is known [10, 12] that equality (8.13) has a solution provided that $n = p_1^{n_1} \cdots p_k^{n_k}$ and system (8.10) takes the form $N = (n_1, \ldots, n_k)$ where W consists of the w_{ij} given in eqn (8.12) and each $y_i \in Y = (y_1, \ldots, y_t)$ denotes the number of occurrences of a_i in the word x. Also, if x is a solution to eqn (8.13), then the insertion or deletion of a b symbol anywhere in the word x results in another solution of eqn (8.13).

Anshel and Goldfeld proved that if there exists a solution x of equality (8.13) (involving only the generators $a_1, \ldots, a_t$) then the word length of x, denoted by $|x|$ satisfies the bound

$$|x| \le B(N, W),$$

with $B(N, W)$ given in eqn (8.11). They obtained the following corollary involving the Frobenius number.

[4] Introduced by Higman *et al.* in [195].

Corollary 8.7.3 *[11] If the group $G = G(p^{w_1}, \dots, p^{w_t})$ with p a fixed prime and $w_1 < \cdots < w_t$ with $(w_1, \dots, w_t) = 1$ and $n > g(w_1, \dots, w_t)$ then there exists a solution x of eqn (8.13) with*

$$|x| \leq \frac{n}{\sqrt{w_t \sum_{i=1}^{t} w_i}}.$$

8.7.3 Invariant cubature formulas

A *Cubature formula* is a formula for the approximate calculation of multiple integrals of the form

$$I(f) = \int_{\Omega} p(x) f(x) \mathrm{d}x,$$

where the integration is performed over a set Ω in the Euclidean space $\mathbb{R}^n$, $x = (x_1, \dots, x_n)$ with $p(x)$ fixed. A cubature formula is an approximate equality

$$I(f) \cong \sum_{j=1}^{N} C_j f(x^j). \tag{8.14}$$

A cubature formula is said to have the *m-property* if eqn (8.14) is an exact equality whenever $f(x)$ is a polynomial of degree at most m. Let G be a finite subgroup of the group of orthogonal transformations of the space $\mathbb{R}^n$ that leave the origin fixed.

Theorem 8.7.4 *[431] A cubature formula that is invariant under G possesses the m-property if and only if it is exact for all polynomials of degree at most m that are invariant under G.*

This theorem is of essential importance in the construction of invariant cubature formulas. It made possible the construction of fairly convenient formulas for the approximate integration on spheres and on their interiors.

Theorem 8.7.4 shows the necessity to know the number of invariant polynomials of degree at most m. It turns out that this number coincides with $d(m; a_1, \dots, a_n)$ for some values $a_1, \dots, a_n$.

We refer the reader to [128] for both an excellent introduction as well as an advanced treatment of cubature formulas.

8.8 Other applications

8.8.1 Generating random vectors

One standard way to generate random vectors uses a procedure to generate random numbers, say, $\psi_1, \psi_2, \dots$ and thus to generate random vectors $\eta_1 = (\psi_1, \ldots, \psi_n), \eta_2 = (\psi_{n+1}, \ldots, \psi_{2n}), \ldots$. As remarked by Vizvári [474], one of the serious drawbacks of this method is that if the random number generator is cyclic (with cycle length C) then the random vector generators are cyclic as well, with cycle length at most C. In particular, in higher dimensions, it means that the random vectors lie very sparsely in the space; see [308, 381].

Vizvári [474] used the vector generalization of **FP** (see Section 6.5) to present a new method that generates the random vector directly (avoiding the above-mentioned disavantage). This method generates all of the integer points of a given m-dimensional rectangle with equal probability and thus the cycle length of it can be greater than any prior given large number. Let us see how this method proceeds. Let $(d_1, \ldots, d_m)$ be a fixed vector of positive integers. Let

$$U = \{u = (u_1, \ldots, u_m) | 0 \le u_i < d_i,\ u_i \in \mathbb{R}^+ \text{ for all } i\}.$$

Let D be the set of integer points of the rectangle U, that is

$$D = \{u = (u_1, \ldots, u_m) | 0 \le u_i < d_i,\ u_i \in \mathbb{N}^+ \text{ for all } i\}.$$

Let $\{a_1, \ldots, a_n\} \subset D$ of fixed vectors and let ξ_i, $i \ge 1$ be a random number that is uniformly distributed on the set $\{1, \ldots, n\}$. We shall denote by $n(i)$ the i-th coordinate of vector n.

Random Vector Algorithm

```
**Begin**
$n_0 := 0$
$k := 0$
**While** true **Do**
**Begin**
   $n_{k+1} := n_k + a_{\xi_k}$
   **For** $i := 1$ **To** $m$ **Do**
      **If** $n_{k+1}(i) \ge d_i$ **Then** $n_{k+1}(i) = n_{k+1}(i) - d_i$
**End**
$k := k + 1$
**End**
```

Vizvári [474] showed that if the set $\{a_1, \ldots, a_n\}$ contains a linear basis of $\mathbb{R}^m$ and the condition (6.7) of Theorem 6.5.1 is satisfied then

$$\lim_{k \to \infty} P(n_k = u) = \frac{1}{\prod_{j=1}^{m} d_j} \quad \text{for all } \ u \in U.$$

Notice that this method uses a random number generator (for the ξ_is). If the latter is acyclic then the random vector generator is also acyclic but if it is cyclic (say, with periodic length C) then the random vector generator can also be cyclic (say, with periodic length γ). It is clear that

$$\gamma \geq |C| = \prod_{j=1}^{m} d_j,$$

and as $|D|$ is independent of C and it can be arbitrarily large then γ can also be arbitrarily large.

8.8.2 Non-hamiltonian graphs

We say that a graph G is *Hamiltonian* if there is a cycle in G that passes through every vertex. A graph G is called a *hypo-Hamiltonian* if G is not Hamiltonian but every vertex-deleted subgraph $G - v$ is Hamiltonian.

Example 8.8.1 The Petersen graph is the smallest (of order 10) hypo-Hamiltonian graph; see Fig. 8.3.

Chvátal [95] introduced a class of graphs called *flip-flops* for constructing new hypo-Hamiltonian graphs and showed that the number $h(p)$ of non-isomorphic hypo-Hamiltonian graphs of order p has the property that $h(p) \longrightarrow \infty$. A graph is *traceable* if it contains a Hamiltonian path. Clearly every Hamiltonian graph is also traceable but the converse does not always hold (for instance, a path is traceable but not

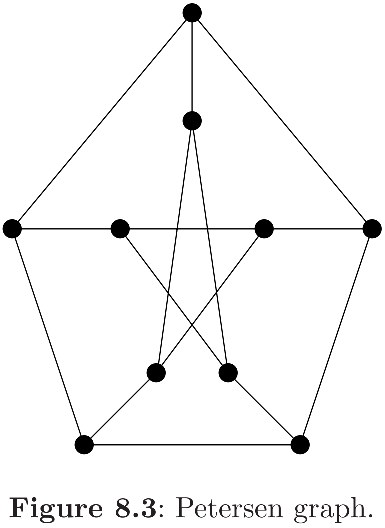

Figure 8.3: Petersen graph.

Hamiltonian). A graph is *homogeneously traceable* if there is a Hamiltonian path beginning at every vertex of G. Figure 8.4 illustrates a homogeneously traceable non-Hamiltonian graph.

Notice that every hypo-Hamiltonian graph is also homogeneously traceable. Skupień [426] introduced the notion of homogeneously traceable graphs and the existence of homogeneously traceable non-Hamiltonian graphs for all orders $p \geq 9$ was shown in [87]. Let $F \subset E(G)$. G is called a F*-Hamiltonian* if it contains a Hamiltonian cylce through F. In [428], Skupień contructs exponentially many n-vertex *minimum* homogeneously traceable non-F-Hamiltonian graphs (here, minimum means that the number of edges is as large as possible provided the number of vertices is fixed). Skupień's idea is based in some new constructions, involving flip-flops, that depend on the existence of the value $k(m; r, s)$ (defined in the modular generalization problem in Section 6.2) for some integers r, s and m. Skupień's construction is as follows. Let M and S be the graphs defined in Fig. 8.5.

We construct the graph $G(r, s)$ by aligning r consecutive copies of M and afterward s consecutive copies of S and by joining vertices c and a and vertices d and b of two consecutive copies (not necessarily of

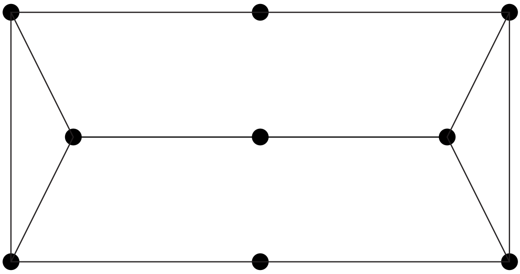

Figure 8.4: A homogeneously traceable non-Hamiltonian graph.

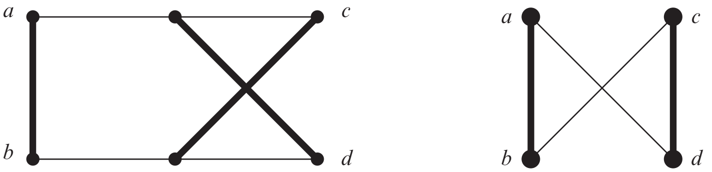

Figure 8.5: Graphs M and S each containing a special 1-factor denoted by bolded edges.

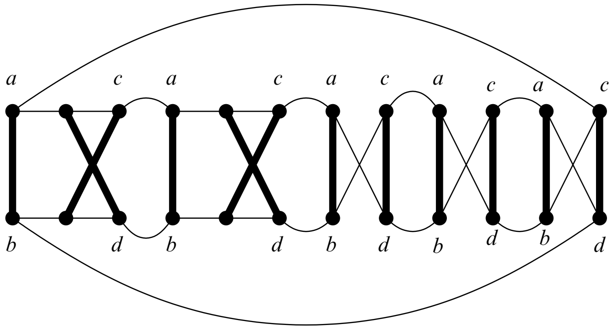

Figure 8.6: Graph $G(2,3)$.

the same type) including the last and first copies. Figure 8.6 illustrates $G(2,3)$.

Let F be the set of edges induced by the set of 1-factors of each copy.

Proposition 8.8.2 *Let r and s be a solution of equation*

$$n = 2r + 3s, \quad \textit{where } r + s \textit{ is odd}, \tag{8.15}$$

with $n \geq 22$. Then, $G(r,s)$ is a n-vertex minimum homogeneously traceable non-F-Hamiltonian graph.

We notice that Theorem 6.2.2 ensures the existence of integers $1 \leq r \leq 3$ and $s \geq 2$ verifying eqn (8.15) since $k(2;2,3) = 2(2)(3)-2-3 = 7$ is the largest integer such that it is j-omitted with $j = 0$ or 1. Thus, for any integer $n \geq 8$ there exist non-negative integers s, r such that $n = sa + rb$ and $s + r \equiv j \bmod 2$ for $j = 0, 1$, in particular if $j = 1$ this implies that $r + s$ is odd, as desired. The condition $n \geq 22$ is required for the non-F-Hamiltonicity of $G(r,s)$.

8.9 Supplementary notes

Xu and Wu [483] presented two sets of necessary and sufficient conditions for the existence of non-negative integer solutions for the indeterminate equation $\sum_{i=1}^{n} x_i a_i = m$, where $m \leq \sum_{i=2}^{n} a_i(d_{i-1}/d_i) - \sum_{i=1}^{n} a_i$. These conditions were developed from the discussion of the reachability and liveness, of the Petri net model Type I of an indeterminate equation of the first degree. Using these conditions, two kinds of algorithms for **FP** were given.

In [155], Gaubert and Klimann studied the algebraic problems that arise when considering rational computations of *diod* algebras in connection with the analysis of a specific class of discrete event systems. They investigated the periodicities of algebras and showed how **FP** helps in the computation of the periodic behaviour.

Anderson and Winner [8] examined factorization problems in the semigroup ring $k[S]$ and gave upper bounds in terms of the conductor of S. In [200], Hofmeister used **FP** to generalize other related problems. Pellikaan and Torres [325] have nicely applied results of Weierstrass semigroups to AG codes; see also [139] and [81].

Blażewicz *et al.* [48] used the upper bound of Theorem 6.1.1 to study the computational complexity of the following problem that arises in DNA sequencing by hybridization.

Given integers l and k and a set S of words of length k over the alphabet $\{A, B, C, D\}$, does there exist a word w of length l with k-spectrum (*i.e.* the set of all subsequences of w consisting of k consecutive letters) equal S? (see [49] for more details).

Motivated by their work on primality testing, Lenstra and Pomerance [265] stated recently a problem that can be viewed as a continuous analogue of **FP** in which bounded sets of positive *real* numbers are considered instead of positive integers.

Results in connection with the complexity of *learning* problems can be found in [2,3]. Applications of **FP** in relation with the *automata* are given in [102, 293, 411]. Rosenmüller and Weidner [371] have studied **FP** in relation to *linear diophantine analysis.* Rosiak [372] estimated certain functions related to primitive digraphs by using the Frobenius number. An application of the Frobenius number to representation theory is discussed in [370]. Remy and Thiel [350] used the Frobenius number to solve certain problems in relation to image description.

Appendix A

Problems and conjectures

A.1 Algorithmic questions

It is known [342] that **FP** is $\mathcal{NP}$-hard under *Turing* reductions.

Problem A.1.1 *Is* **FP** *$\mathcal{NP}$-complete (under* Karp reductions*)?*

One may wonder whether the knowledge of the Frobenius number could help to find a desired representation. Consider the following *promising* question.

Problem A.1.2 *Let $a_1, \ldots, a_n$ and t be positive integers such that $t > g(a_1, \ldots, a_n)$. Is there a polynomial time algorithm that finds $s \subseteq \{1, \ldots, n\}$ such that $t = \sum\limits_{i \in s} a_i$?*

Vizvári conjecture[1] that there exists an integer K such that the above question is easy if $t > K$.

To show that **FP** is solvable in polynomial time with n fixed, Kannan [228] gave a polynomial time algorithm that finds the covering radius $\mu(P, L)$ for any convex set P in $\mathbb{R}^n$ and any lattice L of dimension n also in $\mathbb{R}^n$ with fixed n.

Problem A.1.3 *Does there exist a polynomial time algorithm that finds $\mu(P, L)$ where P and L are defined as in Theorem 1.2.14?*

Maybe the constructive version for the covering radius given in Corollary 1.2.16 could leads to such an algorithm. The following conjecture is due to L. Lovász.

Conjecture A.1.4. *[280] If n is fixed and A is an integral matrix then the set of vectors b yielding maximal lattice free bodies (see Section*

[1] Personal communication.

1.2.1 for definitions) is the union of the set of lattice points contained in a polynomial number of polyhedra (with a particular lattice for each polyhedron).

Maximizing a linear function over the lattice points in each such polyhedron is a standard integer program which can be solved in polynomial time for a fixed number of variables (by using Lenstra's algorithm [264]). So, if the Lovász conjecture were correct, this would yield to an alternative polynomial algorithm for **FP**.

A.2 $g(a_1, \ldots, a_n)$

Davison has proposed the following two conjectures [104, Conjectures 1 and 2]. Let a, b, c be positive integers and let $X_n = \{(a,b,c) | 1 \leq a, b, c \leq n,\ (a,b,c) = 1\}$.

Conjecture A.2.1. *Is it true that* $\sup_n(\frac{1}{X_n}) \sum\limits_{(a,b,c) \in X_n} \left(\frac{g(a,b,c)-a-b-c}{\sqrt{abc}}\right) < \infty$*?*

Conjecture A.2.2. *Does* $\lim\limits_{n \to \infty} \sum\limits_{(a,b,c) \in X_n} \frac{g(a,b,c)-a-b-c}{\sqrt{abc}}$ *exist and is finite?*

In [208], Hujter posed the following problem (*cf.* Theorem 3.6.2).

Problem A.2.3 *Compute the exact value for* $\liminf\limits_{\frac{ab}{c} \to \infty} \frac{g(a,b,c)}{\sqrt{abc}}$.

After the general expresion for $g(a_1, a_2, a_3)$ given in Theorem 2.2.3, an appealing question is to find a similar formula for $n \geq 4$.

Problem A.2.4 *Is there an explicit formula for* $g(a_1, a_2, a_3, a_4)$*?*

As Hujter remarks, Boros' technique, via subadditive functions (*cf.* Theorem 3.1.20), seems to be very useful in order to obtain new results concerning **FP**.

Problem A.2.5 *Develope the subadditive approach in relation to* **FP**.

In [32], Beck and Robins generalized **FP** as follows. An integer m is said *k-representable* if $d(m; a_1, \ldots, a_n) = k$, that is, m can be represented in exactly k ways; see [343, 341, 450] for a closely related problem. Let $g_k(a_1, \ldots, a_n)$ be the largest no k-representable integer (it is easy to see that for each k, eventually all integers are representable at least k times). Thus, $g_0(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$. Beck and Robins found that $g_k(a_1, a_2) = (k+1)a_1 a_2 - a_1 - a_2$. Their proof for the latter is by induction and based in the fact that $d(m + a_1a_2; a_1, a_2) = d(m; a_1, a_2) + 1$. They proposed the following problem.

Problem A.2.6 *Investigate $g_k(a_1, \ldots, a_n)$ when $n \geq 3$.*

Supported by many computations, Beihoffer *et al.* [37] presented the following conjecture

Conjecture A.2.7. *Let $A = \{a_1, \ldots, a_n\}$. Then the expected value of $g(A)$ is a small constant multiple of $\left(\frac{1}{2}n! \prod A\right)^{\frac{1}{n-1}} - \sum A$.*

In [19, Problem 2003–5], Arnold has also posed a closely related question. In [17], Arnold proposed to investigate the *asymptotical* behaviour of what it was called the *derivate*

Problem A.2.8 *What is the behaviour of $\Delta(m; a_1, a_2, a_3) = d(m + 1; a_1, a_2, a_3) - d(m; a_1, a_2, a_3)$?*

A.3 Denumerant

Problem A.3.1 *Is computing $d(m; a_1, \ldots, a_n)$ $\#\mathcal{P}$-complete?*

Note that $d(m; a_1, a_2, a_3)$ is known if $m \geq P_3$ (*cf.* Theorem 4.5.1 part b) and if $P_3 - S_3 + 1 \leq m < P_3$ (*cf.* Corollary 4.5.3). In [408], Sertöz and Özlük proposd the following problem.

Problem A.3.2 *Find a formula for $d(m; a_1, a_2, a_3)$ when $m < P_3 - S_3 + 1$.*

The following question turned up in [341] while investigating **FP**.

Problem A.3.3 *Let p and q be prime numbers. Is there a polynomial time algorithm that finds $d(m; p, p^2, \ldots, p^n, q, q^2, \ldots, q^n)$?*

This does not seem to be immediate even if we insist that $p = 3$ and $q = 5$.

A.4 $N(a_1, \ldots, a_n)$

Problem A.4.1 *Is computing $N(a_1, \ldots, a_n)$ $\mathcal{NP}$-complete?*

Or perhaps,

Problem A.4.2 *Is computing $N(a_1, \ldots, a_n)$ $\#\mathcal{P}$-complete?*

Selmer [392] has shown that the number $N(a_1, \ldots, a_n)$ can be increased by the removal of some a_is.

Problem A.4.3 *Given integers $a_1, \ldots, a_n$, what is the influence of a new (independent) element a_{n+1} in $N(a_1, \ldots, a_n)$?*

Wilf [480] proposed the following two problems.

Problem A.4.4 *Is it true that for fixed n the fraction $N(a_1, \ldots, a_n)/(g(a_1, \ldots, a_n) + 1) \leq 1 - \frac{1}{n}$ with equality only for $(a_1, \ldots, a_n) = (n, n+1, \ldots, 2n-1)$?*

Frőberg *et al.* [149] remarked that Lemmas 7.2.4 and 7.2.6 show that there is always equality in Wilf's question if $n = 2$. They also showed that Wilf's question can be answered positively in the case $n = 3$ by proving that the type of any semigroup $S =< s_1, s_2, s_3 >$ is at most two. Finally, they also showed that there is always equality for all semigroups $S =< k, mk+1, mk+2, \ldots, (m+1)k-1 >$ since $g(S) = mk - 1$, $N(S) = m$ and the number of generators is k. In [121] Dobbs and Matthews answered Problem A.4.4 when the semigroup $< a_1, \ldots, a_n >$ is symmetric, pseudo-symmetric or of maximal embedding dimension.

Problem A.4.5 *Let $q(n)$ be the number of semigroups having the same Frobenius number. What is the order of magnitude of $q(n)$ for $n \to \infty$?*

In relation to ProblemA.4.5, Backelin [21] posed the following question.

Problem A.4.6 *Find explicit formulas or good upper bounds for the quantities*

$$K(n, k, q) = |\{X \subseteq \{1, \ldots, n\} : |X| = k,\ |2X| \leq q\}|.$$

Backelin [21] remarked that for $q < 3k - 3$ fairly good results for Problem A.4.6 can be obtained by means of [145, Theorem 1.9] and that [145, Theorem 2.8]may also yield good results in general.

A.5 Gaps

Recall that $l_1, < \cdots < l_{N(S)}$ denotes the gaps (ordered increasingly) of the semigroup S where $N(S) = \#(\mathbb{N} \setminus S)$ is the genus of S; see Section 7.1.

Problem A.5.1 *Let $S =< s_1, \ldots, s_n >$. Investigate the behaviour of the l_is.*

In particular,

Problem A.5.2 *Is there an explicit formula that computes l_i for each $1 \leq i \leq N(S)$ when $S =< s_1, s_2 >$?*

We know that $l_{N(S)} = s_1s_2 - s_1 - s_2$ but, for general n, the search for such a formula seems to be a difficult task. This is not very surprising since computing the i-th gap of a semigroup is as hard as to calculate the Frobenius number. Indeed, for calculating the i-th gap of a semigroup S we may calculate $g^{N(S)-i}(S) = g(S \cup \{g^{N(S)}(S)\} \cup \cdots \cup \{g^{N(S)-i+1}(S)\})$ where $g^{N(S)}(S) = g(S)$.

May be a formula for gaps in some special sequences could be accesible.

Problem A.5.3 *Let $S =< a, a+d, \ldots, a+sd >$ with $s \geq 1$ and $(a,d) = 1$. Is there a formula that computes l_i for each $1 \leq i \leq N(S)$?*

This problem is solved [345] in the simplest case when $s = 1$. Notice that Theorem 3.3.2 gives a positive answer when $i = N(S)$ for any integers a, s and d.

Recall that $n(\rho_i)$ denotes the number of gaps smaller than ρ_i where ρ_i denotes the i-th non-gap of S.

Problem A.5.4 *Is $n(\rho_i)$ computable in polynomial time?*

A.6 Miscellaneous

The major unsolved analytic problem of Shell-sort is to determine the asymptotic behaviour of its average running time. Discovering increment sequences for Shell-sort with better perfomance than those previously known is always a valuable practical result because the new sequence can be immediately used with only a one line change in the Shell-sort routine.

Problem A.6.1 *Investigate further increment sequences for the Shell-sort method.*

Let $I(a_1, \ldots, a_n)$ be the greatest number of elements that can be omitted without altering $g(a_1, \ldots, a_n)$; see Section 3.5.

Problem A.6.2 *What is the behaviour of $I(a_1, \ldots, a_n)$?*

Recall that $\Omega_k(m; a_1, \ldots, a_n)$ (respectively $N_k(m; a_1, \ldots, a_n)$) is the number of k-omitted natural non-negative numbers and (respectively the largest of the k-omitted numbers); see Section 6.2.

Problem A.6.3 Study the functions $\Omega_k(m; a_1, \ldots, a_n)$ and $N_k(m; a_1, \ldots, a_n)$ in the case $n \geq 3$.

Skupień has posed the following problem.

Problem A.6.4 *Characterize the sequences $a_1, \ldots, a_n$ and the integers m such that $\Omega_k(m; a_1, \ldots, a_n) > \frac{k(m;a_1,\ldots,a_n)}{2}$ for all $k \in \{0, \ldots, m-1\}$.*

While investigated **FP**, Norman [314] came up with the following conjecture.

Conjecture A.6.5. *Let $M = \{0, 1, \ldots, m-1\}$, let $S \subseteq M$ with $0 \in S$ and let $B = \{b_1, \ldots, b_k\} \subset M$ with $b_i \neq 0$ for all i and $(m, d) = 1$ where $(b_1, \ldots, b_k) = d$. Let $U = S + B$ (addition modulo m). Then, the following two conditions are sufficient for the inequality $|U| - |S| \geq k$:*

(i) $|S| \leq m - k$ and
(ii) for any positive integers p and q such that $p < q < k$, $\frac{pm}{q} \notin B$.

Furthermore, if the second condition is satisfied and the first is not then $U = M$.

Recall that $N(t_1, \ldots, t_k, q)$ is the least integer such that if $n > N(t_1, \ldots, t_k, q)$ and $(t_1, \ldots, t_k)$ divides n then the vector space $V_n(q)$ admits a partition of type $\{t_1, \ldots, t_k\}$. In [190], Heden conjecture the following bound for $N(t_1, \ldots, t_k, q)$.

Conjecture A.6.6. *$N(t_1, \ldots, t_k, q) < 2t_k$.*

The following question turned up in [341] while investigating Problem A.3.3.

Problem A.6.7 *Investigate the complexity of the following question. Given integer z, are there integers x and y such that $x^2 + y^2 = z$?*

Let I_S be the *toric ideal* of the semigroup S and let $\alpha(I)$ denote the minimal number of generators of ideal I. Bresinsky [61, page 218] raised the following problem.

Problem A.6.8 *Let S be a symmetric numerical semigroup. Does there exist an upper bound for $\alpha(I_S)$ which depends only on the minimal number of generators of S?*

If $n = 2$ then $\alpha(I_S) = 1$ because I_S is a principal ideal in $k[X_1, X_2]$. If $n = 3$ Herzog [191] proved that $\alpha(I_S) = 2$. If $n = 4$, Bresinsky

[61] proved that $\alpha(I_S) \leq 5$. If $n = 5$, Bresinsky [63] proved that $\alpha(I_S) \leq 13$ under certain conditions; see [81] and [76, Section 5.1] for further details.

Guy [176] has posed several problems concerning the Sylver Coinage game. Notice that an answer to Problem A.4.3 may yield to a winning strategy for the Sylver Coinage game; see Section 5.6.1.

Problem A.6.9 *Investigate further winning strategies for the Sylver coinage game.*

Problem A.6.10 *Generalize the results of the jugs problem when there are four or more jugs.*

A.6.1 Erdős' problems

In a rich and fruitful mailing (in relation to **FP**) with Chrząstowski-Wachtel, Erdős posed the following questions.

Problem A.6.11 *What is the smallest integer $f(n)$ for which one can divide the integers $1 \leq t \leq n$ into $f(n)$ classes so that n should not be the sum of a subset of the elements of the same class (i.e. $n \neq \sum x_i u_i$ with $x_i = 0$ or 1 and $\{u_i\}$ are in the same class)?*

Problem A.6.12 *Is there a non-trivial lower bound for $f(n)$? perhaps, $f(n) > n^{\frac{1}{3}-\epsilon}$?*

Problem A.6.13 *Is it true that for every integer k there is a integer $h(k)$ so that every prime $p > h(k)$ if $a_1, \ldots, a_k$ all less that p are any set of k integers one can always divide them into two classes so that p is not the sum of a subset of the numbers of the same class?*

Problem A.6.14 [2]*Let $a_1 < a_2 < \cdots < a_{n+1} \leq 2n$ be $n+1$ integers less than or equal to $2n$. Trivially, two of them are consecutive and thus relatively prime. Is it true that there are $(a_i, a_j) = 1$ where the smallest is less or equals to n? Also, is $(a_i, a_j) = 1$ with $a_j - a_i > n - \sigma(n)$ solvable? i.e. are there two of them which are far apart and are realtively prime? If $n - \sigma(n)|n$ is not true a weaker inequality might also be of interest.*

[2] In one of the letters, Erdős wrote

> 'this is a very annoying elementary problem of mine which I cannot solve'.

This page intentionally left blank

Appendix B

B.1 Computational complexity aspects

We outline some relevant notions of computational complexity, for a detailed presentation see [154]. *Decision* problems are problems having only two possible answers: either *yes* or *no*. Several well-known computational problems are decision problems. People are interested in classifying decision problems according to their complexity. We shall denote by $\mathcal{P}$ the class of decision problems that can be solved by a polynomial time algorithm. The class $\mathcal{P}$ can be defined very precisely in terms of *Turing machines*. Informally, $\mathcal{P}$ is the class of relatively easy decision problems, those for which an *efficient* algorithm exists.

We shall now introduce $\mathcal{NP}$. For a problem to be in $\mathcal{NP}$, we do not require that every instance can be answered in polynomial time by an algorithm. We simply require that, if x is a *yes* instance of a problem, then there exists a *concise* (that is, of length bounded by a polynomial in the size of x) *certificate* for x that can be checked in polynomial time for validity.

We can formalize this idea as follows: Let Σ be a fixed finite alphabet and # be a *distinguished symbol* in Σ (the symbol # marks the end of the input and the beginning of a certificate). If x is a string of symbol from Σ, then its length (the number of symbols that x contains) is denoted by $|x|$. We say that a decision problem Π is in the class $\mathcal{NP}$ if there exists a polynomial $p(n)$ and an algorithm A (the *certificate checking algorithm*) such that the following is true. The string x is a *yes* instance of Π if and only if there exists a string of symbols in Σ, $c(x)$ (the *certificate*) with the property that A, if supplied with the input $x\#c(x)$, reaches the answer *yes* after at most $p(|x|)$ steps.

We say that a decision problem Π_1 *polynomially reduces* to another decision problem Π_2 if, given any string x, we can construct a string y within polynomial time (in $|x|$) such that x is a *yes* instance of Π_1

if and only if y is a *yes* instance of Π_2. A decision problem $\Pi \in \mathcal{NP}$ is said to be *$\mathcal{NP}$-complete* if all other problems in $\mathcal{NP}$ polynomially reduce to Π.

Suppose Π_1 and Π_2 are two problems, a *polynomial time Turing reduction* from Π_1 to Π_2 is an algorithm A that solves Π_1 by using a hypothetical subroutine A' for solving Π_2, such that, if A' were a polynomial time algorithm for Π_2 then A would be a polynomial time algorithm for Π_1. It is said that Π_1 can be *Turing reduced* to Π_2. A problem Π_1 is called (Turing) *$\mathcal{NP}$-hard* if there is an $\mathcal{NP}$-complete decision problem Π_2 such that Π_2 can be Turing reduced to Π_1.

B.2 Graph theory aspects

We describe some graph theory terminology used in this book. We refer the reader to [54] for further details. A *finite graph* is a triple $G(V, E, \phi)$, where V is a finite set of *vertices*, E is a finite set of *edges* and ϕ is a function that assigns to each edge e a 2-element multiset of vertices. Thus, $\phi : E \to \left(\binom{V}{2}\right)$. An edge e is called a *loop* if $e = \{v, v\}$ for some $v \in V$. Two vertices u and v are said to be *adjacent* if there is an edge e such that $e = \{u, v\}$. Otherwise, they are called *non-adjacent*. A set $U \subseteq V$ is a *stable set* if they are pairwise non-adjacent. A graph is *bipartite* if its set of vertices can be partitioned into two stables sets. If there exist vertices $v_1, \ldots, v_k$ such that $(s, v_1), (v_1, v_2), \ldots, (v_k, t)$ are edges of the graph then s is said to be connected to t by a *path*. A graph is *connected* if any two distinct vertices are joined by a path. A *cycle* is a path that begins and ends with the same vertex (edges and vertices may be repeated). An *elementary* cycle is a cycle that repeats neither edges nor vertices. A graph G is said to be *Hamiltonian* if it has an elementary cycle containing all the vertices of G.

A *directed* graph is defined analogously to a graph, except now $\phi : E \to V \times V$, that is, an edge consist of an *ordered* pair (i, j) of vertices. A graph G is *strongly connected* if for every pair of vertices s and t there is a directed path connecting s to t.

B.3 Modules, resolutions and Hilbert series

We outline some algebraic geometry notions needed in Section 4.6. We refer the reader to [99, 258, 434] for a more detailed presentation.

A *module* M over a ring R is a set together with a binary operation and an operation of R on M satisfying the following properties.

- M is an abelian group under addition.
- For all $a \in R$ an all $f, g \in M$, $a(f+g) = af + ag$.
- For all $a, b \in R$ an all $f \in M$, $(a+b)f = af + bf$.
- For all $a, b \in R$ an all $f \in M$, $(ab)f = a(bf)$.
- If 1 is the multiplicative identity in R, $1f = f$ for all $f \in M$.

Given a ring R, a simple check shows that R is a module over itself. Also, R^m is an R-module, with the addition and scalar multiplication operations being the componentwise ones.

M is said to be a *free module* if it has a module basis (that is, a generating set that is R-linearly independent). An R-module M is said to be *projective* if there is an R-module N such that $M \bigoplus N$ (the direct sum $M \bigoplus N$ is the set of all ordered pairs (f, g) with $f \in M$ and $g \in N$) is a free module.

Let $R = k[X_1, \ldots, X_n]$ be the polynomial ring in n variables, over the field k where each X_i has degree 1. R is a graded algebra and we can express it as

$$R = \bigoplus_{i=0}^{\infty} R_i,$$

where the R_is are k-vector spaces of homogeneous polynomials of degree i, and $R_i R_j \subset R_{i+j}$.

A *graded module* over a graded algebra R is a module M with a family of subgroups $M_t : t \in \mathbb{Z}$ of the additive group of M. The elements M_t must satisfy

(a) $M = \bigoplus_{i=0}^{\infty} M_i$,

and

(b) $R_s M_t \subset M_{s+t}$ for all $s \geq 0$ and all $t \in \mathbb{Z}$.

The elements of M_t are called *homogeneous of degree* t. Notice that, by definition, each M_t is a k-vector subspace of M and that if M is finitely generated then the M_t are finite-dimensional over k. The free modules R^m are graded modules since by defining $(R^m)_t = (R_t)^m$ we obtain a grading, that is the elements of $(R^m)_t$ are the m-tuples whose entries are homogeneous elements of degree t. If M is a finitely generated graded R-module and $s \in \mathbb{N}$, we define $M(d)$ as the *regrading* of M

obtained by a *shift* of the graduation of M, more precisely,

$$M(d) = \bigoplus_{i=0}^{\infty} M(d)_i, \tag{B.1}$$

where $M(d)_i = M_{d+i}$, we set $M_i = 0$ if $i < 0$. It turns out that $M(d)$ is also a graded R-module. The graded module $R(d)^m$ has the same standard basis as R^m, but since $R(d)_{-d} = R_0$, the standard basis of $R^m(d)$ is homogeneous of degree $-d$. The graded modules $R(d)^m$ are called *shifted* or *twisted* graded free modules over R. We have that if $d_1, \ldots, d_m$ are integers then

$$M = R(d_1) \bigoplus R(d_2) \bigoplus \cdots \bigoplus R(d_m)$$

is a graded free module where the basis elements are homogeneous of degree $-d_i$, $1 \leq i \leq m$. If M and N are graded R-modules then

$$\psi : M \to N$$

is said to be a *homogeneous map* (of degree d) if ψ is an R linear map (that is, $\psi(af + g) = a\psi(f) + \psi(g)$ for all $a \in R$ and all $f, g \in M$) and $\psi(M_i) \subset N_{i+d}$ for all i. Observe that the kernel and image of a homogeneous map are also graded. Suppose that $M = \langle f_1, \ldots, f_m \rangle$ is a graded R-module where the polynomials f_i are homogeneous of degree d_i. Then the following map is homogenous of degree zero

$$\phi : R(-d_1) \bigoplus R(-d_2) \bigoplus \cdots \bigoplus R(-d_m) \to M,$$

where $\phi(e_i) = f_i$, with e_i the standard basis elements of R^m, but $deg(e_i) = d_i$.

A *graded resolution* of M is a resolution of the form

$$\cdots \longrightarrow F_2 \xrightarrow{\psi_2} F_1 \xrightarrow{\psi_1} F_0 \xrightarrow{\psi_0} M \longrightarrow 0,$$

where each F_i is a twisted free graded R-module (that is, sums of modules of the form $R(d)$ for various integers d) and the maps are all homogeneous map of degree zero. In this case the ψ_is are given by certain *graded matrices* (see [99, Chapter 6] for a detailed definition of these matrices).

Theorem B.3.1 *[196]* (**Graded Hilbert Syzygy Theorem**) *Let $R = k[X_1, \ldots, X_n]$. Then, every finitely generated graded R-module has a finite graded resolution of length at most n.*

Let M be a finite generated module over $R = k[X_1, \ldots, X_n]$, then the *Hilbert function*, denoted by $H_M(z)$ and the *Hilbert series*, denoted by $H(M, z)$, of M are defined by

$$H_M(z) = \dim_k(M_z) \text{ and } H(M, z) = \sum_{t=0}^{\infty} H_M(t) z^t,$$

where dim_k means dimension as a vector space over k.

It is known that if $M(d)$ is the twist defined in eqn (B.1) then

$$H_{M(d)}(t) = H_M(t + d).$$

The latter is used to prove the following important classical result regarding graded resolution.

Theorem B.3.2 *[196] Let $R = k[X_1, \ldots, X_n]$ and let M be a graded R-module. For any graded resolution of M of the form*

$$0 \longrightarrow F_m \longrightarrow F_{m-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

we have

$$H_M(z) = \sum_{j=0}^{m} (-1)^j H_{F_j}(z).$$

Moreover,

$$H(M, z) = \sum_{j=0}^{m} (-1)^j H(F_j, z).$$

The *toric ideal* of the semigroup $S = < s_1, \ldots, s_n >$ is the kernel of the homomorphism ϕ of semigroup algebras from $k[X_1, \ldots, X_n]$ to the polynomial ring $k[z^{s_1}, \ldots, z^{s_n}]$ induced by S, that is, $\phi(X_i) = z^{s_i}$, where I denotes the kernel of the map ϕ given by $X_i \to z^{s_i}$ for each i.

B.4 Shell-sort method

One classical sorting algorithm, the perfomance of which remains unanalysed in most cases, is the *Shell-sort* proposed by Shell [414]. Shell-sort is simple to code and can efficiently take advantage of parallel supercomputer architectures with little extra effort. These considerations make Shell-sort an attractive algorithm.

Recall that Shell-sort performs an h_k-sort, an h_{k-1}-sort, an so on until an $h_1 = 1$-sort; see Section 8.1. The running time of the algorithm is clearly quite dependent on the specific increment sequence $h_1, \ldots, h_k$ that is used. Unfortunately, little is known on how to pick the 'best' increment sequence. In the table some sequences are listed that have been suggested for use.

Shell	$1, 2, 4, 8, \ldots, 2^k, \ldots$
Hibbard	$1, 3, 7, 15, \ldots, 2^k - 1, \ldots$
Papernov–Stasevich	$1, 3, 5, 9, \ldots, 2^k + 1, \ldots$
Knuth	$1, 4, 13, 40, \ldots, \frac{1}{2}(3^k - 1), \ldots$

If $k = 1$, then Shell-sort is equivalent to *insertion sort*, an algorithm whose perfomance is well understood. For insertion sort, the running time is known to be proportional to the number of *inversions* in the input (each element must move past the elements that are greater than it to the left). In this case, the worst-case running time is quadratic; see [246]. For $k > 1$, the running time of Shell-sort is known to be $O(N^{3/2})$ where N is the number of elements of the file (on the average and in the worst case) for the special case where each increment divides the previous increment; see [414]. At the other end of the spectrum, Pratt [336] gave a set of increments for which the running time is $O(N \log^2 N)$. Although the asymptotic growth of the average case running time of Shell-sort is unknown for the types of increment sequence used in practice, it appears to be considerably less than $O(N \log^2 N)$ (Gonnet [163] conjectured that the real value is $O(N \log N \log \log N)$).

Empirical tests indicate that there might exist increment sequences for which the average running time is $O(N \log N)$; see [119]. Thus, the study of increment sequences for Shell-sort is also important because of the potential for a simple constructive proof of the existence of an $O(N \log N)$ *sorting network*. The existence of such a network (with depth $O(\log N)$) was presented by Ajtai *et al.* [6] but their construction is hardly practical. Further refinements have been made by Leighton [263], but these networks are still far more complex than a Shell-sort network would be.

Finally, let us mention that Yao [484] has analysed the average behaviour of Shell-sort in the general three-pass case when the increments are $(h, g, 1)$. The most interesting part of his analysis dealt with the third pass, where the running time is $O(N)$ plus a term proportional to the average number of inversions that remain after a random permutation that has been h-sorted and g-sorted.

B.5 Bernoulli numbers

Jakob Bernoulli (1654–1705) discovered a curious relationship while working out the formulas for sums of m-th powers. Define $S_m(n) =$

$1^m + 2^m + \cdots + (n-1)^m$. By the binomial theorem, we have

$$(k+1)^{m+1} - k^{m+1} = 1 + \binom{m+1}{1}k + \binom{m+1}{2}k^2 + \cdots + \binom{m+1}{m}k^m,$$

and by substituting $k = 0, 1, \ldots, n-1$ and adding, we have

$$n^m + 1 = n + \binom{m+1}{1}S_1(n) + \binom{m+1}{2}S_2(n) + \cdots + \binom{m+1}{m}S_m(n). \tag{B.2}$$

Thus, one can have a formula for $S_m(n)$ if formulas for $S_1(n), \ldots, S_{m-1}(n)$ are known. Bernoulli observed that $S_m(n)$ is a polynomial of degree $m+1$ in n with leading term $\frac{n^{m+1}}{m+1}$ (this follows by induction from eqn (B.2)). One can see also that the value of the constant term is always zero (the coefficient values for the other terms are less obvious). Bernoulli empirically discovered that

$$\begin{aligned} S_m(n) &= \frac{1}{m+1}\left(B_0 n^{m+1} + \binom{m+1}{1}B_1 n^m + \cdots + \binom{m+1}{m}B_m n\right) \\ &= \frac{1}{m+1}\sum_{k=0}^{m}\binom{m+1}{k}B_k n^{m+1-k}. \end{aligned}$$

The *Bernoulli numbers* $B_0, B_1, B_2, \ldots$ are defined inductively as follows. $B_0 = 1$ and

$$(m+1)B_m = -\sum_{k=0}^{m-1}\binom{m+1}{k}B_k.$$

The first Bernoulli numbers turn out to be

n	0	1	2	3	4	5	6	7	8	9	10	11	12
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$

With this result in hand, Bernoulli was able to answer the question of evaluating[1] the sums $S_m(n)$. Bernoulli numbers appear in many different areas. In 1960, Vandiver [462] published a survey article in which he remarks that some 1500 papers on these numbers had been

[1] Bernoulli proudly remarks (in his book *Ars Conjectandi* (1713)) that in less than a half of a quarter of an hour he was able to sum the tenth powers of the first thousand integers [429].

published. This suggests how important and fascinating this sequence of numbers are. We refer the reader to [168] for further discussions on Bernoulli numbers. Most of the material presented in this section is based on [215, Chapter 15].

B.6 Irreducible and primitive matrices

A *permutation* matrix is a square matrix that in each row and each column has some one entry, all other zero. An $n \times n$ matrix B is called *reducible* if there exists an $n \times n$ *permutation* matrix P such that

$$PBP^T = \begin{bmatrix} B_{1,1} & B_{1,2} \\ 0 & B_{2,2} \end{bmatrix},$$

where $B_{1,1}$ is an $r \times r$ submatrix and $B_{2,2}$ is an $(n-r)\times(n-r)$ submatrix. If no such permutation matrix exists, then B is called *irreducible*[2].

One motivation to study reducible matrices is the following. To solve the matrix equation $\bar{A}\mathbf{x} = \mathbf{k}$, where $\bar{A} = PAP^T$ is the partitioned matrix as above, then we can partition the vectors $\mathbf{x}$ and $\mathbf{k}$ similarly so that the matrix equation $\bar{A}\mathbf{x} = \mathbf{k}$ can be written as

$$\begin{aligned} A_{1,1}\mathbf{x_1} + A_{1,2}\mathbf{x_2} &= \mathbf{k_1} \\ A_{2,2}\mathbf{x_2} &= \mathbf{k_2}. \end{aligned}$$

Thus, by solving the second equation for $\mathbf{x_2}$ and with this known solution for $\mathbf{x_2}$ solving the first equation for $\mathbf{x_1}$, we have *reduced* the solution of the original matrix equation to the solution of two lower-order matrix equations.

The geometrical interpretation of the concept of irreducibility by means of graph theory is quite useful. Let $G(B)$ be the associated directed graph to matrix B as defined in Section 1.2.2.

Theorem B.6.1 *An $n \times n$ complex matrix B is irreducible if and only if its associated directed graph $G(B)$ is strongly connected.*

Example B.6.2 Let $B_1 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$ and $B_2 = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}$. The corresponding graphs are shown in Fig. B.1.

[2] The term *irreducible* (*unzerlegbar*) was introduced by Frobenius [147]; it is also called *irreduced* and *indecomposable* in the literature; see [361].

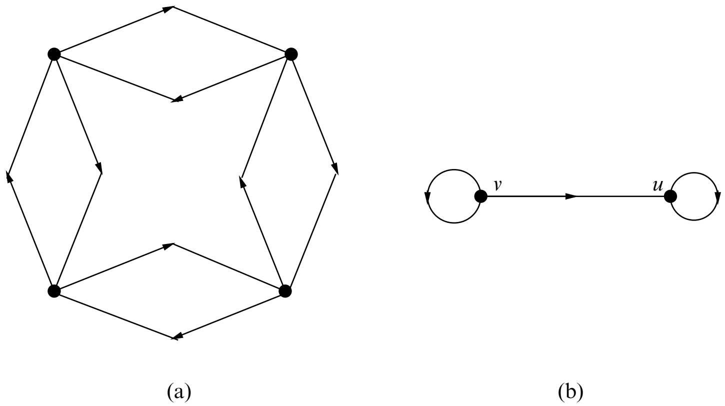

Figure B.1: (a) $G(B_1)$ and (b) $G(B_2)$.

By inspection, we can see that $G(B_1)$ is strongly connected but $G(B_2)$ is not (there exists no path from vertex u to vertex v).

Now, suppose that $B^k = (b_{ij}^{(k)})$. Since

$$(b_{ij}^{(k)}) = \sum_{1\leq i_i,\ldots,i_{k-1}\leq m} b_{ri_1}b_{i_1i_2}\cdots b_{i_{m-1}s}, \quad m \geq 2,$$

then $(b_{ij}^{(k)}) \neq 0$ if and only if there is a path of $G(B)$ of length m connecting r to s. With this in mind, the following fundamental lemma is immediate.

An irreducible, non-negative matrix B is *primitive* if $B^t > 0$ for some integer $t \geq 1$ (and hence, it can be shown, for all integers greater than t). The least integer $\gamma(B)$ such that $B^{\gamma(B)} > 0$ is called the *index of primitivity* of B.

Lemma B.6.3 *[187] If B is primitive then $\gamma(B)$ is the least integer such that for all $m \geq \gamma(B)$ there is a path of length m connecting two arbitrary (not necessarily distinct) vertices of $G(B)$.*

The above lemma yields the following well-known result.

Lemma B.6.4 *[361, 465] If $B \geq 0$ is irreducible then B is primitive if and only if the lengths of all circuits of $G(B)$ are relatively prime.*

Heap and Lynn [187] have proved the following fact.

Lemma B.6.5 *[187] Let B be a primitive matrix and let $0 < a_1 < \ldots < a_k$ be the distinct lengths of all* elementary *circuits of $G(B)$. Then, the length L of any circuit of $G(B)$ can be expressed in the form $L = \sum_{i=1}^{n} x_i a_i$ with $x_i \geq 0$ for all i.*

Proof. Let $C = \{x_{i_1}, \ldots, x_{i_c}\}$ denote any circuit, not necessarily elementary of $G(B)$ and let c be its length. Let $q_1, \ldots, q_k$ be the set of all distinct lengths of all elementary circuits of $G(B)$. We claim that $c = \sum_{i=1}^{k} x_i q_i$ with $x_i \geq 0$. Indeed, if C is elementary, this is obvious ($c = q_i$ for some i). Otherwise, we have that $x_{i_j} = x_{i_l}$ for some $j \neq l$, $l \geq 1$. Thus, C can be decomposed into two circuits, say C_1 and C_2, whose lengths add up to c. If C_1 and C_2 are elementary circuits then we are done; otherwise, we may decompose the appropiate one (or both) in two circuits, and so on.

Since c is finite, C can be decomposed into a finite number of elementary circuits whose lengths add up to c and the claim follows and so does the result. □

B.6.1 Upper bounds of index of primitivity

Let $B = (b_{ij})$ be a real $(m \times m)$ matrix. Let $G(B)$ be the directed graph, associated to B, having vertex set $\{1, \ldots, m\}$ and directed edge from i to j if and only if $b_{ij} \neq 0$. The well-known Dulmage–Mendelsohn [122] bound states

Theorem B.6.6 *[122] Let A be an $(n \times n)$-matrix. Then,*

$$\gamma(A) \leq n + s(n-2),$$

where s is the girth of the directed graph $G(A)$ associated to A.

In [415], Shen improved the above upper bound

Theorem B.6.7 *[415]*

$$\gamma(A) \leq d + 1 + s(d-1),$$

where d is the diameter of the adjacency digraph $G(A)$ associated to matrix A.

In [416], Shen presented a much shorter proof of Theorem B.6.7. Hartwig and Neumann [186] conjectured that $\gamma(A) \leq (m-1)^2 + 1$ and that $\gamma(A) \leq d^2 + 1$, where m is the degree of the *minimal* polynomial of A and d is the diameter of the directed graph $G(A)$. It is known that the latter is stronger than the former because $d \leq m-1$. In [417, 418], Shen has proved both conjectures.

Theorem B.6.8 *[417, 418]*

$$\gamma(A) \leq (m-1)^2 + 1 \textit{ and } \gamma(A) \leq d^2 + 1.$$

B.6.2 Computation of index of primitivity

One may compute the index of primitivity of a matrix A as follows. Let $\mathcal{B}(A)$ denote the associated Boolean matrix of a non-negative matrix A, that is, the matrix whose elements are one if the corresponsing elements of A are positive, and zero otherwise. It can be shown that, given a non-negative matrix A,

$$\mathcal{B}(A^{r+s}) = \mathcal{B}(A^r)\mathcal{B}(A^s),$$

where $\mathcal{B}\,(A^r)\mathcal{B}(A^s)$ denotes the Boolean product of the matrices $\mathcal{B}(A^r)$ and $\mathcal{B}(A^s)$. For the definition of this and other concepts in connection to Boolean matrices, the reader is referred to [475]. The $\gamma(A)$ is the smallest integer for which $\mathcal{B}(A^{\gamma(A)}) > 0$. The procedure for obtaining $\gamma(A)$ is to form and store the Boolean matrices $\mathcal{B}(A), \mathcal{B}(A^2), \mathcal{B}(A^4), \ldots, \mathcal{B}(A^{2^r})$, until either the last formed matrix is positive or else r is such that 2^{r+1} is known to be greater than an upper bound for $\gamma(A)$. In fact, using the results in [187] one may verify that, for the Frobenius graph defined in Section 1.2.2,

$$\gamma(B) \leq (n+1)(a_n - a_{n-1} - 1) + a_1 - 1(a_n - 1) - \sum_{i=1}^{n} a_i.$$

It is a simple procedure to evaluate the smallest integer m for which $\mathcal{B}(A^m) > 0$ by using a binary search on the previously computed matrices $\mathcal{B}(A^{2^s})$ with $1 \leq s \leq r$. Notice that this procedure does not imply a polynomial time algorithm since it may require an exponential number of matrix multiplications.

This page intentionally left blank

References

[1] K. Aardal and A.K. Lenstra, Hard equality constrained integer knapsacks, *Mathematics of Operat. Res.* **29**(3) (2004), 724–738.

[2] N. Abe, Characterizing PAC-learnability of semilinear set, *Inform. and Comp.* **116**(1) (1995), 81–102.

[3] N. Abe, Money changing problem is NP-Complete, *Technical Report MS-CIS-87-45, University of Pennsylvania*, June (1987).

[4] O. Achou, The number of feasible solutions to a Knapsack problem, *SIAM J. Appl. Math.* **27**(4) (1974), 606–610.

[5] G. Agnarsson, On the Sylvester denumerants for general restricted partitions, in the proceedings of the thirty-third southeastern international conference on combinatorics, graph theory and computing (Boca Raton, Florida, 2002) *Congr. Numer.* **154** (2002), 49–60.

[6] M. Ajtai, J. Komlós and E. Szmerédi, An $O(n \log n)$ sorting method, *Proceedings 15th Annual ACM Symposium of Theory of Computing*, Boston Mass., (1983).

[7] R. Alter and J.A. Barnett, A postage stamp problem, *Am. Math. Monthly* **87** (1980), 206–210.

[8] D.F. Anderson and J. Winner, Factorization in $K[\![S]\!]$, in Factorization in integral domains (Iowa City, 1996), *Lecture Notes in Pure and Appl. Math.*, **189**, Dekker, New York, (1997), 243–255.

[9] G. Angermüller, Die Wertehalbgruppe einer ebenen irreduziblen Kurven, *Math. Z.* **153** (1977), 267–282.

[10] M. Anshel, Vectors group and the equality problem for vector addition systems, *Math. Comp.* **32** (1978), 614–616.

[11] M. Anshel and D. Goldfeld, Applications of the Hardy-Ramanujan partition theory to linear Diophantine problems, *J. Ramanujan Math. Soc.* **3**(1) (1988), 97–110.

[12] M. Anshel and K. McAloon, Reducibilites among decision problems for HNN groups, vector addition systems and subsystems of Peano arithmetic, *Proc. Am. Math. Soc.* **89**(3) (1983), 425–429.

[13] R. Apéry, Sur les branches superlinéaires des courbes algébriques, *C.R. Acad. Sci. Paris* **222** (1946), 1198–1200.

[14] T.M. Apostol, Introduction to Analytic Number Theory, Undergraduate Texts in Mathematics, Springer-Verlag, New York, Heidelberg, (1976).

[15] E. Arbarello, M. Cornalba, P.A. Griffiths and J. Harris, Geometry of algebraic curves, **I** (Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]), **267** Springer-Verlag, New York, (1985).

[16] C. Arf, Une interprétation algébrique de la suite des ordres de multiplicité d'une branche algébrique, *Proc. London Math. Soc.* **50**(2) (1948), 256–287.

[17] V.I. Arnold, Weak asymptotics for the number of solutions of diophantine problems, *Functional Analysis and Its Applications* **33**(4) (1999), 292–293.

[18] V.I. Arnold, Frequent representations, *Moscow Math. J.* **3**(4) (2003), 1209–1221.

[19] V.I. Arnold, Problem No. 2003-5 in *Arnold's Problems*, Springer Berlin, New York (2004).

[20] M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass. (1969).

[21] J. Backelin, On the number of semigroups of natural numbers, *Math. Scand.* **66**(2) (1990), 197–215.

[22] A. Badra, Frobenius number of a linear diophantine equation, *Commutative ring theory and applications (Fez, 2001) Lecture Notes in Pure and Applied Mathematics*, **231**, Dekker, New York, (2003), 23–36.

[23] R.M. Barbosa, Partitions of numbers in allowed parts 1-3-4, 1-3-5 and 1-4-5, *Rev. Mat. Estatist.* **2** (1984), 43–49.

[24] V. Barucci, D.E. Doobs and M. Fontana, Maximality properties in numerical semigroups, with applications to one-dimensional analytically irreducible local domains, Proc. of the Conference 'Commutative Ring Theory', Fés, *Lectures Notes in Pure Applied Mathematics* **153**, M. Dekker, New York (1993), 13–25.

[25] V. Barucci, D.E. Doobs and M. Fontana, Maximality properties of one-dimensional analytically irreducible local domains, *Memoires Am. Math. Soc.* **125/598** (1997).

[26] A. Barvinok, Lattice points and lattice polytopes, in Handbook of Discrete and Computational Geometry (eds. J.E. Goodman

and J. O'Rourke), *CRC Press Ser. Discrete Math. Appl.*, CRC, Boca Raton, Florida, (1997), 133–152.

[27] A. Barvinok and J. Pommersheim, An algorithmic theory of lattice points in polyhedra, in New Perspectives in Algebraic Combinatorics (eds. L.J. Billera, A. Björner, C. Green, R.E. Simion and R.P. Stanley) *Math. Sci. Res. Inst. Publ.* **38** Cambridge University Press, (1999).

[28] A. Barvinok and K. Woods, Short rational generating functions for lattices point problems, *J. Am. Math. Soc.* **16**(4) (2003), 957–979.

[29] P.T. Bateman, Remark on a recent note on linear forms, *Am. Math. Month.* **65** (1958), 517–518.

[30] D. Bayer and M. Stillman, Computation of Hilbert functions, *J. Symb. Comput.* **14** (1992), 31–50.

[31] M. Beck, R. Diaz and S. Robins, The Frobenius problem, rational polytopes, and Fourier-Dedekind sums, *J. Number Theory*, **96**(1) (2002), 1–21.

[32] M. Beck and S. Robins, A formula related to the Frobenius problem in two dimensions, *Number Theory (New York) 2003* Springer New York, (2004), 17–23.

[33] M. Beck, I.M. Gessel and T. Komatsu, The polynomial part of a restricted partition function related to the Frobenius problem, *Electron. J. Combinatorics* **8**(1) (2001), Note 7, 5 pages.

[34] M. Beck, D. Einstein and S. Zacks, Some experimental results on the Frobenius problem, *Experiment. Math.* **12**(3) (2003), 263–269.

[35] M. Beck and S. Zacks, Refined upper bounds for the linear diophantine problem of Frobenius, *Adv. Appl. Math.* **32**(3) (2004), 454–467.

[36] A.G. Beged-Dov, Lower and upper bounds for the number of lattice points in a simplex, *SIAM J. Appl. Math.* **22**(1) (1972), 106–108.

[37] D.E. Beihoffer, J. Hendry, A. Nijenhuis and S. Wagon, Faster algorithms for Frobenius numbers, *Elect. J. Comb.*, to appear.

[38] E.T. Bell, Interpolated denumerants and Lambert series, *Am. J. Math.* **65** (1943), 382–386.

[39] E.T. Bell, Notes on denumerants, *J. Indian Math. Soc.* **3** (1938), 41–45.

[40] E.R. Berlekamp, J.C. Conway and R.K. Guy, *Winning Ways*, Academic Press, London, (1985), 575–606.

[41] J. Bertin and P. Carbonne, Sur la structure des semi-groupes d'entiers et application aux branches, *C.R. Acad. Sci. Paris*, Ser A **280** (1975), 1745–1748.

[42] J. Bertin and P. Carbonne, Semi-groupes d'entiers et application aux branches, *J. Algebra* **49** (1977), 81–95.

[43] A. Beutelspacher, Partitions of a finite vector space: An application of the Frobenius number in geometry, *Arch. Math.* **31**(2) (1978), 202–208.

[44] O. Beyer, The problem of Frobenius in three variables (in Norwegian), Thesis, University of Bergen, Dept. of Mathematics, (1976).

[45] G.R. Blakley, Combinatorial remarks on partitions of a multipartite number, *Duke Math. J.* **31** (1964), 335–340.

[46] G.R. Blakley, Algebra of formal power series, *Duke Math. J.* **31** (1964), 341–345.

[47] G.R. Blakley, Formal solution of nonlinear simultaneous equations: Reversion of series in several variables, *Duke Math. J.* **31** (1964), 347–357.

[48] J. Blażewicz, P. Formanowicz, M. Kasprzak, P. Schuurman and G. Woeginger, DNA sequencing, Eulerian graphs, and the exact perfect matching problem *Lectures Notes in Computer Sciences* **2573** (2002), 13–24.

[49] J. Blażewicz, P. Formanowicz, M. Kasprzak, W.T. Markiewicz and J. Weglarz, DNA sequencing with positive and negative errors, *J. Comput. Biol.* **6** (1999), 113–123.

[50] G. Blom and C.-E. Frőberg, On money changing, (Swedish), *Nordisk Matematisk Tidskrift. Normat* **10** (1962), 55–69.

[51] S. Böcker and Z. Lipták, The money changing problem revisited: computing the Frobenius number in time $O(ka_1)$, *Technical Report No. 2004–2, University of Bielefeld, Technical Faculty* (2004), 7 pages.

[52] B. Bojanok, The conductor of positive integers, a problem of Frobenius, *J. Math. Informat. Quart.* **7**(2) (1997), 58–61.

[53] P. Boldi, M. Santini and S. Vigna, Measuring with jugs, *Theor. Comput. Sci.* **282** (2002), 259–270.

[54] J.A. Bondy and U.S.R. Murty, *Graph Theory with Applications*, McMillan, London; North-Holland, New York, (1976).

[55] E. Boros, Subadditive approach to a linear diophantine problem of Frobenius, *Technical Report* **MO/38** Computer and Automation Inst., Hungarian Academy of Sciences, (1983).

[56] E. Boros, On a linear diophantine problem for geometrical type sequences, *Technical Report* Computer and Automation Inst., Hungarian Academy of Sciences, (1986); *Discrete Math.* **66** (1987), 27–33.

[57] A. Brauer, On a problem of partitions, *Am. J. Math.* **64** (1942), 299–312.

[58] A. Brauer and B.M. Seelbinder, On a problem of partitions II, *Am. J. Math.* **76** (1954), 343–346.

[59] A. Brauer and J.E. Shockley, On a problem of Frobenius, *J. Reine Angewandte Math.* **211** (1962), 215–220.

[60] H. Bresinsky, On prime ideals with generic zero $x_i = t^{n_i}$, *Proc. Am. Math. Soc.* **47**(2) (1975), 329–332.

[61] H. Bresinsky, Symmetric semigroups of integers generated by 4 elements, *Manuscripta Math.* **17** (1975), 205–219.

[62] H. Bresinsky, Monomial Gorenstein curves in A^4 as set theoretical complete intersection, *Manuscripta Math.* **27** (1979), 353–358.

[63] H. Bresinsky, Monomial Gorenstein idelas, *Manuscripta Math.* **29** (1979), 159–181.

[64] H. Bresinsky, Minimal free resolutions of monomial curves in P_k^3, *Linear Algebra Applic.* **59** (1984), 121–129.

[65] V.E. Brimkov, A polynomial algorithm for solving a large subclass of linear diophantine equations in nonnegative integers, *C.R. Acad. Bulgare Sci.* **41**(11) (1988), 33–35.

[66] V.E. Brimkov, Effective algorithms for solving a broad class of linear diophantine equations in nonnegative integers, *Mathematics and Mathematical Education (Bulgarian) (Albena, 1989)* Bulgar. Akad. Nauk., Sofia (1989), 241–246.

[67] V.E. Brimkov, On a Frobenius problem, *Mathematics and Mathematical Education* (Bulgarian) (Proceedings 19th Spring Conf. Sunny Beach/Bulg., 1990), Acad. Sci., Sofia (1990), 84–87.

[68] V.E. Brimkov and R.P. Bârneva, Gradient Elements of the Knapsack Polytope, *Calcolo* **38**(1) (2001), 49–66.

[69] V.E. Brimkov and R.P. Bârneva, Polynomial subclasses of the linear diophantine problems, Rapport 96/11, Université Louis Pasteur, Strasbourg, France (1996).

[70] M. Brion, Points entiers dans les polyèdres convexes, *Ann. Sci. École Normale Superieur* **21** (1988), 653–663.

[71] M. Brion and M. Vergne, Lattice points in simple polytopes, *J. Am. Math. Soc.* **10**(2) (1997), 371–392.

[72] M. Brion and M. Vergne, Residue formulae vector partition functions and lattice points in rational polytopes, *J. Am. Math. Soc.* **10**(4) (1997), 797–833.

[73] W. Brown and F. Curtis, Numerical semigroups of maximal and almost length, *Semigroup Forum* **42**(2) (1991), 219–235.

[74] T.C. Brown, W.-S. Chou and P.J. Shiue, On the partition function of a finite set, *Australasian J. Comb.*, 27(2003), 193–204.

[75] T.C. Brown and P.J. Shiue, A remark related to the Frobenius problem, *The Fibonacci Quarterly* **31**(1) (1993), 32–36.

[76] W. Bruns, J. Gubeladze and N.V. Trung, Problems and algorithms for affine semigroups, *Semigroup Forum* **64** (2002), 180–212.

[77] R.-O. Buchweitz, On Zariski's criterion for equisingularity and non-smoothable monomial curves, *Thèse, Paris VII*, (1981).

[78] R.-O. Buchweitz, Über deformationem monomialer kurvensingularitäten und Weierstrasspunkte auf Riemannschen flächen, *Thesis, Hannover*, (1976).

[79] J.S. Byrnes, On a partition problem of Frobenius, *J. Comb. Theor.* Ser.A **17** (1974), 162–166.

[80] J.S. Byrnes, A partition problem of Frobenius II, *Acta Arithmetica* **28** (1975), 81–87.

[81] A. Campillo and J.I. Farrán, Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models, *Finite Fields Appl.* **6**(1) (2000), 71–92.

[82] A. Campillo and C. Marijuan, Higher order relations for a numerical semigroup, *Séminaire de Théorie des Nombres, Bordeaux* **3** (1991), 249–260.

[83] A. Campillo and M.A. Revilla, Coin exchange algorithms and toric projective curves, *Commun. Algebras* **29**(7) (2001), 2985–2989.

[84] S.E. Cappell and J.L. Shaneson, Genera of algebraic varieties and counting of lattice points, *Bull. Am. Math. Soc.* **30** (1994), 62–69.

[85] A. Cayley, On a problem of double partitions, *Philos. Mag.* **XX** (1860), 337–341.

[86] K. Chandrasekhar, *Arithmetical Functions*, Springer-Verlag, New York, Berlin, (1970).

[87] G. Chartrand, R.J. Gould and S.F. Kapoor, On homogeneously traceable nonhamiltonian graphs, *Annals N.Y. Acad. Sci.* **319** (1979), 130–135.

[88] Z.-M. Chen, *Acta Sci. Sichuan Univ.* **1** (1956), 57–59.

[89] Z.-M. Chen, A theorem on linear form with integral coefficient (in Chinese), *Sichuan Daxue Xuebao* **1** (1956), 1–3.

[90] Z.-M. Chen, An algorithm to find M_3, (in Chinese), *J. Southwest Teachers College* **3** (1984), 2–8.

[91] Q.H. Chen and Y.J. Liu, A result on the Frobenius problem, (Chinese) *Fujian Shifan Daxue Xuebao Ziran Kexue Ban*, **11**(3) (1995), 33–37

[92] P. Chrząstowski-Wachtel, A bound for the diophantine problem of Frobenius, unpublished manuscript, (1992).

[93] P. Chrząstowski-Wachtel and M. Raczunas, Liveness of weighted circuits and the Diophantine problem of Frobenius; in Fundamentals of Computation Theory (Szeged, Hungary 1993), *Lecture Notes Comput. Sci.* **710** (1993), 171–180.

[94] J.H. Clarke, Conditions for the solutions of a linear diophantine equation, *The New Zealand Math. Mag.* **14** (1977), 45–47.

[95] V. Chvátal, Flip-flops in hypohamiltonian graphs, *Can. Math. Bull.* **6** (1973), 33–41.

[96] L. Comtet, *Advanced Combinatorics*, D. Reidel Publishing Company, Dordrecht, Holland, (1974).

[97] W.H. Cornish, A combinatorial problem and the generalized cosh, in Combinatorial Mathematics, X (Adelaide, 1982), *Lecture Notes in Math.* **1036**, Springer, Berlin (1983), 147–153.

[98] G. Cornuejols, R. Urbaniak, R. Weismantel and L. Wolsey, Decomposition of integer programs and of generating sets,

Algorithms—ESA '97 (Graz), Lecture Notes in Comput. Sci. **1284** (1997), 92–103.

[99] D. Cox, J. Little and D. O'Shea, Using Algebraic Geometry, *Graduate Text in Mathematics* **185**, Springer-Verlag, New York (1998).

[100] F. Curtis, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.* **67** (1990), 190–192.

[101] G. Csorba, Über die partitionen der ganzen Zahlen, (German) *Math. Annal.* **75** (1914), 545–568.

[102] Z. Dang, O.H. Ibarra and Z.-W. Sun, On the emptiness problem for two-way NFA with one reversal-bounded counter, *Algorithms and Computation, Lectures Notes in Computer Sciences* **2518**, (2002), 103–114.

[103] M. D'Anna, Type Sequences of Numerical Semigroups, *Semigroup Forum* **56** (1998), 1–31.

[104] J.L. Davison, On the linear diophantine of Frobenius, *J. Number Theory* **48** (1994), 353–363.

[105] J.A. Deddens, A combinatorial identity involving relatively prime integers, *J. Comb. Theory* Ser.A **26**(2) (1979), 189–192.

[106] C. Delorme, Sous-monoïdes d'intersection complète de $\mathbb{N}$, *Ann. Scient. de l'École Normale Supérieure* **9**(4) (1976), 145–154.

[107] C. Delorme, Espaces projectifs anisotropes, *Bull. Soc. Math. France* **103**(2) (1975), 203–223. Erratum: in ibid., **103**(4) (1975), 510.

[108] P. Dembowski, Finite Geometries, *Ergebnisse der Mathematik und ihrer Grenzgebiete, Band* **44** Springer-Verlag, Berlin, New York, (1968).

[109] G. Denham, Short generating functions for some semigroup algebras, *Electron. J. Comb.* **10** (2003), Research paper 36, 7 pages.

[110] C. Del Vigna, Partition colorée d'entiers: Applications à une methode de calcule des denumerants, *Analyse appliquée et informatique (journée de combinatoire et informatique)* (eds. J.-C. Bermond and R. Cori) Bordeaux (1975), 103–109.

[111] R. Diaz and S. Robins, The Ehrhart polynomial of a lattice n-simplex, *Electron. Res. Announc. Am. Math. Soc.* **2**(1) (1996), 1–6.

[112] R. Diaz and S. Robins, The Ehrhart polynomial of a lattice polytope *Ann. Math* **145**(3) (1997), 503–518. Erratum in ibid., **146**(1) (1997), 237.

[113] J. Dixmier, Proof of a conjecture by Erdős and Graham concerning the problem of Frobenius, *J. Number Theory* **34** (1990), 198–209.

[114] L.E. Dickson, *History of the Theory of Numbers*, Vol II, New York, Chelsea, (1992).

[115] M. Djawadi, Kennzeichnung von Mengen mit einer additiven mininaleigenschaft, *J. Reine Angewandte Math.* **311/312** (1979), 307–314.

[116] M. Djawadi, Zum linearen Diophantischen Problem von Frobenius, (On the linear diophantine problem of Frobenius), *Bull. Iranian Math. Soc.*, **9**(2) (1981/82), 127–142.

[117] M. Djawadi and G.R. Hofmeister, Linear diophantine problems, *Arch. Math.*, **66** (1996), 19–29.

[118] M. Djawadi and G.R. Hofmeister, Linear diophantine problems, *Number Theory, New York, 1991–1995*, Springer, New York, (1996), 91–95.

[119] W. Dobosiewicz, An efficient variation of bubble sort, *Informat. Process. Lett.* **11**(1) (1980), 5–6.

[120] D.E. Doobs and G.L. Matthews, On comparing two chains of numerical semigroups and detecting Arf semigroups, *Semigroup Forum* **63** (2001), 273–246.

[121] D.E. Dobbs and G.L. Matthews, On a question of Wilf concerning numerical semigroups, manuscript, 16 pages.

[122] A.L. Dulmage and N.S. Mendelsohn, Gaps in the exponent set of primitive matrices, *Illinois J. Math.* **8** (1964), 642–656.

[123] E. Ehrhart, Sur un problème de géometrie diophantienne linéaire I, *J. Reine Angewandte Math.* **226** (1967), 1–29.

[124] E. Ehrhart, Sur un problème de géometrie diophantienne linéaire II, *J. Reine Angewandte Math.* **227** (1967), 25–49.

[125] E. Ehrhart, Nombre de solutions d'un systeme diophantienne eulerien, *C. R. Acad. Sci. Paris* Séries A **285** (1977), 317–320.

[126] E. Ehrhart, *Polynôme Arithmetique et Méthode des Polyedres en Combinatoire*, **35** Serie ISNM, Birkhauser, Basle, (1977).

[127] E. Ehrhart, Sur les polyèdres rationnels homothétiques à n dimensions, *C.R. Acad. Sci. Paris*, **254** (1962), 616–618.

[128] H. Engels, *Numerical Cuadrature and Cubature, Computational Mathematics and Applications*, Academic Press, London, New York, (1980).

[129] P. Erdős, Problem P-84, *Can. Math. Bull.* **14** (1971), 275–277.

[130] P. Erdős, On an elementary proof of some asymtoptic formulas in the theory of partition, *Ann. Math.* **43**(2) (1942), 437–352.

[131] P. Erdős and R.L. Graham, On a linear diophantine problem of Frobenius, *Acta Arithmetica* **21** (1972), 399–408.

[132] P. Erdős and R.L. Graham, Old and new problems and results in combinatorial number theory, *Monographies de l'Enseignement Mathématiques* **28**, Université de Genève, (1980).

[133] P. Erdős, P.M. Grüber and J. Hammer, Lattice Points, *Pitman Monograph Series in Pure and Applied Mathematics* **39** Longman, Harlow (1989).

[134] P. Erdős and J. Lehner, The distribution of the number of summands in the partitions of a positive integer, *Duke J. of Math.* **8** (1941), 335–345.

[135] M. Estrada and A. López, A note on symmetric semigroups and almost arithmetic sequences, *Commun. Algebra* **22**(10) (1994), 3903–3905.

[136] L. Euler, Observ. anal. de combinationibus, *Comm. Acad. Pretrop.* **13**, ad annum 1741–1743 (1751).

[137] L. Euler, Introductio in Analysin Infinitorium, Vol. **I**, M.-M. Bousqut, Lausanne, (1748) [reprinted as *Leonhardi Euleri Opera Omnia*, Ser. I Vol. **VIII** (A. Krazer and F. Rudio, eds.), Teubner, Leipzig, 1922] [German translation by H. Maser: *Einleitung in die Analysis des Unendlichen, Erster Teil*, Springer, Berlin, (1885)].

[138] L. Euler, De partitione numerorum in partes tam numero quam specie dates, *Novi Commentarii Academiae Scientiarum Imperialis Petropolitanae* **14** (1769) (1770), 168–187 [reprinted in *Leonhardi Euleri Opera Omnia,* Ser. I Vol. **III** (*Commentationes Arithmeticae* Vol. **II**) (F. Rudio, ed.), Teubner, Leipzig, (1917), 132–147.]

[139] J.I. Farrán, On Weierstrass semigroups and one-point algebraic geometry codes, *Coding theory, cryptography and related areas (Guanajuato, 1998)*, (2000), 90–101.

[140] L.G. Fel, Frobenius problem for semigroups $S(d_1, d_2, d_3)$, manuscript (2004), 43 pages.

[141] W. Feller, *An Introduction to Probability Theory and its Applications*, J. Wiley, New York (1950).

[142] G.L. Feng and T.R.N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance, *IEEE Trans. Inform. Theory* **39** (1993), 37–45.

[143] K.G. Fischer and J. Shapiro, Mixed matrices and binomial ideals, *J. Pure Appl. Algebra* **113** (1996), 39–54.

[144] K.G. Fischer, W. Morris and J. Shapiro, Affine semigroups rings that are complete intersections, *Proc. Am. Math. Soc.* **125**(11) (1997), 3137–3145.

[145] K.G. Fischer, W. Morris and J. Shapiro, Mixed dominating matrices, *Linear Algebra Appl.* **270** (1998), 191–214.

[146] F.G. Frobenius, Theorie der linearen Formen mit ganzen Coefficienten, *J. Reine Angewandte Math.* **86** (1878), 146–208.

[147] F.G. Frobenius, Über Matrizen aus nicht negative Elementen, *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, (1912), 456–477.

[148] R. Frőberg, The Frobenius number of some semigroups, *Commun. Algebra* **22**(14) (1994), 6021–6024.

[149] R. Frőberg, C. Gottlieb and R. Hăggkvist, On numerical semigroups, *Semigroup Forum* **35** (1987), 63–83.

[150] M.A. Frumkin, On the number of nonnegative integer solutions of a system of linear diophantine equations, *Studies on Graphs and Discrete Programming* (ed. P. Hansen), North-Holland (1981), 95–108.

[151] P.A. García-Sánchez and J.C. Rosales, Numerical semigroups generated by intervals, *Pacific J. Math.* **191**(1) (1999), 75–83.

[152] P.A. García-Sánchez and J.C. Rosales, on complete intersection affine semigroups, *Commun. Algebra* **23**(14) (1995), 5395–5412.

[153] P.A. García-Sánchez and J.C. Rosales, On free affine semigroups, *Semigroup Forum* **58** (1999), 367–385.

[154] M.R. Garey and D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, W.H. Freeman and Company, New York, (1979).

[155] S. Gaubert and C. Klimann, Rational computation in dioid algebra and its application to performance evaluation of discrete event systems, in Algebraic computing in control (Paris, 1991), *Lecture Notes in Control and Inform. Sci.* **165** Springer, Berlin, (1991), 241–252.

[156] G. Gilmore and R.E. Gomory, A linear programming approach to the cutting stock problem, *Operat. Res.* **9** (1961), 849–859.

[157] J.W.L. Glaisher, Formulae for partitions into given elements, derived from Sylvester's theorem, *Quart. J. Math.* **40** (1909), 275–348.

[158] J.W.L. Glaisher, On a number of partitions of a number into a given number of parts, *Quart. J. Math.* **40** (1909), 57–143.

[159] E.L. Goldberg, On a linear diophantine equation, *Acta Arithmetica* **31** (1976), 239–246.

[160] R.E. Gomory, An algorithm for integer solutions to linear programs, *Princeton IBM Math. Res. Report* Nov. (1958); and in *Recent Advanced in Mathematical Programming* (eds. R.L. Graves and P. Wolf), McGraw-Hill, New York (1963), 269–302.

[161] R.E. Gomory, Outline of an algorithm for integer solutions to linear programs, *Bull. Am. Math. Soc.* **64** (1958), 275–278.

[162] R.E. Gomory, Solving linear programmming problems, in: *Combinatorial Analysis* (eds. R. Bellman and M. Hall Jr.) Proceedings of Symposia in Applied Mathematics X, American Math. Soc. Providence, R.I. (1960), 211–215.

[163] G. Gonnet, *Handbook of Algorithms and Data Structures*, Addison-Wesley, (1984).

[164] V.D. Goppa, Codes that are associated with divisors, (Russian) *Problemy Peredači Informacii* **13**(1) (1977), 33–39; Translation in *Probl. Inform. Transm.* **13**(1) (1977), 22–26.

[165] V.D. Goppa, Algebraic-geometric codes (Russian) *Izv. Akad. Nauk SSSR Ser. Mat.* **46**(4) (1982), 762–781; Translation in *Math. USSR Izv.* **21**(3) (1983), 75–91.

[166] V.D. Goppa, Codes on algebraic curves, (Russian) *Dokl. Akad. Nauk SSSR* **259** (1981), 1289–1290; Translation in *Sov. Math. Dokl.* **24** (1981), 170–172.

[167] D. Gorenstein, An arithmetic theory of adjoint plane curves, *Trans. Am. Math. Soc.* **72** (1952), 414–436.

[168] R.L. Graham, D.E. Knuth and O. Patashnik, *Concrete Mathematics*, Reading, Mass. Addison-Wesley, (1990).

[169] D.D. Grant, A finite integer sequence associated with a linear Diophantine equation, *Nanta Math.* **8**(1) (1975), 99–103.

[170] D.D. Grant, On linear forms whose coefficients are in arithmetic progression, *Israel J. Math.* **15** (1973), 204–209.

[171] H. Greenberg, An algorithm for a linear diophantine equation and a problem of Frobenius, *Numerische Math.* **34**(4) (1980), 349–352.

[172] H. Greenberg, Solution to a diophantine equation for nonnegative integers, *J. Algorithm.*, **9**(3) (1988), 343–353.

[173] P. Griffiths and J. Harris, *Principles of Algebraic Geometry in Pure and Applied Mathematics.* Wiley-Interscience [John Wiley and Sons], New York, (1978).

[174] P.M. Grundy and C.A.B. Smith, Disjunctive games with the last player losing, *Proc. Camb. Philos. Soc.* **52** (1956), 527–533.

[175] S. Gupta and A. Tripathi, Density of M-sets in arithmetic progression, *Acta Arithmetica* **89** (1999), 255–257.

[176] R.K. Guy, Twenty questions concerning Conway's Sylver coinage, *Am. Math. Monthly* **83**(10) (1976), 634–637.

[177] H. Hadwiger, Vorlesungen über Inhalt, Oberfläche und Isoperimetrie, Springer, Berlin, (1957).

[178] F. Halter-Koch, The integral closure of a finitely generated monoid and the Frobenius problem in higher dimensions, in *Semigroups (Luino, 1992)* World Sci. Publishing, River Edge, NJ, (1993), 86–93.

[179] Y.O. Hamidoune, On the diophantine Frobenius problem, *Portugal Math.* **55**(4) (1998), 425–449.

[180] Y.O. Hamidoune, Some results in additive number theory I: The critical pair theory, *Acta Arithmetica* **96**(2) (2000), 97–119.

[181] J. Hammer, Unsolved Problems Concerning Lattice Points, *Research Notes in Mathematics* **15** Pitman, London (1977).

[182] S. Han, C. Kirfel and M.B. Nathanson, Linear forms in finite sets of integers, *Ramanujan J.* **2** (1998), 271–281.

[183] H. Hann-Shuei, An algorithm for the solution of a linear Diophantine Problem of Frobenius, *Chin. J. Math.* **9**(1) (1981), 67–74.

[184] G.H. Hardy, *Some Famous Problems of the Theory of Numbers and in Particular Waring's Problem*, Oxford, U.K. (1920).

[185] G.H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.* **17** (1918), 75–115.

[186] R.E. Hartwig and M. Neumann, Bounds on the exponenet of primitivity which depend on the spectrum and the minimal polynomial, *Linear Algebra Appl.* **184** (1993), 103–122.

[187] B.R. Heap and M.S. Lynn, The index of primitivity of a non-negative matrix, *Numerische Math.* **6** (1964), 120–141.

[188] B.R. Heap and M.S. Lynn, A graph-theoretic algorithm for the solution of a linear diophantine problem of Frobenius, *Numerische Math.* **6** (1964), 346–354.

[189] B.R. Heap and M.S. Lynn, On a linear diophantine problem of Frobenius: an improved algorithm *Numerische Math.* **7** (1965), 226–231.

[190] O. Heden, The Frobenius number and partitions of a finite vector space, *Arch. Math.* **42**(2) (1984), 185–192.

[191] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, *Manuscripta Math.* **3** (1970), 175–193.

[192] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, Thesis, *Lousiana State University*, New Orleans, La., USA, (1969).

[193] J. Herzog and E. Kunz, Die Werthalbgruppe eines lokalen Rings der dimension 1, *Sitzungsberichte der Heidelberger Akademie der Wissenschaften* **2** (1971), 27–67.

[194] M. Herzog and J. Schønheim, Group partition, factorization and the vector covering problem, *Can. Math. Bull.* **15**(2) (1972), 207–214.

[195] G. Higman, B.H. Neumann and H. Neumann, Embedding theorems for groups, *J. London Math. Soc.* **24** (1949), 247–254.

[196] D. Hilbert, Ueber die Theorie der algebraischen Formen, *Math. Annalen* **36** (1890), 473–534.

[197] C.W. Ho, J.L. Parish and P.J. Shiue, On the sizes of elements in the complement of a monoid of integers, *Proceedings of the*

Fourth International Conference on Fibonacci Numbers and Their Applications (1991), 139–144.

[198] G.R. Hofmeister, Zu einem Problem von Frobenius, *Norske Videnskabers Selskabs Skrifter*, **5** (1966), 1–37; *Math. Rev.* **34** (1967) # 5792.

[199] G.R. Hofmeister, Lineare diophantische Probleme, *Joh. Gutenberg-Universität, Mainz*, (1978).

[200] G.R. Hofmeister, Eine Verallgemeinerung des Reichweitenproblems (German), *Abh. Braunschweig. Wiss. Ges.* **33** (1982), 161–163.

[201] G.R. Hofmeister, Remark on linear forms, *Arch. Math.* **65** (1995), 511–515.

[202] G.R. Hofmeister, Extremal Frobenius number in a class of sets, *Arch. Math.* **70** (1998), 357–365.

[203] G.R. Hofmeister, Linear diophantine problems, *Bull. Iranian Math. Soc.* **8**(2) (1980/81), 121–155.

[204] A. Horváth and M. Hujter, Some algorithms for a problem of Frobenius, preprint, Hungary, (1982).

[205] T. Høholdt, J.V. van Lint and R. Pellikaan, Algebraic geometry codes, in *Handbook of Coding Theory* **1** (eds. V.S. Pless, W.C. Huffman and R.A. Brualdi) Amsterdam, The Netherlands, Elsevier (1998), 871–961.

[206] H.S. Huang, An algorithm for the solution of a linear diophantine problem of Frobenius, *Chinese J. Math.* **9**(1) (1981), 67–74.

[207] M. Hujter, Lower bounds for the Frobenius problem, *Technical Report* **MO/43** Computer and Automation Inst., Hungarian Academy of Sciences, (1982).

[208] M. Hujter, On a problem of Frobenius: a Survey, *Technical Report* **MO/44** Computer and Automation Inst., Hungarian Academy of Sciences, (1982).

[209] M. Hujter, On a sharp upper and lower bounds for the Frobenius problem, *Technical Report* **MO/32** Computer and Automation Inst., Hungarian Academy of Sciences, (1982).

[210] M. Hujter, On the lowest value of the Frobenius number, *Technical Report* **MN/31** Computer and Automation Inst., Hungarian Academy of Sciences, (1987).

[211] M. Hujter, On the coin exchange problem of Frobenius, *Technical Report* **MN/32** Computer and Automation Inst., Hungarian Academy of Sciences, (1987).

[212] M. Hujter, Improved lower and upper bounds for the number of feasible solutions to a Knapsack problem, *Optimization* **19**(6) (1988), 889–894.

[213] M. Hujter and B. Vizvári, The exact solution to the Frobenius problem with three variables, *J. Ramanujan Math. Soc.* **2**(2) (1987), 117–143.

[214] J. Incerpi and R. Sedgewick, Improved upper bounds on ShellSort, *J. Comput. Systems Sci.* **31** (1985), 210–224.

[215] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, Heidelberg, Berlin, (1980).

[216] M.Z. Israilov, Numbers of solutions of linear diophantine equations and their applications in the theory of invariant cubature formulas (in Russian), *Sibirskii Matematicheskii Zhurnal* **22**(2) (1981), 121–136 [English translation: *Siberian Math. J.* **22**(2) (1981), 260–273].

[217] N.N. Ivanov and V.N. Shevchenko, The structure of a finitely generated semilattice (Russian), *Dokl. Akad. Nauk. BSSR*, **19** (1975), 773–774.

[218] A. Janz, Bestimmung der maximalen Frobeniuszahl, Master thesis, *Johannes Guttenberg Universität*, Mainz, April (1997).

[219] S.M. Johnson, A linear diophantine problem, *Can. J. Math.* **12** (1960), 390–398.

[220] S.C. Johnson and B.W. Kernighan, Making change with a minimum number of coins, *Bell Laboratories, Murray Hill*, New Jersey, manuscript undated.

[221] C.A. Jones, Using linear forms to determine the set of integers realizable by $(g_0, g_1, \ldots, g_n)$-trees, *Discrete Math.* **47** (1983), 247–254.

[222] L. Juan, Some results about symmetric semigroups, *Commun. Algebra* **21**(10) (1993), 3637-3645.

[223] I.D. Kan, On the Frobenius problem, (Russian) *Fundam. Prikl. Mat.* **3**(3) (1997), 821–835.

[224] I.D. Kan, B.S. Stechkin and I.V. Sharkov, On the Frobenius problem for three arguments, (Russian) *Mat. Zametki*, **62** (4) (1997), 626–629; translation in *Math. Notes*, **62**(3–4) (1997), 521–523.

[225] I.D. Kan, Representation of numbers by linear forms, (Russian) *Mat. Zametki* **68**(2) (2000), 210–216; translation in *Math. Notes* **68**(1–2) (2000), 185–190.

[226] I.D. Kan, The Frobenius problem for classes of polynomial solvability, (Russian) *Mat. Zametki* **70**(6) (2001), 845–853; translation in *Math. Notes* **70**(5–6) (2001), 771–778.

[227] J. Kang and Z. Liu, A relation between M_3 and linear congruence equations (Chinese) *J. Southwest Teach. Univ., Ser. B* **2** (1987), 1–7.

[228] R. Kannan, Lattice translates of a polytope and the Frobenius problem, *Combinatorica* **12**(2) (1992), 161–177.

[229] R. Kannan, The Frobenius problem, *Foundations of software technology and theoretical computer science*, Bengalore, 1981, Lectures Notes in Comput. Sci. **405**, Springer, Berlin, (1989), 247–251.

[230] J.M. Kantor and A. Khovanskii, Une application du théorème de Riemann-Roch combinatoire au polynôme d'Ehrhart des polytopes entier de $\mathbb{R}^n$, *C.R. Acad. Sci. Paris Serie I* **317** (1993), 501–507.

[231] H. Kaufman, A bibliographical note on higher order sine functions, *Scripta Math.* **28** (1967), 29–36.

[232] Z. Ke, On the equation of $ax + by + cz = n$, *J. Sichuan Univ. Math. Biquarterly* (natural science edition) **1** (1955), 1–4.

[233] J.G. Kemeny and J.L. Snell, *Finite Markov Chains*, D. Van Nostrand Company, Inc., Princeton (1960).

[234] A.G. Khovanskii, Newton polyhedron, Hilbert polynomial and sums of finite sets, *Functional Analalysis and Its Applications* **26**(4) (1992), 276–281; translation from *Funkts. Anal. Prilozh.* **26**(4) (1992), 57–63.

[235] A.G. Khovanskii, Sums of finite sets, orbits of commutative semigroups, and Hilbert functions, *Func. Anal. Appl.* **29**(2) (1995), 120–112.

[236] H.G. Killingbergtrø, Betjening av figur i Frobenius' problem (Using figures in Frobenius' problem), (Norwegian) *Normat* **2** (2000), 75–82.

[237] C. Kirfel, Erweiterung dreielementiger Basen bei konstanter Frobeniuszahl, *Math. Scand.* **54** (1984), 310–316.

[238] C. Kirfel, Erweiterung dreielementiger Basen bei konstanter Frobeniuszahl II, *Math. Scand.* **58** (1986), 149–160.

[239] C. Kirfel, Stabilität bei symmetrischen h-basen, (German), *Acta Arith.* **51** (1988)(1), 85–96.

[240] C. Kirfel and R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, *IEEE Trans. Informat. Theor.* **41**(6) (1995), 1720–1732.

[241] C. Kirfel and E.S. Selmer, Regular h-ranges and weakly pleasant h-bases, *Math. Scand.* **59** (1986), 30–40.

[242] G. Kiss, Extremal Frobenius number in some special cases, *Annales Univ. Sci. Budapest* **44** (2001), 27–31.

[243] G. Kiss, Extremal Frobenius number in a new aspect, *Annales Univ. Sci. Budapest* **44** (2002), 139–142.

[244] L.F. Klosinski, G.L. Alexanderson and L.C. Larson, The Fifty-Second William Lowell Putnman Mathematical Competition, *Am. Math. Monthly* **9** (1992), 715–724.

[245] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.

[246] D. E. Knuth, *The Art of Computer Programming*, Vol. **3**: Sorting and Searching, Addison-Wesley, Reading Mass. (1973).

[247] C. Ko, *Acta Sci. Sichuan Univ.* **1** (1955), 1–4.

[248] C. Ko, D. Li and W. Yin, *Acta Sci. Sichuan Univ.* **3** (1964), 39–50.

[249] T. Komatsu, The number of solutions of the diophantine equation of Frobenius—general case, *Math. Commun.* **8**(2)(2003), 195–206.

[250] J. Komeda, Non-Weierstrass numerical semigroups, *Semigroup Forum* **57** (1998), 157–185.

[251] J. Komeda, Remarks on non-Weierstrass numerical semigroups, *Algebras and Combinatorics. An International Congress, ICAC'97, Hong Kong* (eds. K.-P. Shum, E.J. Taft and Z.-X. Wan), Springer-Verlag (1999), 313–319.

[252] J. Komeda, On Weierstrass points whose first non-gaps are four, *J. Reine Angew. Math.* **341** (1983), 68–86.

[253] J. Kraft, Singularity of monomial curves in A^3 and Gorenstein monomial curves in A^4, *Can. J. Math.* **37**(5) (1985), 872–892.

[254] E. Krätzel, Die maximale Ordnung der Anzahl der wesentlich verschiedenen abelschen Gruppen n-ter Ordnung (German), *Quart. J. Math. Oxford* Ser. 2 **21** (1970), 273–275.

[255] H. Krawczyk and A. Paz, The diophantine problem of Frobenius: A close bound, *Discrete Appl. Math.* **23** (1989), 289–291.

[256] E. Kunz, The value-semigroup of a one-dimensional Gorenstein ring, *Proc. Am. Math. Soc.* **25** (1970), 748–751.

[257] E. Kunz, Über die Klassifikation numerischer Halbgruppen, (German) (On the classification of numerical semigroups), *Regensburger Mathematische Schriften (Regensburg Mathematical Publications)* **11** Universität Regensburg, Fachbereich Mathematik, Regensburg, (1987).

[258] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Basel (1985).

[259] S. Kuriki, Une identité introduite par le dénumérant, *TRU Math.* **13** (1977), 53–54.

[260] S. Kuriki, Sur une méthode de calcul du dénumérant, *TRU Math.* **14** (1978), 47–48.

[261] E.N. Laguerre, Partition des nombres, (French) *Bull. Soc. Math. France* **V** (1877).

[262] D.T. Lee, C.L. Liu and C.K. Wong, $(g_0, \ldots, g_k)$-trees and unary OL systems, *Theor. Comput. Sci.* **22** (1983), 209–217.

[263] T. Leighton, Tight bounds on the complexity of parallel sorting, in *Proc. 16th Annual ACM Symposium of Theory of Computing*, Washington D.C., April (1984).

[264] H.W. Lenstra, Integer programming with a fixed number of variables, *Math. Operat. Res.* **8** (1983), 538–548.

[265] H.W. Lenstra and C. Pomerance, *Primality testing with Gaussian periods*, preprint (2004), 41 pages.

[266] V.F. Lev, Structure theorem for multiple addition and the Frobenius problem, *J. Number Theory* **58** (1996), 79–88.

[267] V.F. Lev, On the extremal aspect of the Frobenius problem, *J. Comb. Theory* Ser. A **73** (1996), 111–119.

[268] V.F. Lev, Addendum to ‘Structure theorem for multiple addition’, *J. Number Theory* **65** (1997), 96–100.

[269] V.F. Lev, Optimal representations by sumsets and subset sums, *J. Number Theory* **62** (1997), 127–143.

[270] V.F. Lev, On consecutive subset sums, *Discrete Math.* **187** (1998), 151–160.

[271] M. Lewin, An algorithm for a solution of a problem of Frobenius, *J. Reine Angewandte Math.* **276** (1975), 68–82.

[272] M. Lewin, A bound for a solution of a linear diophantine problem, *J. London Math. Soc.* **6** (1972), 61–69.

[273] M. Lewin, On a diophantine problem of Frobenius, *Bull. London Math. Soc.* **5** (1973), 75–78.

[274] M. Lewin, On a problem of Frobenius for almost consecutive set of integers, *J. Reine Angewandte Math.* **273** (1975), 134–137.

[275] W. Lex, Über Lösungsanzhlen linearer diophantischer Gleichungen, *Math.-phys. Semesterberichte* **24** (1977), 254–279.

[276] J. Lipman, Stable ideals and Arf rings, *Am. J. Math.* **93** (1971), 649–685.

[277] P. Lisoněk, Denumerants and their approximations, *J. Combin. Math. Combin. Comput.* **18** (1995), 225–232.

[278] P. Lisoněk, ‘Quasi-Polynomials: A case study in Experimental Combinatorics’, *Technical report Series, RISC-Linz, Austria* **93–18** (1993).

[279] C.L. Liu, *Introduction to Combinatorial Mathematics*, McGraw-Hill, New York (1955).

[280] L. Lovász, Geometry on numbers and integer programming, in: proceedings of the 13th International Symposium on Mathematical Programming, (eds. M. Iri and K. Tanabe), Tokyo *Math. Prog.* (1989), 177–178.

[281] W. Lu, *Acta Sci. Sichuan Univ.* **1** (1956), 49–55.

[282] W. Lu and C. Wu, *Acta Sci. Sichuan Univ.* **2** (1957), 151–171.

[283] G.S. Lueker, Two NP-complete problems in nonnegative integer programming, *Technical Report TR-178*, Department of Electrical Engineering, Princeton University (1975).

[284] S. L’vovsky, On inflection points, monomial curves, and hypersurfaces containing projective curves, *Math. Ann.* **306** (1996), 719–735.

[285] P.L. Manley, A note on linear forms, *Ranchi Univ. Math. J.* **9** (1978), 77–80.

[286] H.B. Mann, An addition theorem for sets of elements of an abelian group, *Proc. Am. Math. Soc.* **4** (1953), 423.

[287] O. Marstrander, On a problem of Frobenius, *Math. Scand.* **58**(2) (1986), 161–175.

[288] H. Matternich, Über ein Problem bei Frobenius, Basiserweiterung bei Konstanter Mathematik, *Johannes Gutenberg-Univ.*, Mainz, (1981).

[289] C. McDiarmid and J.L. Ramírez Alfonsín, Sharing jugs of wine, *Discrete Math.* **125** (1994), 279–287.

[290] P. McMullen, Valuations and Euler-type relations on certain classes of convex polytopes, *Proc. London Math. Soc.* **35**(3) (1977), 113–135.

[291] P. McMullen, Lattice invariant valuations on rational polytope, *Arch. Math.* **31** (1978), 509–516.

[292] N.S. Mendelsohn, A linear diophantine equation with applications to non-negative matrices, in *Proceedings of the International Conference on Combinatorial Mathematics*, New York 1970 (eds. A. Gewirtz and L.V. Quintas), *Ann. New York Acad. Sci.*, **175** (1970), 287–294.

[293] C. Mereghetti and G. Pighizzini, Optimal simulations between unary automata, *SIAM J. Comput.* **30**(6) (2001), 1976–1992.

[294] G. Meures, Zusammenhang zwischen Reichweite und Frobeniuszahl, Staatexamenarbeit, *Johannes Gutenberg-Univ.*, Mainz, (1977).

[295] H. Metternich, Über ein Problem von Frobenius. Basiserweiterung bei konstanter Frobeniuszhl, *Diplomarbeit Math. Inst., Joh. Gutenberg-Univ.*, Mainz (1981).

[296] V. Micale, On monomial semigroups, *Comm. Alg.* **30**(10) (2002), 4687–4698.

[297] P.B. Milanov, The linear diophantine problem of Frobenius and discrete optimization, (German) *Diskrete Optimierung*, Wissensch. Beitr., Friedrich-Schiller-Univ., Jena, (1985), 73–82.

[298] H. Minc, Nonnegative matrices, *Series in Discrete Mathematics and Optimazation*, Wiley-Interscience, New York, (1988).

[299] M. Morales, Syzygies of monomial curves and a linear diophantine problem of Frobenius, *Internal Report, Max Planck Institut für Mathematik, Bonn*, (1987).

[300] M. Morales, Noetherian symbolic blow-ups, *J. Algebra* **140**(1) (1991), 12–25.

[301] L.J. Mordell, Lattice points in a tetrahedron and generalized Dedekind sums, *J. Indian Math. Soc. (N.S.)* **15** (1951), 41–46.

[302] R. Morikawa, On the linear diophantine problem of Frobenius in three variables, *Bull. Fac. Liberal Arts Nagasaki Univ.* **38**(1) (1997), 1–17.

[303] M. Nagata and H. Matsumura, A theorem in elementary arithmetic, (Japanese) *Sûgaku* **13** (1961–62), 161; *Math. Rev.* **25**(3) (1963).

[304] D.A. Narayan and A.J. Schwenk, Tiling large rectangles, *Math. Mag.* **75**(5) (2002), 372–380.

[305] M.B. Nathanson, Sums of finite sets of integers, *Am. Math. Monthly* **79** (1972), 1010–1012.

[306] M.B. Nathanson, Partitions with parts in a finite set, *Proc. Am. Math. Soc.* **128** (2000), 1269–1273.

[307] E. Netto, *Lehrbuch der Combinatorik*, (Second Edition) Leipzig and Berlin, B.G. Teubner (1927).

[308] H. Niederreiter, Random numbers generation and Quasi-Monte Carlo Methods, *CBMS-NSF Regional Conference Series in Applied Mathematics*, **63**, SIAM, Philadelphia, (1992).

[309] M. Nijenhuis, A minimal-path algorithm for the 'money changing problem', *Am. Math. Monthly* **86** (1979), 832–838. Correction in ibid., **87** (1980), 377.

[310] M. Nijenhuis and H.S. Wilf, Representation of integers by linear forms in nonnegative integers, *J. Number Theory* **4** (1972), 98–106.

[311] C. Niu and Z. Oiu, On a problem of Frobenius, (Chinese) *J. Shandong Univ. Nat. Sci. Ed.* **21**(1) (1986), 1–6.

[312] X.F. Niu, A formula for the largest integer which cannot be represented as $\sum_{i=1}^{s} a_i x_i$, (Chinese) *Heilongjiang Daxue Ziran Kexue Xuebao* **9**(4) (1992), 28–32.

[313] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edn New York, John Wiley and Sons, (1991).

[314] R.Z. Norman, Some observations on linear diophantine representations, *Proc. 8th Con. Combinatorics, Graph Theory and Computing; Baton Rouge, Congressus Nemeratium* **19** (1977), 511–522.

[315] B.V. Novikov, On the structure of subsets of a vector lattice that are closed with respect to addition, *J. Math. Sci.* **72**(4) (1994), 3223–3225.

[316] T.H. O'Beirne, *Puzzles and Paradoxes*, Oxford University Press, New York and London, (1965).

[317] G. Oliveira, Weierstrass semigroups and the canonical ideal of non-trigonial curves, *Manuscripta Math.* **71** (1991), 431–450.

[318] M. Ontkush, A closed formula for linear indeterminate equations in two variables, *Pi Mu Epsilon* **9**(1) (1989), 16–18.

[319] Th. Ottman, H.W. Six and D. Wood, On the correspondance between AVL trees and brother trees, *Computing* **23** (1979), 43–54.

[320] R.W. Owens, An algorithm to solve the Frobenius problem, *Math. Mag.* **74**(4) (2003), 264–275.

[321] M.W. Padberg, A remark on 'an inequality for the number of lattice points in a simplex', *SIAM J. Appl. Math.* **20**(4) (1971), 638–641.

[322] C.H. Papadimitriou and K. Steiglitz, *Combinatorial Optimization: Algorithms and Complexity*, Prentice-Hall, Inc., (1982).

[323] A.A. Papernov and G.V. Stasevich, A method of information sorting in computer memories, *Probl. Inform. Transmiss.* **1**(3) (1965), 63–75.

[324] D.P. Patil and B. Singh, Generators for the derivation modules and the relation ideals of certain curves, *Manuscripta Math.* **68** (1990), 327–335.

[325] R. Pellikaan and F. Torres, On Weierstrass semigroups and the redundancy of improved geometric Goppa codes, *IEEE Trans. Informat. Theor.* **45**(7) (1999), 2512–2519.

[326] C.A. Petri, 'Kommunikation mit Automaten', Schriften des Rheinisch-Westfalischen Institutes für Instrumentelle Mathematik an der Universität Bonn, Hft. **2** Bonn, (1962). Translated

into English by Project ISTP: ‘Communication with Automata,’ translated by C.F. Greene, Jr., a Supplement to Technical Documentary Report No. 1 prepared for Rome Air Development Center #AF 30 (602)-3344, (1965).

[327] G. Pick, Geometrisches zur Zahlenlehre, *Sitzungsber. Lotos (Prague)* **19** (1899), 311–319.

[328] J. Piehler, Bemerkungen zum Frobenius-problem, (German) *Wiss. Z. Tech. Hochsch. Leuna-Merseburg* **29**(4) (1987), 496–502.

[329] J. Piehler, Bemerkungen zu einer Arbeit von über die Anzahl zulässiger Lösungen eines Knapsack-Problems, (German) *Math. Operationsforsch. Statist. Ser. Optim* **9**(2) (1978), 167–170.

[330] J. Piehler, Über die nichtnegativen Lösungen linearer diophantischer Gleichungen, (German) *Wiss. Z. Tech. Hochsch. Leuna-Merseburg* **27**(3) (1985), 320–327.

[331] J. Pitman and P. Leske, A number-theoretical note on Cornish’s paper, in Combinatorial Mathematics, X (Adelaide, 1982), *Lecture Notes in Math.* **1036**, Springer, Berlin (1983), 316–318.

[332] P. Pleasants, H. Ray and R.J. Simpson, The Frobenius problem on lattices, *Australasian J. Comb.*, **32** (2005), 27–45.

[333] G. Pólya and G. Szegó, *Aufgaben und Lehrsätze aus der Analysis*, Srpinger-Verlag, Berlin (1925). English translation: *Problems and Theorems in Analysis*, Springer-Verlag, New York, (1972).

[334] J.E. Pommersheim, Toric varieties, lattice points and Dedekind sums, *Math. Ann.* **295** (1993), 1–24.

[335] T. Popoviciu, Asupra unei probleme de patitie a numerelor, *Acad. Republicii Populare Romane, Filiala Cluj, Studii si cercetari stiintifice* (Romanian) **4** (1953), 7–58.

[336] V. Pratt, Shellsort and Sorting Networks, Garland Publishing, New York (1979); Ph.D. thesis, Stanford University, (1971).

[337] M. Raczunas and P. Chrząstowski-Wachtel, A diophantine problem of Frobenius in terms of the least common multiple, *Discrete Math.* **150** (1996), 347–357.

[338] H. Rademacher and E. Grosswald, Dedekind Sums, Carus Mathematical Monographs *Math. Assoc. Am.*, **16** (1972).

[339] H. Rademacher, On the partition function, *Proc. London Math. Soc.* **43** (1937), 241–254.

[340] H. Rademacher, A convergent series for the partition function, *Proc. Nat. Acad. Sci. U.S.A.* **23** (1973), 78–84.

[341] J.L. Ramírez Alfonsín, Topics in Combinatorics and Computational Complexity, D.Phil. Thesis, *University of Oxford*, U.K., (1993).

[342] J.L. Ramírez Alfonsín, Complexity of the Frobenius problem, *Combinatorica* **16**(1) (1996), 143–147.

[343] J.L. Ramírez Alfonsín, On variations of the subset sum problem, *Discrete Appl. Math.* **81** (1998), 1–7.

[344] J.L. Ramírez Alfonsín, The diophantine Frobenius problem, *Forschungsinstitut für Diskrete Mathematik, Bonn*, Report No.00893 (2000), 43 pages.

[345] J.L. Ramírez Alfonsín, Gaps in semigroups, manuscript, 15 pages.

[346] J.L. Ramírez Alfonsín, On the Frobenius number and the covering radius, manuscript, 18 pages.

[347] J.L. Ramírez Alfonsín, The Frobenius number via Hilbert Series, manuscript, 12 pages.

[348] J.E. Reeve, On the volume of lattice polyhedra, *Proc. Lond. Math. Soc.* **III**(7) (1957), 378–395.

[349] L. Reid and L.G. Roberts, Monomial subrings in arbitrary dimension, *J. Algebra* **236** (2001), 703–730.

[350] E. Remy and E. Thiel, Medial axis for chamfer distances: computing look-up tables and neighbourhoods in 2D or 3D, *Pattern Recong. Lett.* **23** (2002), 649–661.

[351] D.S. Rim and M.A. Vitulli, Weierstrass points and monomial curves, *J. Algebra* **48** (1977), 454–476.

[352] J. Riordan, *An Introduction to Combinatorial Analysis*, Princeton University Press, Guildford, Surrey, (1978).

[353] S.M. Ritter, The linear diophantine problem of Frobenius for subsets of arithmetic sequences, *Arch. Math.* **69** (1997), 31–39.

[354] S.M. Ritter, On a linear diophantine problem of Frobenius: Extending the basis, *J. Number Theory* **69** (1998), 201–212.

[355] J.B. Roberts, Note on linear forms, *Proc. Am. Math. Soc.* **7** (1956), 465–469.

[356] J.B. Roberts, On a diophantine problem, *Can. J. Math.* **9** (1957), 219–222.

[357] J.B. Roberts, Interaction of cycles, *Bull. Math. Biophys.* **10** (1948), 123–129.

[358] H. Rohrbach, Einige neuere Untersuchungen über die Dichte in der additiven Zahlentheorie, *Jahresbericht der Deutschen Mathematiker Vereinigung* **48** (1939), 199–236.

[359] H. Rohrbach, Ein Beitrag zur additiven Zahlentheorie, *Math. Zeitschrift* **42** (1937), 1–30.

[360] H. Rohrbach, Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Frag., *Math. Zeitschrift* **42** (1937), 538–542.

[361] V. Romanovski, Recherches sur les chaîn de Markoff, *Acta Math.*, **66** (1936), 147–251.

[362] J.C. Rosales, On numerical Semigroups, *Semigroup Forum* **52** (1996), 307–318.

[363] J.C. Rosales, On symmetric numerical semigroups, *J. Algebra* **182** (1996), 422–434.

[364] J.C. Rosales, Numerical semigroups with Apéry sets of unique expression, *J. Algebra* **226** (2000), 479–487.

[365] J.C. Rosales and M.B. Branco, Numerical semigroups that can be expressed as an intersection of symmetric numerical semigroups, *J. Pure Appl. Algebra* **171**(2–3) (2002), 303–314.

[366] J.C. Rosales and M.B. Branco, Irreducible numerical semigroups, *Pacific J. Math.* **209** (1) (2003), 131–143.

[367] J.C. Rosales and P.A. García-Sánchez, Every positive integer is the Frobenius number of an irreducible numerical semigroup with at most four generators, *Ark. Mat.* **42**(2) (2004), 301–306.

[368] J.C. Rosales, P.A. García-Sánchez and J.I. García-García, Every positive integer is the Frobenius number of a numerical semigroup with three generators, *Math. Scand.* **94**(1) (2004), 5–12.

[369] J.C. Rosales, P.A. García-Sánchez, J.I. García-García and J.A. Jiménez Madrid, Fundamental gaps in numerical semigroup, *J. Pure Appl. Algebra* **189**(1) (2004), 301–313.

[370] J.C. Rosales and P.A. García-Sánchez, Numerical semigroups with embedding dimension three, *Arch. Math.* **83** (2004), 488–496.

[371] J. Rosenmüller and H.G. Weidner, extreme convex set functions with finite carrier: General Theory, *Discrete Math.* **10** (1974), 343–382.

[372] J. Rosiak, The minimum exponent of the primitive diagraphs on the given number of arcs, *Opuscula Math.* **24**(2) (2004), 197–202.

[373] Ø.J. Rødseth, On a linear diophantine problem of Frobenius, *J. Reine Angewandte Math.* **301** (1978), 171–178.

[374] Ø.J. Rødseth, On a linear diophantine problem of Frobenius II, *J. Reine Angewandte Math.* **307/308** (1979), 431–440.

[375] Ø.J. Rødseth, A note on Brown and Shiue's paper on a remark related to the Frobenius problem, *Fibonacci Quart.* **32**(5) (1994), 407–408.

[376] Ø.J. Rødseth, An upper bound for the h-range of the postage stamp problem, *Acta Arith.* **54**(4) (1990), 301–306.

[377] Ø.J. Rødseth, On h-bases for n, *Math. Scand.* **48**(2) (1981), 165–183.

[378] Ø.J. Rødseth, On h-bases for n. II, *Math. Scand.* **51**(1) (1982), 5–21.

[379] Ø.J. Rødseth, Two remarks on linear forms in nonnegative integers, *Math. Scand.* **51**(2) (1982), 193–198.

[380] Ø.J. Rødseth, An upper bound for the h-range of the postage stamp problem, *Acta Arith.* **54**(4) (1990), 301–306.

[381] R.Y. Rubistein, *Simulation and Monte Carlo Method*, John Wiley and Sons, New York, (1981).

[382] A. Rycerz, Conductors and the generalized problem of Frobenius, *Discuss. Math.* **14** (1994), 15–20.

[383] A. Rycerz and Z. Skupień, Conductors in the integral monoids, *3rd Twente Workshop on Graphs and Combinatorial Optimization* (eds. U. Faigle and C. Hoede), University of Twente, Holland 1993, Memorandum No. 1132, (1993), 154–158.

[384] A. Rycerz, The generalized residue classes and integral monoids with minimal sets, *Opuscula Math.* **20**(7–10) (2000), 65–69.

[385] A.V. Sardo-Infirri, Lefschetz fixed-point theorem and lattice points in convex polytopes, *Adv. Math.* **116** (1995), 55–81.

[386] H.E. Scarf and D.F. Shallcross, The Frobenius problem and maximal lattice free bodies, *Math. Oper. Res.* **18** (1993), 511–515.

[387] J.-C. Schlage-Puchta, An estimate for Frobenius's diophantine problem in three dimensions, *J. Integer Sequences* **8**(1) (2005), Article 05.1.7.

[388] M. Schoch, An investigation to the Frobenius problem, *Advances in Mathematical Optimization, Math. Res.* **45** Akademie-Verlag, Berlin (1988), 191–195.

[389] M. Schoch, Zur Lösung einer speziellen linearen diskreten Optimierungsaufgabe mit Zusatzforderungen, *Math. Operatinsforsch. Statist. Series Optimization* **13**(3) (1982), 373–392.

[390] I.J. Schur, Zur additiven zahlentheorie, *Sitzungsberichte Preussische Akad. Wiss. Phys. Math. Kl.* (1926), 488–495.

[391] R. Sedgewick, A new upper bound for ShellSort, *J. Algorithms* **7** (1986), 159–173.

[392] E.S. Selmer, On the linear diophantine Problem of Frobenius, *J. Reine Angewandte Math.* **293/294**(1) (1977), 1–17.

[393] E.S. Selmer, On ShellSort and the Frobenius problem, *BIT* **29**(1) (1989), 37–40.

[394] E.S. Selmer and B.K. Selvik, On Rødseth's h-bases $A_k = \{1, a_2, 2a_2, \ldots, (n-k)a_2, a_k\}$, *Math. Scand.* **68**(2) (1991), 180–186.

[395] E.S. Selmer, On regular Frobenius bases, *Math. Scand.* **63**(1) (1988), 109–116.

[396] E.S. Selmer, Two popular problems in number theory. I. Changing coins, *Normat* **29**(2) (1981), 81–87.

[397] E.S. Selmer, Two popular problems in number theory. II. The postage stamp problem, *Normat* **29**(3) (1981), 105–114.

[398] E.S. Selmer, Note on the postage stamp problem, *Normat* **31**(1) (1983), 30–48.

[399] E.S. Selmer, On the postage stamp problem with three stamp denominations, *Math. Scand.* **47**(1) (1980), 29–71.

[400] E.S. Selmer, On the postage stamp problem with three stamp denominations. II, *Math. Scand.* **53**(2) (1983), 145–156.

[401] E.S. Selmer, On the postage stamp problem with three stamp denominations. III, *Math. Scand.* **56**(2) (1985), 105–116.

[402] E.S. Selmer, Associate bases in the postage stamp problem, *J. Number Theory* **42** (1992) 320–336.

[403] E.S. Selmer, The local postage stamp problem, I-III Institute Rep. Nos. **42**, **44**, **57**, *University of Bergen*, Dept. of Pure Math., (1986, 1990).

[404] E.S. Selmer and O. Beyer, On the linear diophantine problem of Frobenius in three variables, *J. Reine Angewandte Math.* **301** (1978), 161–170.

[405] S. Sertöz, On the number of solutions of the diophantine equation of Frobenius, *Diskret. Mat.* **10**(2) (1998), 62–71; translation in *Discrete Appl. Math.* **8**(2) (1998), 153–162.

[406] S. Sertöz, On Arf rings, Appendix in 'The Collected Papers of Cahit Arf, *Turkish Math. Soc.* (1990), 416–419.

[407] S. Sertöz and A. Özlük, On a diophantine problem of Frobenius, *Bull. Tech. Univ. Istanbul* **39**(1) (1986), 41–51.

[408] S. Sertöz and A. Özlük, On the number of representations of an integer by a linear form, *Instanbul Üniv. Fen Fak. Mat. Der.* **50** (1991), 67–77.

[409] J. Shallit, What this country needs is a 18 cents piece, *The Mathematical Intelligencer* (2003), 20–23.

[410] J. Shallit, The computational complexity of the local postage stamp problem, *SIGACT News* **33**(1) (2002), 90–94.

[411] J. Shallit and M.-W. Wang, Automatic complexity of string, *J. Automata, Languages, Comb.* **6**(4) (2001), 537–554.

[412] J.Y. Shao, Some computational formulas of the Frobenius numbers (Chinese), *J. Math. (Wuhan University)* **8**(4) (1988), 375–388.

[413] W.J.C. Sharp, Solution to Problem 7382, *Educational Times* **37** (1884), 26; reprinted in Mathematical questions with their solutions, *Educational Times* (with additional papers and solutions) **41** (1884), 21.

[414] D.L. Shell, A high-speed sorting procedure, *Commun. ACM* **27** (1959), 30–32.

[415] J. Shen, An improvement of the Dulmage-Mandelsohn theorem, *Discrete Math.* **158** (1996), 295–297.

[416] J. Shen, A short proof of a theorem on primitive matrices, Proceedings of the Twenty-seventh Southeastern International Conference on Combinatorics, Graph Theory and Computing (Baton Rouge, LA, 1996), *Congr. Numer.* **121** (1996), 204–210.

[417] J. Shen, A Bound on the exponent of primitivity in terms of diameter, *Linear Algebra Appl.* **244** (1996), 21–33.

[418] J. Shen, A problem on the exponent of primitive digraphs, *Linear Algebra Appl.* **244** (1996), 244–264.

[419] J. Shen, Some estimated formulas for the Frobenius number, *Linear Algebra Appl.* **244** (1996), 13–20.

[420] V.N. Shevchenko, The exchange problem, the Frobenius problem and the group minimization problem, (Russian), *Combinatorial-Algebraic methods in applied mathematics* Gors'kov. Gos. Univ. Gorki, (1982).

[421] G. Sicherman, Theory and practice of Sylver coinage, *Integers: Electron. J. Comb. Number Theory* **2**(# G2) (2002), 11 pages.

[422] E. Siering, Über lineare Formen und ein Problem von Frobenius, Dissertation, *Joh. Gutenberg-Univertät Mainz* (1974).

[423] E. Siering, Über lineare Formen und ein Problem von Frobenius, *J. Reine Angewandte Math.* **301** (1978), 161–170.

[424] R.J. Simpson and R. Tijdeman, Multi-dimensional version of a theorem of fine and Wilf and a formula of Sylvester, *Proc. Am. Math. Soc.* **131**(6) (2003), 1661–1671.

[425] T. Skolem, Über einige Satzfunktionen in der Arithmetik, (Gernman) *Skrifter Norske Vitenskapsakademiet Akad., Oslo, Math.-Naturv. KI.* **7** (1931), 1–28.

[426] Z. Skupień, Homogeneously traceable and Hamiltonian connected graphs, *Demonstratio Math.* **17** (1984), 1051–1067.

[427] Z. Skupień, A generalization of Sylvester's and Frobenius' problems on numerical semigroups, *Acta Arithmetica* **65**(4) (1993), 353–366.

[428] Z. Skupień, Exponential constructions of some nonhamiltonian minima, in: Proc. 4th Czechoslovakian Symposium on Combinatorics, Graphs and Complexity, (eds. J. Nešetřil and M. Fiedler) *Ann. Discrete Math.* **51** Elsevier (1992), 321–328.

[429] P.E. Smith, *Source Book in Mathematics* **1** and **2** Dover, New York, (1959).

[430] C. Smoryński, Skolem's solution to a problem of Frobenius, *Math. Intelligencer* **3**(3) (1980/1981), 123–132.

[431] S.L. Sobolev, The formulas of mechanical cubature on the surface of a sphere, *Sib. Mat. Zh.* **3** (1962), 769–796.

[432] G. Springer, *Introduction to Riemann Surfaces*, Addison-Wesley Publishing Company, Inc., Reading, Mass. (1957).

[433] R.P. Stanley, Hilbert functions of graded algebras, *Adv. Math.* **28** (1978), 57–83.

[434] R.P. Stanley, *Combinatorics and Commutative Algebra*, Prog. in Math., Birkhäuser **41** (1983).

[435] B.S. Stechkin and V.I. Baranov, Extremal Combinatorial problems and their application, *Mathematics and its Applications* **335**, Kluwer Acad. Publishers Group, Dordrecht, (1995).

[436] Q. Sun, Some results on diophantine equations, in Number theory and its applications in China, *Contemp. Math.* **77** (1988), 113–126.

[437] J.J. Sylvester, Problem 7382, *Educational Times* **37** (1884), 26; reprinted in: Mathematical questions with their solution, *Educational Times* (with additional papers and solutions) **41** (1884), 21.

[438] J.J. Sylvester, On the partition of numbers, *Quart. J. Pure Appl. Math.* **1** (1857), 141–152.

[439] J.J. Sylvester, On subinvariants, i.e. semi-invariants to binary quanties of an unlimited order, *Am. J. Math.* **5** (1882), 119–136.

[440] J.J. Sylvester, A constructive theory of partitions arranged in three acts, an interact and an exodion, *Am. J. Math.* **5** (1882), 251–330.

[441] L.A. Székely and N.C. Wormald, Generating functions for the Frobenius problem with 2 and 3 generators, *Math. Chronicle* **15** (1986), 49–57.

[442] M.C.K. Tweedie, A Graphical Method of Solving Tartaglian Measuring Puzzles, *Math. Gazette* **23** (1939), 278–282.

[443] B. Temkin, The problem of Frobenius for three variables, Ph.D. Thesis, *The City University of New York*, (1983).

[444] E. Teruel, P. Chrząstowski-Wachtel, J.M. Colom and M. Silva, On weighted T-systems, *Advances in Petri Nets, Lecture Notes in Computer Science* **616** (1992), 348–367.

[445] A. Thoma, Construction of set theoretic complete intersections via semigroup gluing, *Beiträge zur Algebra und Geometrie* (*Contributions to Algebra and Geometry*) **41** (1) (2000), 195–198.

[446] C. Tinaglia, Su alcune soluzioni di un problema di Frobenius in tre variabili, *Boll. U.M.I.* **7**(2) (1988), 361–383.

[447] C. Tinaglia, Some results on a linear problem of Frobenius (Italian), *Geometry Seminars, 1996–1997*, Univ. Stud. Bologna, Bologna (1998), 231–244.

[448] C. Tinaglia, Sulle soluzioni non negative di un sistema lineare diofanteo, *Riv. Mat. Univ. Parma* **13**(4) (1987), 85–90.

[449] C. Tinaglia, On the integers independent from three given positive integers, *Boll. U.M.I.* **7**(6) (1992), 1–22.

[450] C. Tinaglia, Su certi interi minimi rappresentati da forme lineari a coefficienti interi positivi, *Atti dell'Accademia di Scienze Lettere e Arti di Palermo*, Serie V-Vol. **IX**, (1988–89), 189–191.

[451] C. Tinaglia, Su un problema lineare di Frobenius in tre variabili, Convegno Per I Sessantacinque anni di Francesco Speranza, Pitagora Editrice, Bologna (1997), 140–145.

[452] F. Torres, On γ-hyperelliptic numerical semigroups, *Semigroup Forum* **55** (1997), 364–379.

[453] F. Torres, Weierstrass points and double coverings of curves. With application: symmetric numerical semigroups which cannot be realized as Weierstrass semigroups, *Manuscripta Math.* **83**(1) (1994), 39–58.

[454] A. Tripathi, The number of solutions to $ax+by=n$, *J. Fibonacci Quart.* **38** (2000), 290–293.

[455] A. Tripathi, The coin exchange problem for arithmetic progressions, *Am. Math. Monthly* **101** (1994), 779–781.

[456] A. Tripathi, On a variation of the coin exchange problem for arithmetic progressions, *Integers: Electron. J. Combinat. Number Theory* **3**(# A01) (2003), 1–5.

[457] A. Tripathi and S. Vijay, On a generalization of the coin exchange problem for three variables, manuscript (2004), 11 pages.

[458] K.M. Tsang, On the linear diophantine problem of Frobenius, *Studia Scientiarum Math. Hungarica* **23** (1998), 443–453.

[459] M.A. Tsfasman, S.G. Vlăduţ and T. Zink, Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **104** (1982), 13–28.

[460] H.J.H. Tuenter, The Frobenius problem, sums of powaer of integers and recurrences for Bernoulli numbers, *J. Numb. Theory*, to appear.

[461] J.H. van Lint, Algebraic geometric codes, Coding Theory and Design Theory, *IMA Volume in Mathematics and its Applications* **20** (1988), 137–162.

[462] H.S. Vandiver, On developments in an arithmetic theory of the Bernoulli and allied numbers, *Scripta Math.* **25** (1961), 273–303.

[463] D.E. Varberg, Pick's theorem revisited, *Am. Math. Monthly* **92** (1985), 584–587.

[464] I. Vardi, *Computational Recreations in Mathematica*, Reading, M.A., Addison-Wesley (1991), 19–20.

[465] R.S. Varga, *Matrix Interactive Analysis*, Princeton-Hall New Jersey, (1962).

[466] Y. Vitek, Bounds for a linear diophantine problem of Frobenius, *J. London Math. Soc.* **10**(2) (1974), 79–85.

[467] Y. Vitek, Bounds for a linear diophantine problem of Frobenius II, *Can. J. Math.* **28**(6) (1976), 1280–1288.

[468] B. Vizvári, Beiträge zum Frobenius-Problem, *D.Sc. Nat. Dissertation*, Technische Hohschule Carl Schorlemmer, Leuna-Merseburg, Germany (1987).

[469] B. Vizvári, On the connection of the Frobenius problem and the knapsack problem, *Coll. Math. Soc. János Bolyai, Finite and Infinite Sets* **37** (1983), 799–819.

[470] B. Vizvári, On a generalization of the Frobenius problem, *Technical Report* **MN/30** Computer and Automation Inst., Hungarian Academy of Sciences (1987).

[471] B. Vizvári, An application of Gomory cuts in number theory, *Periodica Math. Hung.* **18** (1987), 213–228.

[472] B. Vizvári, An application of an optimal behaviour of the greedy solution in number theory, *Report, 89–9. MTA Számíástechnikai és Automatizálási Kutató Intézete, Budapest* (1989).

[473] B. Vizvári, An application of an optimal behaviour of the greedy solution in number theory, *Periodica Math. Hung.* **27**(2) (1993), 69–83.

[474] B. Vizvári, Generation of uniformly distributed random vectors of good quality, Rutcor Research Report (1994), No. RRR 17–93.

[475] S. Warshall, A theorem of Boolean matrices, *J. A.C.M.* **9** (1962), 11–12.

[476] K. Watanabe, Some examples of one dimensional Gorenstein Domains, *Nagoya Math. J.* **49** (1973), 101–109.

[477] M.A. Weiss, R. Sedgewick, E. Hentschel and A. Pelin, ShellSort and the Frobenius problem, Nineteenth Southeastern Conference on Combinatorics, Graph Theory and Computing (Baton Rouge, LA, 1988) *Congressus Numerantium* **65** (1988), 253–259.

[478] E.W. Weisstein,"McNugget Number" from *MathWorld*– A Wolfram Web resource. http://mathworld.wolfram.com/McNuggetNumber.html.

[479] D.J.A. Welsh, Percolation and the random cluster model: *Combinatorial and Algorithmic Problems, Probabilistic Methods for Algorithmic Discrete Mathematics.* (eds. M. Habib, C. McDiarmid, J.L. Ramírez-Alfonsín and B. Reed) *Algorithms and Combinatorics* **16** Springer-Verlag, Berlin, (1998), 166–194.

[480] H.S. Wilf, A circle-of-lights algorithm for the "money-changing problem", *Am. Math. Monthly* **85** (1978), 562–565.

[481] H.S. Wilf, *Generatingfunctionology*, (Second edition) Academic Press, Inc. Boston, (1994).

[482] E.M. Wright, A simple proof of a known result in partitions, *Am. Math. Monthly* **68** (1961), 144–145.

[483] A. G. Xu and Z. H. Wu, The petri net method for solving first-degree indeterminate equations. III. research on the Frobenius problem (Chinese), *Shandong Kuangye Xueyuan Xuebao* **12**(1) (1993), 63–69.

[484] A.C. Yao, An analysis of $(h, k, 1)$-shellsort, *J. Algorithms* **1** (1980), 14–50.

[485] J.W. Young, On the partitions of a group and mixed perfect codes, *Bull. Am. Math. Soc.* **33** (1972), 453–461.

[486] J. Yuan, Frobenius problem for a linear form in three variables, (Chinese) *J. Southwest Teach. Univ.* Ser B **3** (1987), 10–19.

[487] O. Zariski, *Algebraic Surfaces*, Springer-Verlag, Berlin (1971).

[488] O. Zariski, *Le problème des modules pour les branches planes*, Hermann, Paris, (1986).

[489] De X. Zheng, A note on the Frobenius problem for linear forms, (Chinese) *Sichuan Daxue Xuebao* **29**(2) (1992), 188–192.

[490] N. Zhu, A relation between the knapsack and group knapsack problems, *Discrete Appl. Math.* **87**(1–3) (1998), 255–268.

[491] J. Zöllner, A note on a paper of Hofmeister, *Bull. Iranian Math. Soc.* **8**(2) (1980/81), 157–160.

[492] J. Zöllner, Über angenehme Mengen, *Mainzer Seminarberichte in additiver Zahlentheorie* **1** (1983), 53–71.

This page intentionally left blank

Index

$(a_1, \ldots, a_n)$, 1
$(a_1, \ldots, a_n)$-tree, 128
$< s_1, \ldots, s_n >$, 135
$H(M, z)$, 197
$H_M(t)$, 197
$N(a_1, \ldots, a_n)$, 103
$S(s_1, \ldots, s_n)$, 135
$[a_1, \ldots, a_n]$, 57
$\gamma(B)$, 11
$\mu(S)$, 135
$d(m; a_1, \ldots, a_n)$, 72
$f(a_1, \ldots, a_n, t) = f(n, t)$, 119
$g(S)$, 135
$g(a_1, \ldots, a_n)$, 1
$h(a_1, \ldots, a_n, t) = h(n, t)$, 123
$i(P, t)$, 92
$p(m)$, 71

Apéry set, 149

balls and cells problem, 175
basis, 1
  Hilbert, 132
  regular, 62
Bell's method, 78
Bernoulli numbers, 112, 198

code
  algebraic geometric, 171
  designed minimum distance
    Feng-Rao, 173
    Goppa, 173
  evaluation, 173
    dual, 173
conjugate power equation, 178
convex set, 91
covering radius, 22
cubature formula, 179
  m-property, 179
cube-figure, 7
cutting stock problem, 96

Davison's algorithm, 5
decision problem, 185
Dedekind sums, 95
denumerant, 72

Ehrhart polynomial, 92
  reciprocity law, 92

Frobenius
  directed graph, 12
  minimal graph, 15
  number, 1
  problem **FP**, 1
function
  Kronecker delta, 153
  Möbius, 153
  partition, 71
  subadditive, 55

Gomory cuts, 67
Gorenstein condition, 107
graded
  Hilbert syzygy theorem, 196
  resolution, 196
graph
  F-Hamiltonian, 182
  connected, 194
  cycle, 194
  Hamiltonian, 181
  homogenously traceable, 182
  hypo-Hamiltonian, 181
  path, 194

graph (*cont.*)
  Petersen, 181
  strongly connected, 194
  traceable, 182
Greenberg's algorithm, 18

Heap and Lynn method, 11
Hilbert
  function, 197
  serie, 197
HNN group, 178

Johnson integers, 42
jugs problem, 114

Kannan's method, 21
Killingbergtrø's algorithm, 6
Knapsack
  problem, 53
    integer, 25

liveness problem, 162

matrix
  dominating, 157
  graded, 196
  index of primitivity, 11, 202
  irreducible, 11, 200
  mixed, 157
  non-negative, 11
  permutation, 200
  positive, 11
  primitive, 11
  reducible, 11, 200
maximal lattice free body, 8
modular change problem, 124
module, 194
  free, 195
  graded, 195
  projective, 195
  regrading, 195
  shift, 196
money-changing problem, 1
monoid, 55
monomial curve, 142

Nijenhuis' algorithm, 19

partition vector space problem, 165
Petri net, 161
Pick's theorem, 32
place/transition net, 161
  pure, 162
  system, 162
    dead, 162
    live, 162
    weighted circuit, 163
polygon
  lattice, 32
  simple, 32
polytope
  convex, 91
  face, 92
  facet, 92
  integral, 92
  rational, 92
postage stamp problem, 127
  global, 133
pseudo-conductor, 130
  m-conductor, 133

quantifier elimination, 45
quasipolynomial, 93

random vector algorithm, 180
Rødseth's algorithm, 3

Scarf and Shallcross' algorithm, 9
semigroup, 135
  γ-hyperelliptic, 154
  Arf numerical, 156
  Buchweitz, 155
  complete intersection, 152
  conductor, 135
  critical number, 157
  derived, 146
  embedding dimension, 135
  free, 140
  gaps, 135
    fundamental, 155
  genus, 135

hyperelliptic, 140
irreducible, 148
multiplicity, 135
non-gaps, 135
numerical, 135
pseudo-symmetric, 146
ring, 87
Schubert index, 156
symmetric, 141
telescopic, 139
toric ideal of, 197
type, 142
Weierstrass, 154
sequence
almost arithmetic, 29
almost chain, 29
arithmetic, 59
chain, 29
chain-divisible, 98
flat, 58
independent, 38
pleasant, 127
saturated, 122
strongly flat, 58
superincreasing, 98
telescopic, 139
type of, 151
Shell-sort method, 159, 197
Skupień's algorithm, 125
Sylver coinage game, 113

tessalation, 174
tiling, 174
Turing reduction, 194

unimodular zonotope, 92

Wilf's algorithm, 19

Zorn's Lemma, 143