Applications of Group Theory to Combinatorics

Editors

Jack Koolen
Jin Ho Kwak
Ming-Yao Xu

CRC Press
Taylor & Francis Group
A BALKEMA BOOK

APPLICATIONS OF GROUP THEORY TO COMBINATORICS

SELECTED PAPERS FROM THE COM^{2}MAC CONFERENCE ON APPLICATIONS OF GROUP THEORY TO COMBINATORICS, POHANG, KOREA, 9–12 JULY 2007

Applications of Group Theory to Combinatorics

Editors

Jack Koolen

Department of Mathematics, Pohang University of Science
and Technology, Pohang 790–784, Korea

Jin Ho Kwak

Department of Mathematics, Pohang University of Science
and Technology, Pohang 790–784, Korea

Ming-Yao Xu

Department of Mathematics, Peking University, Beijing 100891, P.R. China

CRC Press
Taylor & Francis Group
Boca Raton London New York Leiden

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A BALKEMA BOOK

Supported by Com^{2}MaC-KOSEF, Korea

CRC Press/Balkema is an imprint of the Taylor & Francis Group, an informa business

Typeset by Vikatan Publishing Solutions (P) Ltd., Chennai, India
Printed and bound in Great Britain by Anthony Rowe (A CPI-group Company),
Chippenham, Wiltshire

Although all care is taken to ensure integrity and the quality of this publication and the information herein, no responsibility is assumed by the publishers nor the author for any damage to the property or persons as a result of operation or use of this publication and/or the information contained herein.

Published by: CRC Press/Balkema
P.O. Box 447, 2300 AK Leiden, The Netherlands
e-mail: Pub.NL@taylorandfrancis.com
www.crcpress.com – www.taylorandfrancis.co.uk – www.balkema.nl

ISBN: 978-0-415-47184-8 (Hardback)
ISBN: 978-0-203-88576-5 (ebook)

Applications of Group Theory to Combinatorics - Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Table of Contents

Applications of Group Theory to Combinatorics - Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Foreword

The 2007 Com^{2}MaC International Workshop on Applications of Group Theory to Combinatorics was held at Pohang University of Science and Technology on July 9–12, 2007 under the sponsorship of the Combinatorial and Computational Mathematics Center. The aim of the meeting was to bring together some foremost experts in the areas of combinatorics, group theory and combinatorial topology in order to stimulate mutual understandings, communications and researches among all the participants. Presented and discussed topics encompass quite a diverse spectrum, such as coding theory, design theory, Belyi functions, distance-regular graphs, transitive graphs, regular maps, and Hurwitz problems.

Among the about 70 participants from Australia, China, France, Japan, Korea, Netherlands, New Zealand, Russia, Singapore, Slovakia, Slovenia, United Kingdom and United States of America, 27 invited speakers presented their results. This volume contains 11 papers of invited talks at the workshop which mark the vitality and enthusiasm during the workshop.

Marston Conder gives a brief summary of various aspects of combinatorial group theory and associated computational methods, with special reference to finitely-presented groups and their applications, found useful in the study of graphs, maps and polytopes having maximal symmetry. He discusses recent computational results and how this led to new general results in the theory of maps.

Yan-Quan Feng, Zai-Ping Lu and Ming-Yao Xu give a brief survey of recent results on automorphism groups of Cayley digraphs concentrating on the normality of Cayley digraphs.

Michael Giudici, Cai Heng Li and Cheryl E. Praeger introduce three new types of combinatorial structures associated with group actions, namely symmetrical covers, symmetrical decompositions, and symmetrical factorisations of graphs. These structures are related to and generalise various combinatorial objects, such as 2-designs, regular maps, near-polygonal graphs, and linear spaces. General theory is developed for each of these structures, pertinent examples and constructions are given, and a number of open research problems are posed.

Gareth Jones surveys recent progress on the combinatorial problem of classifying the orientably regular embeddings of complete bipartite graphs. The motivation for this problem comes from two main areas, topological graph theory and arithmetic algebraic geometry, while the techniques required to solve it come from a third area, finite group theory—specifically the theories of factorisable groups and of finite solvable groups.

Goansu Kim and C.Y. Tang discuss separability properties of groups. They discuss S-separable groups, in particular, residually finite groups, subgroup separable groups and conjugacy separable groups.

Jin Ho Kwak, Jaeun Lee and Alexander Mednykh discuss the enumeration problem for (branched) coverings of Riemann surfaces and, more generally, graphs, manifolds and orbifolds with finitely generated fundamental group. They present some well-known results in this field, recent developments of the problem and indicate a general approach to solve the problem in the high-dimensional case. They cover group-theoretical, combinatorial and topological view points on the problem.

Sergei Lando surveys recent progress in understanding Hurwitz numbers, with stress made on their combinatorial rather than geometric nature. Hurwitz numbers enumerate ramified coverings of two-dimensional surfaces. They have many other manifestations in other fields such as in group theory, combinatorics, algebraic topology and mathematical physics.

Huiling Li discusses the applications of finite permutation groups to combinatorial designs. He discusses block transitive $2-(v,k,1)$ designs with k small and how classical groups act on designs.

Martin Mačaj, Jozef Širáň and Mária Ipolyiová survey the algebraic background for constructing representations of triangle groups in linear groups over algebras arising from quotients of multivariate polynomial rings, leading to improvements of upper bounds on the order of epimorphic images of triangle groups with a given injectivity radius and to bounds on the size of the associated hypermaps with a given planar width.

Tom Tucker views the various genus parameters for finite groups in the broader context of 'sizings' of groups, that is, order-preserving functions from the collection of all finite groups to the natural numbers. He discusses topics like the range of a sizing and whether a sizing provides a certificate of isomorphism. Also he discusses asymptotic behavior of several sizings.

Alexander Zvonkin studies Belyi functions, also known as *dessins d'enfants*. These functions provide a link between many important theories, namely Riemann surfaces, Galois theory, and the theory of combinatorial maps. More generally, many properties of functions, surfaces, fields, and groups in question may be "read from" the corresponding pictures, or sometimes constructed in a "picture form". Group theory is related to all the above subjects and therefore plays a central role in the theory of Belyi functions.

The organizers truly thank Ministry of Science and Technology of Korea and the Korean Science and Engineering Foundation for their financial support for this successful workshop.

Jack Koolen
Jin Ho Kwak
Ming-Yao Xu

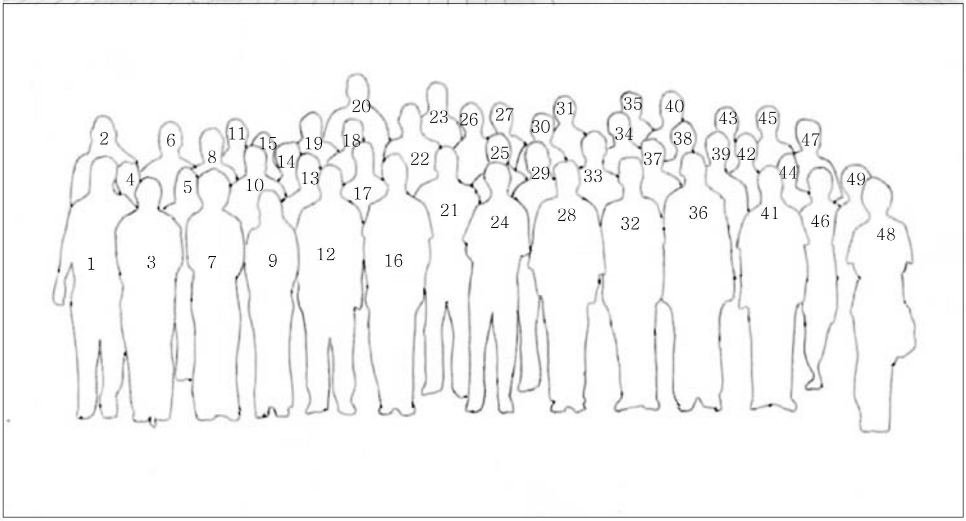
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

About the editors

Jack Koolen teaches in the Department of Mathematics at the Pohang University of Science and Technology. His main research interests lie in the interaction of geometry, linear algebra and combinatorics. He has published more than 60 papers in these areas.

Jin Ho Kwak is a professor in the Department of Mathematics at the Pohang University of Science and Technology and the director of the Combinatorial and Computational Mathematics Center (Com^{2}MaC). He works on combinatorics and topology, mainly on covering enumeration related to Hurwitz problems and regular maps on surfaces. He has published more than 100 papers in these areas.

Ming-Yao Xu is a professor in the Department of Mathematics at Peking University. He works on finite group theory and algebraic graph theory. His main research interests lie in finite *p*-groups and the interaction of groups and graphs. He has published more than 80 papers in these areas.



1. Jack Koolen
2. Aleksander Malnič
3. Tatsuro Ito
4. Rongxia Hao
5. Chuixiang Zhou
6. Jin-Xin Zhou
7. Cheryl E. Praeger
8. Yan-Quan Feng
9. Klavdija Kutnar
10. Sergei K. Lando
11. Weili He
12. Marston Conder
13. Young Soo Kwon
14. Han Guk Kang
15. Sanming Zhou
16. Jin Ho Kwak
17. Huiling Li
18. Jozef Širáň
19. Alexander Zvonkin
20. Roman Nedela
21. Alexander D. Mednykh
22. Brian Alspach
23. Primož Šparl
24. Gareth A. Jones
25. Francis C.Y. Tang
26. Thomas W. Tucker
27. Oyeon Kum
28. Mingyao Xu
29. Shaofei Du
30. Haipeng Qu
31. Moo Young Sohn
32. Jaeun Lee
33. Goansu Kim
34. Young Gheel Baik
35. Kijung Kim
36. Reza Sharafdini
37. Maozhi Xu
38. San Ling
39. Cai Heng Li
40. Jongyook Park
41. Eiichi Bannai
42. Jae Ho Lee
43. Kyoung-tark Kim
44. Wang Yan
45. Yoshio Sano
46. Jing Xu
47. Zaiping Lu
48. Sejeong Bang
49. Mitsugu Hirasaka

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Combinatorial and computational group-theoretic methods in the study of graphs, maps and polytopes with maximal symmetry

Marston Conder[1]
Department of Mathematics, University of Auckland, Auckland, New Zealand

ABSTRACT: This paper gives a brief summary of various aspects of combinatorial group theory and associated computational methods, with special reference to finitely-presented groups and their applications, found useful in the study of graphs, maps and polytopes having maximal symmetry. Recent results include the determination of all arc-transitive cubic graphs on up to 2048 vertices, and of all regular maps of genus 2 to 100, and construction of the first known examples of finite chiral 5-polytopes. Moreover, patterns in the maps data have led to new theorems about the genus spectrum of chiral maps and regular maps with simple underlying graph.

2000 Mathematics Subject Classification: 20B25 (primary), 05C25, 20F05, 52B15, 57M60 (secondary).

1 INTRODUCTION

This paper is intended to give a brief summary of various aspects of combinatorial group theory and associated computational methods that have proved useful (to the author, at least) in the study of graphs, maps and polytopes having maximum possible symmetry under certain conditions. It extends (and updates) an earlier summary given in [9], but is not intended to be a comprehensive survey, by any means. Our aim is to provide examples of potential interest to students and others wishing to learn about the use of such theory and methods, together with some references to places where further details are available.

Special focus is given to finitely-presented groups and means of investigating them (and their subgroups of finite index and quotients of finite order), with numerous applications.

We begin by giving some background on symmetries of discrete structures and their connection with certain finitely-presented groups, in Section 2. Then in Section 3 we briefly describe some ways in which Schreier coset diagrams can be used to depict and construct homomorphic images of these groups, and give some applications to exhibit the remarkable power of such an approach. We summarise a number of computational procedures for handling finitely-presented groups in Section 4, and then look at the particular case of methods for finding subgroups of small index and quotient of small order, in Section 5. Finally, we describe a theorem of Schur about centre-by-finite groups and its use in these contexts in Section 6, and complete the paper by announcing some recent results about the genus spectra of various classes of arc-transitive maps in Section 7.

[1] Research supported in part by the N.Z. Marsden Fund, Grant UOA 412.

2 BACKGROUND: SYMMETRIES OF DISCRETE STRUCTURES, AND CONNECTIONS WITH FINITELY-PRESENTED GROUPS

2.1 *Symmetric graphs*

An *automorphism* of a (combinatorial) graph $X = (V, E)$ is any permutation of its vertices that preserves adjacency. Under composition, the set of all automorphisms of X forms a group known as the *automorphism group* of X and denoted by $\mathrm{Aut}X$. A graph X is called *vertex-transitive*, *edge-transitive* or *arc-transitive* automorphism group $\mathrm{Aut}X$ has a single orbit on the set of vertices, edges or arcs (ordered edges) of X, respectively. Graphs which are arc-transitive are also called *symmetric*, and any graph that is edge-transitive but not vertex-transitive is called *semisymmetric*.

More generally, for any positive integer s, an *s-arc* in a graph X is a directed walk of length s which never includes the reverse of an arc just crossed—that is, an ordered $(s+1)$-tuple of vertices $(v_0, v_1, v_2, \ldots, v_{s-1}, v_s)$ such that any two consecutive v_i are adjacent in X and any three consecutive v_i are distinct. A graph X is then called s-arc-transitive if $\mathrm{Aut}X$ has a single orbit on the set of arcs of X. For example, circuit graphs are s-arc-transitive for all s, while the cube graph Q_3 and all complete graphs on more than three vertices are 2-arc-transitive but not 3-arc-transitive.

The situation for arc-transitive 3-valent graphs (also called symmetric *cubic* graphs) is particularly interesting. In [32, 33] Tutte proved that if G is the automorphism group of a finite symmetric cubic graph, then G is sharply-transitive on the set of s-arcs of X for some $s \leq 5$ (in which case X is called *s-arc-regular*). The smallest example of a finite 5-arc-regular cubic graph is Tutte's 8-cage, on 30 vertices, depicted in Figure 1.

By further theory of symmetric cubic graphs (developed by Tutte, Goldschmidt, et al), it is now known that if X is a 5-arc-regular cubic graph, then $\mathrm{Aut}X$ is a homomorphic image of the finitely-presented group

$$\begin{aligned} G_5 = \langle\, h, a, p, q, r, s \mid {} & h^3 = a^2 = p^2 = q^2 = r^2 = s^2 = 1, \\ & pq = qp,\ pr = rp,\ ps = sp,\ qr = rq,\ qs = sq,\ sr = pqrs, \\ & ap = qa,\ ar = sa,\ h^{-1}ph = p,\ h^{-1}qh = r,\ h^{-1}rh = pqr,\ shs = h^{-1} \,\rangle, \end{aligned}$$

with the subgroups $H = \langle h, p, q, r, s\rangle$, $A = \langle a, p, q, r, s\rangle$ and $H \cap A = \langle p, q, r, s\rangle$ mapping to the stabilizers of a vertex, edge and arc, respectively.

Conversely, given any epimorphism $\theta : G_5 \to G$ to a finite group G, with torsion-free kernel K, a cubic graph X may be constructed on which G acts 5-arc-regularly: Take as vertices the

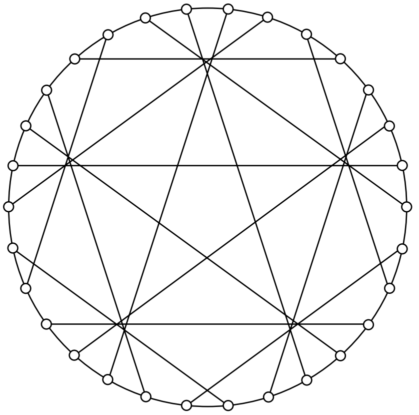


Figure 1. Tutte's 8-cage.

right cosets of $V = HK$ in G_5, and join Vx to Vy by an edge whenever $xy^{-1} \in VaV$. Under right multiplication by G_5, the stabilizer of the vertex V is V, which induces S_3 on the neighbourhood $\{Ha, Hah, Hah^{-1}\}$ of H, and the group induced on X is $G_5/K \cong G$. Thus 5-arc-regular cubic graphs correspond to non-degenerate homomorphic images of the group G_5. See [18] for further details.

Tutte's work for symmetric 3-valent graphs was extended by Richard Weiss to the study of finite symmetric graphs of arbitrary valency, using the classification of doubly-transitive permutation groups. In particular, Weiss proved the following generalisation of Tutte's theorem in [34, 35]:

Theorem 1. (Weiss, 1981 & 1987) *There are no finite k-arc-transitive graphs of degree > 2 for $k \geq 8$. Moreover, if X is a finite 7-arc-transitive graph of degree $d > 2$, then $d = 3^t + 1$ for some positive integer t, and $G = \mathrm{Aut}X$ is obtainable as a homomorphic image of a certain finitely-presented group $R_{d,7}$.*

For example, $R_{4,7}$ has a presentation in terms of generators $p, q, r, s, t, u, v, h, b$ subject to defining relations that include $h^4 = p^3 = q^3 = r^3 = s^3 = t^3 = u^3 = v^2 = b^2 = 1, (hu)^3 = (uv)^2 = (huv)^2 = [h^2, u] = [h^2, v] = 1$, $[s, t] = p$, $[q, r] = 1$, and so on, and the automorphism group of every finite 7-arc-transitive 4-valent graph is a non-degenerate homomorphic image of this group $R_{4,7}$.

2.2 *Regular maps*

A *map* is a 2-cell embedding of a connected (multi)graph in a surface, and an automorphism of a map M is any permutation of its edges that preserves incidence. A map M is called *regular* if its automorphism group $\mathrm{Aut}\,M$ is sharply-transitive (regular) on flags, that is, on incident vertex-edge-face triples. Similarly, a map M on an orientable surface is called *rotary* (or *orientably-regular*) if the group of all its orientation-preserving automorphisms is transitive on the ordered edges of M.

If M is rotary or regular then every face has the same number of edges (say p) and every vertex has the same valency (say q), and M has *type* $\{p, q\}$. Regular maps of type $\{p, q\}$ correspond to non-degenerate homomorphic images of the full $(2, p, q)$ triangle group $\Delta = \langle\, a, b, c \mid a^2 = b^2 = c^2 = (ab)^p = (bc)^q = (ac)^2 = 1\rangle$; the image of $\langle a, b\rangle$ gives the stabilizer of a vertex v, the image of $\langle a, c\rangle$ gives the stabilizer of an edge e, and the image of $\langle b, c\rangle$ gives the stabilizer of a face f, where (v, e, f) is a flag, and incidence corresponds to non-empty intersection of cosets. Similarly, rotary

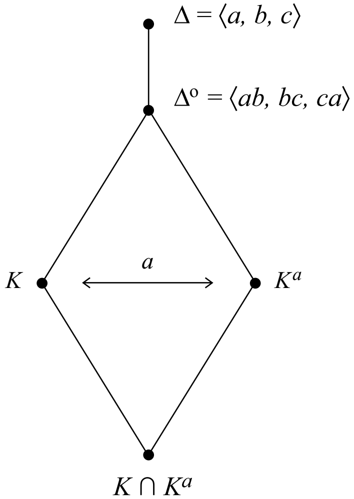

$\Delta = \langle a, b, c\rangle$
$\Delta^{\mathrm{o}} = \langle ab, bc, ca\rangle$
K
a
K^a
$K \cap K^a$

Figure 2. Chirality in terms of normal subgroups of Δ^{o}.

maps of type $\{p,q\}$ correspond to non-degenerate homomorphic images of the ordinary $(2,p,q)$ triangle group $\Delta^{\rm o} = \langle x,y,z \mid x^p = y^q = z^2 = xyz = 1 \rangle$, which has index 2 in Δ (when x,y,z are taken as ab, bc, ca respectively). See [12] for further details.

If the rotary map M of type $\{p,q\}$ admits no orientation-reversing automorphisms, then M is said to be irreflexible, or *chiral*, and $\mathrm{Aut}\,M$ is a quotient of the ordinary $(2,p,q)$ triangle group $\Delta^{\rm o}$ but not the full $(2,p,q)$ triangle group Δ. In that case, the kernel K of the corresponding epimorphism $\theta\colon \Delta^{\rm o} \to \mathrm{Aut}\,M$ is not normal in Δ. Indeed if M is rotary and $\theta\colon \Delta^{\rm o} \to \mathrm{Aut}\,M$ is the corresponding non-degenerate homomorphism, then M is reflexible if and only if K is normalized by any element $a \in \Delta \setminus \Delta^{\rm o}$:

If the subgroup K is not so normalized, then the rotary map M is chiral and K^a is the kernel of the corresponding epimorphism for the mirror image of M.

2.3 *Abstract polytopes*

An abstract *polytope* of rank n is a partially ordered set $\mathcal{P}$ endowed with a strictly monotone rank function having range $\{-1,\dots,n\}$. The elements of rank $0, 1$ and $n-1$ are called the *vertices*, *edges* and *facets* of the polytope, respectively. For $-1 \le j \le n$, elements of $\mathcal{P}$ of rank j are called the *j-faces*, and a typical j-face is denoted by F_j. We require that $\mathcal{P}$ have a smallest (-1)-face F_{-1}, and a greatest n-face F_n, and that each maximal chain (or *flag*) of $\mathcal{P}$ has length $n+2$, and is of the form $F_{-1} - F_0 - F_1 - F_2 - \cdots - F_{n-1} - F_n$.

This poset $\mathcal{P}$ must satisfy certain combinatorial conditions which generalise the properties of geometric polytopes. One requirement is a kind of homogeneity property, called the *diamond condition*: whenever $F \le G$, with $\mathrm{rank}(F) = j-1$ and $\mathrm{rank}(G) = j+1$, there are exactly two j-faces H_i such that $F \le H_i \le G$. It is further required that $\mathcal{P}$ be *strongly flag-connected*, which means that any two flags Φ and Ψ of $\mathcal{P}$ can be joined by a sequence of flags $\Phi = \Phi_0, \Phi_1, \dots, \Phi_k = \Psi$ such that each two successive faces Φ_{i-1} and Φ_i are adjacent (that is, differ in only one face), and $\Phi \cap \Psi \subseteq \Phi_i$ for all i.

An *automorphism* of an abstract polytope $\mathcal{P}$ is an order-preserving bijection $\mathcal{P} \to \mathcal{P}$. A polytope $\mathcal{P}$ is *regular* if the automorphism group $\Gamma(\mathcal{P})$ is transitive on the flags of $\mathcal{P}$.

When $\mathcal{P}$ is regular, $\Gamma(\mathcal{P})$ can be generated by n involutions $\rho_0, \rho_1, \dots, \rho_{n-1}$, where each ρ_i maps a given *base flag* Φ to the adjacent flag Φ^i (differing from Φ only in its i-face). These generators satisfy (among others) the defining relations for the *Coxeter group* of *Schläfli type* $[p_1,\dots,p_{n-1}]$, where $p_i = o(\rho_{i-1}\rho_i)$ for $1 \le i < n$.

The generators ρ_i for $\Gamma(\mathcal{P})$ also satisfy an extra condition known as the *intersection condition*, namely $\langle\, \rho_i : i \in I \,\rangle \cap \langle\, \rho_i : i \in J \,\rangle = \langle\, \rho_i : i \in I \cap J \,\rangle$ for every $I, J \subseteq \{0,1,\dots,n-1\}$.

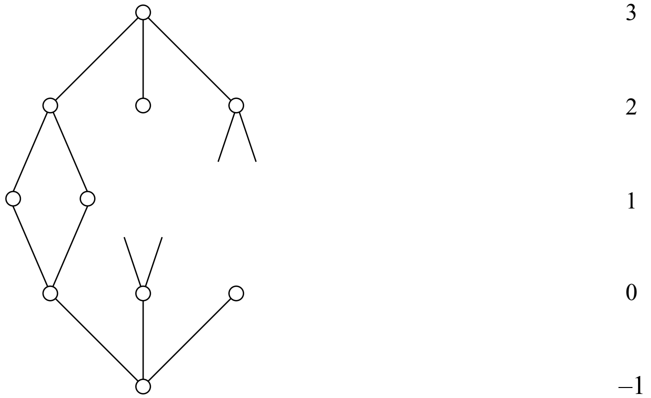


Figure 3. Partial illustration of a 3-polytope.

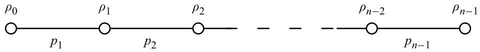


Figure 4. Dynkin diagram for the Coxeter group $[p_1, \ldots, p_{n-1}]$.

Conversely, if Γ is a permutation group generated by n elements $\rho_0, \rho_1, \ldots, \rho_{n-1}$ which satisfy the defining relations for a Coxeter group of rank n and satisfy the intersection condition, then there exists a polytope $\mathcal{P}$ with $\Gamma(\mathcal{P}) \cong \Gamma$.

Similarly, *chiral* polytopes of rank n are obtainable from certain non-degenerate homomorphic images of the 'even-word' subgroups $\langle\, \rho_{i-1}\rho_i : 1 \le i < n \,\rangle$ of these n-generator Coxeter groups. The automorphism group of a chiral polytope has two orbits on flags, with adjacent flags always lying in different orbits.

See [15, 29] (and references therein) for further details.

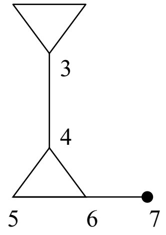
3 SCHREIER COSET DIAGRAMS

Given a transitive permutation representation of a finitely-generated group G on a set Ω, the effect of the generators of G on Ω can be depicted by a graph with Ω as vertex-set, and edges joining α to α^x for each point $\alpha \in \Omega$ and every element x in some generating set for G. Such a graph is known as a *Schreier coset graph* (or *coset diagram*) because, equivalently, given a subgroup H of G, the effect of the generators of G by right multiplication on right cosets of H can be depicted by the same graph, with Ω taken as the coset space $(G\!:\!H)$, and edges joining Hg to Hgx for every generator x. (The correspondence is obtained by letting H be the stabilizer of any point of Ω.) See [25, 8] for further details.

For example, Figure 5 gives a coset diagram for an action of the ordinary $(2,3,7)$ triangle group $\langle x,y \mid x^2 = y^3 = (xy)^7 = 1\rangle$ on 7 points, in which the triangles and heavy dot depict 3-cycles and the fixed point of the permutation induced by the generator y:

Often two Schreier coset diagrams for the same group G on (say) m and n points can be *composed* to produce a transitive permutation representation of larger degree $m+n$. This technique (attributable to Graham Higman) can be used in some instances to construct families of epimorphic images of the given group G (and interesting objects on which they act), and to prove that G is infinite. For example, one method of composition of coset graphs for the ordinary $(2,3,7)$ triangle group is illustrated in Figure 6.

This method was used to prove, for example, that for every integer $m \ge 7$, all but finitely alternating and symmetric groups are epimorphic images of the $(2,3,m)$ triangle group—and hence for all but finitely many n, there exists a rotary map M of type $\{3,m\}$ with A_n or S_n as its orientation-preserving group of automorphisms (see [5]). In fact all those maps are regular, but the same method can be adapted to prove that for all $m \ge 7$ and for all but finitely many n (for each m), there exists a chiral map M of type $\{3,m\}$ with $\mathrm{Aut}(M) \cong A_n$ (see [3]). More generally, Brent



$$x \mapsto (3,4)\,(6,7)$$

$$y \mapsto (1,2,3)\,(4,5,6)$$

Figure 5. Example of a coset diagram.

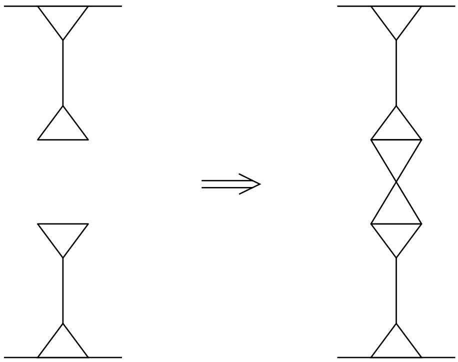


Figure 6. Composition of coset graphs for the ordinary $(2,3,7)$ triangle group.

Everitt has proved that every Fuchsian group has all but finitely many A_n among its epimorphic images; see [27].

A variant of this method of composition can be used to prove that there are infinitely many 5-arc-transitive connected finite cubic graphs [6], and infinitely many 7-arc-transitive connected finite 4-valent graphs [24]. A more careful analysis shows even that there are infinitely many 5-arc-transitive 3-valent finite *Cayley graphs*, and that every such Cayley graph is a cover of one of just six examples, and that for every positive integer t, there are infinitely many 7-arc-transitive finite Cayley graphs of valency $1+3^t$ (see [10]).

4 COMPUTATIONAL PROCEDURES

The last 40 years have seen the development of a wide range of efficient computational procedures for investigating groups with a small number of generators and defining relations. Here we give a brief description of some of those which are very useful in the kinds of contexts mentioned earlier in this paper. All of these procedures are available in the MAGMA package [1]. For further details and references, see the very helpful books on computational group theory by Sims [31] and Eick, Holt & O'Brien [28].

- Todd-Coxeter coset enumeration: This attempts to determine the index of a given finitely-generated subgroup H in a given finitely-presented group $G = \langle X \mid R \rangle$, by systematically enumerating the right cosets of H in G; when it succeeds, the output can given in the form of a *coset table* (in which the (i,j)th entry indicates the number of the coset obtained by multiplying the ith coset of H by the jth generator of G), or as permutations induced by the generators of G on right cosets of H.
- Reidemeister-Schreier algorithm: This gives a defining presentation for a subgroup H of finite index in a finitely-presented group $G = \langle X \mid R \rangle$, when the coset table is known; the generators for H are Schreier generators (obtainable from a Schreier transversal for H in G, which can be identified with a rooted spanning tree for the corresponding coset graph for $(G:H)$), and the relations are easily derived from the coset table and the relations for G (or by 'chasing' each relation for G around the coset diagram).
- Abelian quotient algorithm: This produces the direct factors of the abelianisation $G/G' = G/[G,G]$ of a finitely-presented group $G = \langle X \mid R \rangle$, in Smith normal form. When taken together with a variant of the Reidemeister-Schreier algorithm, it can also determine the abelianisation H/H' of a subgroup H of finite index in G, when the coset table for H in G is known.
- Low index subgroups algorithm: This finds a representative of each conjugacy class of subgroups of up to a given index n in a finitely-presented group $G = \langle X \mid R \rangle$, and will be explained further in the next Section.

- p-quotient algorithm: This finds, for a given prime p and a given positive integer c, the largest possible quotient P of the finitely-presented group $G = \langle X \mid R\rangle$ with the property that P is a p-group of class at most c; for example, when $c = 1$ or 2 this is the largest abelian or metabelian p-quotient, respectively.
- Nilpotent quotient algorithm: This finds, for a given positive integer c, the largest possible nilpotent quotient of the finitely-presented group $G = \langle X \mid R\rangle$ of class at most c; for example, when $c = 1$ or 2 this is the largest abelian or metabelian quotient, respectively.

5 LOW INDEX SUBGROUPS METHODS

Given a finitely-presented group $G = \langle X \mid R\rangle$ and a (small) positive integer n, all subgroups of index up to n in G can be found (up to conjugacy) by a systematic enumeration of coset tables with up to n rows. In practice, this is achieved by using an extended coset table, which includes the effect of multiplying cosets of the (pseudo-) subgroup by the inverses of the elements of the generating set X for G, as depicted below:

Such tables are assumed to be in *normal form*, which means that lexicographically, no coset number j appears for the first time before a coset number k less than j. The enumeration procedure usually defines more than n cosets, and then coincidences are forced between cosets. As cosets Hv and Hw of a subgroup H are equal if and only if $vw^{-1} \in H$, forcing any coincidence gives rise to a new element of the subgroup, which is then taken as an additional generator of the subgroup. The fact that every subgroup of finite index in G is finitely-generated (by Schreier's theorem) ensures that this procedure will terminate, given sufficient time and memory. See [31, 28, 14] for further details and references.

A key point about the low index subgroups algorithm is that it can be used to find 'small' finite epimorphic images of a finitely-presented group G: for each subgroup H of index n in G, the permutations induced by generators of G on right cosets of H generate the factor group G/K where K is the core of H (the intersection of all conjugates of H) in G, as a subgroup of S_n.

These images can often be used as the 'building blocks' for the construction of larger images (as in Section 3), or produce interesting examples in their own right. For instance, the first known examples of arc-transitive cubic graphs admitting no edge-reversing automorphisms of order 2, and first known 5-arc–transitive cubic graph having no s-arc-regular group of automorphisms for $s < 5$, were found in this way (see [18]). The same approach was used to help construct infinite family of 4-arc-transitive connected finite cubic graphs of girth 12, and then (unexpectedly) to a new symmetric presentation for the special linear group $\mathrm{SL}(3, \mathbb{Z})$; see [7]. Similarly, it enabled the construction of a infinite family of vertex-transitive but non-Cayley finite connected 4-valent graphs with arbitrarily large vertex-stabilizers in their automorphism groups [23], the first known example of a finite half-arc-transitive (vertex- and edge-transitive but not arc-transitive) 4-valent finite graph with non-abelian vertex-stabilizer [20], and the first known examples of finite chiral polytopes of rank 5 [15].

Two drawbacks of the (standard) low index subgroups algorithm are the fact that the finite quotients it produces can have large order but small minimal degree (as permutation groups), and

	x_1	x_2	...	x_1^{-1}	x_2^{-1}	...
1	2	3		4		
2				1		
3					1	
4	1					
:						

Figure 7. An extended coset table.

the fact that it tends to be very slow for large index n or complicated presentations. (Also for some groups, like the modular group $\langle x, y \mid x^2, y^3 \rangle$, the number of subgroups grows exponentially, making it impossible to search very far.)

It is not difficult, however, to adapt the algorithm so that it produces only normal subgroups (of up to a given index), and this adaptation runs much more quickly (for given maximum) index, and hence can produce all quotients of up to a given order, not just those which have faithful permutation representations of small degree.

Such an adaptation was developed by the author and Peter Dobcsányi (as part of Peter's PhD thesis project), and applied to find all rotary and regular maps on orientable surfaces of genus 2 to 15, all regular maps on non-orientable surfaces of genus 2 to 30, and all arc-transitive cubic graphs on up to 768 vertices; see [12, 13]. It was also subsequently used to help find all semisymmetric cubic graphs on up to 768 vertices [19], and to assist in obtaining a refined classification of arc-transitive group actions on finite cubic graphs (by types of arc-transitive subgroups) [21].

Recently, a new method for finding normal subgroups of small index has been developed by Derek Holt and his student David Firth. This systematically enumerates the possibilities for the composition series of the factor group G/K (for any normal subgroup K of small index in G), and works much faster, for index up to 100,000 in many groups with straightforward presentations. It too has been implemented in the Magma package [1].

This new method has enabled the determination of all rotary and regular maps (and hypermaps) on orientable surfaces of genus 2 to 101, all regular maps on non-orientable surfaces of genus 2 to 202, and all arc-transitive cubic graphs on up to 2048 vertices (and thereby the accidental discovery of largest known cubic graph of diameter 10); see [11]. Consequences of finding patterns in the list of maps of small genus will be described in Section 7.

6 SCHUR'S THEOREM

A particularly useful (but not so well known) piece of combinatorial group theory is *Schur's theorem* on centre-by-finite groups.

Theorem 2 (Schur). *If the centre $Z(G)$ of the group G has finite index $|G : Z(G)| = m$ in G, then the order of every element of $G' = [G, G]$ is finite and divides m.*

Closely tied to the Schur-Zassenhaus theorem, this theorem can be proved easily using the transfer homomorphism $\tau : G \to Z(G)$ (which takes $g \mapsto g^m$ for all $g \in G$), once it is noted that $\ker \tau$ contains G'. See [30] for further background and details.

The author is grateful to Peter Neumann for pointing out the usefulness of Schur's theorem in order to obtain the following in some work with Ravi Kulkarni on families of automorphism groups of compact Riemann surfaces:

Theorem 3 [16]. *Let p, q and d be positive integers, with $\gcd(p, q) = 1$. Then there are only finitely many finite groups which can be generated by two elements x and y of orders p and q respectively such that xy generates a subgroup of index at most d.*

In turn, the above helps disprove the possibility that certain cyclic-by-finite groups might be rotation groups of orientably-regular maps. For example, suppose the map M is a 'central cover' of the octahedral map, of type $\{3, 4t\}$ for some t, with rotation group $G = \mathrm{Aut}^{\mathrm{o}} M \cong \langle x, y, z \mid x^3 = y^{4t} = (xy)^2 = 1,\ [x, y^4] = 1 \rangle$. How large can t be? Here we may note that $Z(G)$ contains $N = \langle y^4 \rangle$, with $G/N \cong S_4$, so $|G : Z(G)|$ divides 24. Also $G/G' \cong C_2$, and $G' = \langle x, y^{-1}xy, y^2 \rangle$. Hence by Schur's theorem, the order of y^2 divides 24, so t divides 12. (But furthermore, we can use Reidemeister-Schreier theory to obtain presentations (and hence the orders) of subgroups of

G: the index 6 subgroup $H = \langle y^2, (xy^{-1})^2 \rangle$ has order dividing 24, so $|G| = |G:H||H|$ divides 144, so t divides 6.)

7 MORE RECENT RESULTS

Some new discoveries have been made (and proved) very recently as a result of observations made about the data produced from the computations described at the end of Section 5.

Two major breakthroughs in the study of rotary and regular maps were made possible by noticing that there is no orientably-regular but chiral map of genus 2, 3, 4, 5, 6, 9, 13, 23, 24, 30, 36, 47, 48, 54, 60, 66, 84 or 95, and similarly that there is no regular orientable map of genus 20, 32, 38, 44, 62, 68, 74, 80 or 98 with simple underlying graph. A lot of these exceptional genera are of the form $p + 1$ where p is prime—a phenomenon that was not so easy to observe until the rotary maps of genus 2 to 100 were known—and this observation led to the following (proved in joint work with Jozef Siráň and Tom Tucker):

Theorem 4 [22]. *If M is an irreflexible (chiral) orientably-regular map of genus $p + 1$ where p is prime, then*

$$\begin{aligned} \textit{either} \quad & p \equiv 1 \textit{ mod } 3 \textit{ and } M \textit{ has type } \{6, 6\}, \\ \textit{or} \quad & p \equiv 1 \textit{ mod } 5 \textit{ and } M \textit{ has type } \{5, 10\}, \\ \textit{or} \quad & p \equiv 1 \textit{ mod } 8 \textit{ and } M \textit{ has type } \{8, 8\}. \end{aligned}$$

In particular, there are no such maps of genus $p + 1$ whenever p is a prime such that $p - 1$ is not divisible by 3, 5 or 8.

Theorem 5 [22]. *There is no regular map M with simple underlying graph on an orientable surface of genus $p + 1$ whenever p is a prime congruent to 1 mod 6, for $p > 13$.*

In fact, what was achieved in [22] is a complete classification of all regular and orientably-regular maps M for which $|\text{Aut}\,M|$ is coprime to the map's Euler characteristic χ (if χ is odd) or to $\chi/2$ (if χ is even), and that leads not only to the above two theorems, but also to a simpler proof of the following theorem of Breda, Nedela & Siráň:

Theorem 6 [2]. *There is no regular map M on a non-orientable surface of genus $p + 1$ whenever p is a prime congruent to 1 mod 12, for $p > 13$.*

Here is a sketch proof of the classification leading to these three results. First, let M be a rotary map on an orientable surface of genus g, let $G = \text{Aut}^{\text{o}}M$ be its group of orientation-preserving automorphisms, and suppose $|G|$ is coprime to $g - 1$. Then by the Euler-Poincaré formula, the type $\{k, m\}$ of M is restricted (by arithmetic) to one of five different families. Moreover, the group $G = \text{Aut}^{\text{o}}M$ is almost Sylow-cyclic, meaning that every Sylow subgroup of odd order in G is cyclic, and every Sylow 2-subgroup of G contains a cyclic subgroup of index 2. The Suzuki-Wong classification of non-solvable almost Sylow-cyclic groups can be used to deduce that $G = \text{Aut}^{\text{o}}M$ is solvable, except in the case of one of the five families. It is then possible to classify those cases where the vertex-stabilizer and face-stabilizer intersect trivially, and use Ito's theorem and Schur's transfer theory to deal with the more general case. What is remarkable is that the map M turns out to be reflexible whenever the coprime condition is satisfied.

Another outcome concerns reflexibility of Cayley maps. Briefly, a Cayley map for a group G is an embedding of a Cayley graph for G in a surface as a rotary map—or equivalently, a rotary map which admits the action of G as a group of automorphisms acting regularly (sharply-transitively) on vertices. From an inspection of the rotary maps of genus 2 to 100 in [11], it was noticed that for small genus, a rotary Cayley map for a cyclic group is reflexible if and only if it is anti-balanced (that is, if and only if the embedding of the Cayley map sees the neighbours of the identity element ordered in a way that is reversed by their inversion), and then this was proved in general in a piece of joint work with Jozef Siráň and Young Soo Kwon [17] just a few months before this paper was written.

REFERENCES

[1] W. Bosma, J. Cannon and C. Playoust, The Magma Algebra System I: The User Language, *J. Symbolic Computation* 24 (1997), 235–265.

[2] A. Breda, R. Nedela and J. Siráň, Classification of regular maps with negative prime Euler characteristic, *Trans. Amer. Math. Soc.* 357 (2005), 4175–4190.

[3] E. Bujalance, M. Conder and A. Costa, Pseudo-real Riemann surfaces and chiral regular maps, *preprint*.

[4] M.D.E. Conder, Generators for alternating and symmetric groups, *J. London Math. Soc. (2)* 22 (1980), 75–86.

[5] M.D.E. Conder, More on generators for alternating and symmetric groups, *Quarterly J. Mathematics (Oxford) Ser.* 2 32 (1981), 137–163.

[6] M.D.E. Conder, An infinite family of 5-arc-transitive cubic graphs, *Ars Combinatoria* 25A (1988), 95–108.

[7] M.D.E. Conder, A surprising isomorphism, *Journal of Algebra* 129 (1990), 494–501.

[8] M.D.E. Conder, Schreier coset graphs and their applications, *RIMS Kokyuroku* 794 (1992), 169–175.

[9] M.D.E. Conder, Group actions on graphs, maps and surfaces with maximum symmetry, *Groups St Andrews 2001 in Oxford*, London Math. Soc. Lecture Note Series, vol. 304, Cambridge University Press, 2003, pp. 63–91.

[10] M.D.E. Conder, On symmetries of Cayley graphs and the graphs underlying regular maps, *preprint*.

[11] M.D.E. Conder, Regular maps and hypermaps of Euler characteristic -1 to -200, *preprint*, with associated lists of computational data available at http://www.math.auckland.ac.nz/∼conder/hypermaps.html.

[12] M.D.E. Conder and P. Dobcsányi, Determination of all regular maps of small genus, *J. Combinatorial Theory Series B* 81 (2001), 224–242.

[13] M.D.E. Conder and P. Dobcsányi, Trivalent symmetric graphs up to 768 vertices, *J. Combinatorial Mathematics & Combinatorial Computing* 40 (2002), 41–63.

[14] M.D.E. Conder and P. Dobcsányi, Applications and adaptations of the low index subgroups procedure, *Mathematics of Computation* 74 (2005), 485–497.

[15] M.D.E. Conder, I. Hubard and T. Pisanski, Constructions for chiral polytopes, to appear in *J. London Math. Society*, accepted July 2007.

[16] M.D.E. Conder and R. Kulkarni, Infinite families of automorphism groups of Riemann surfaces, in: *Groups and Geometry* (London Math. Soc. Lecture Note Series, vol. 173), 1992, pp. 47–56.

[17] M.D.E. Conder, Y.S. Kwon and J. Širáň, Reflexibility of regular Cayley maps for abelian groups, *preprint*.

[18] M.D.E. Conder and P.J. Lorimer, Automorphism groups of symmetric graphs of valency 3, *Journal of Combinatorial Theory Series B* 47 (1989), 60–72.

[19] M.D.E. Conder, A. Malnič, D. Marušič and P. Potočnik, A census of semisymmetric cubic graphs on up to 768 vertices, *Journal of Algebraic Combinatorics* 23 (2006), 255–294.

[20] M.D.E. Conder and D. Marušič, A tetravalent half-arc-transitive graph with nonabelian vertex stabilizer, *J. Combinatorial Theory Series B* 88 (2003), 67–76.

[21] M.D.E. Conder and R. Nedela, A more detailed classification of symmetric cubic graphs, *preprint*.

[22] M.D.E. Conder, J. Siráň and T.W. Tucker, The genera, reflexibility and simplicity of regular maps, *preprint*.

[23] M.D.E. Conder and C.G.Walker, Vertex-transitive graphs with arbitrarily large vertex-stabilizers, *Journal of Algebraic Combinatorics* 8 (1998), 29–38.

[24] M.D.E. Conder and C.G.Walker, The infinitude of 7-arc-transitive graphs, *Journal of Algebra* 208 (1998), 619–629.

[25] H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Discrete Groups*, 4th ed., Springer Berlin (1980).

[26] D.Ž. Djoković and G.L. Miller, Regular groups of automorphisms of cubic graphs, *J. Combin. Theory Series B* 29 (1980), 195–230.

[27] B.J. Everitt, Alternating quotients of Fuchsian groups, *J. Algebra* 223 (2000), 457–476.

[28] D.F. Holt, B. Eick and E.A. OBrien, *Handbook of Computational Group Theory*, CRC Press, 2005.

[29] P. McMullen and E. Schulte, *Abstract Regular Polytopes*, Encyclopedia of Mathematics & its Applications, vol. 92, Cambridge (2002).

[30] D.J.S. Robinson, *A Course in the Theory of Groups*, 2nd ed., Springer (1996).

[31] C.C. Sims, *Computation with Finitely Presented Groups* (Cambridge University Press, 1994).

[32] W.T. Tutte, A family of cubical graphs, *Proc. Camb. Phil. Soc.* 43 (1947), 459–474.

[33] W.T. Tutte, On the symmetry of cubic graphs, *Canad. J. Math.* 11 (1959), 621–624.

[34] Richard Weiss, The non-existence of 8-transitive graphs, *Combinatorica* 1 (1981), 309–311.

[35] Richard Weiss, Presentations for (G,s)-transitive graphs of small valency, *Math. Proc. Cambridge Philos. Soc.* 101 (1987), 7–20.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Automorphism groups of Cayley digraphs

Yan-Quan Feng
Mathematics, Beijing Jiaotong University, Beijing, P.R. China

Zai-Ping Lu
Center for Combinatorics, LPMC, Nankai University, Tianjin, P.R. China

Ming-Yo Xu
Department of Mathematics, Peking University, Beijing, P.R. China

ABSTRACT: Let G be a group and $S \subset G$ with $1 \notin S$. A Cayley digraph $\mathrm{Cay}(G,S)$ on G with respect to S is the digraph with vertex set G such that, for $x, y \in G$, there is a directed edge from x to y whenever $yx^{-1} \in S$. If $S^{-1} = S$, then $\mathrm{Cay}(G,S)$ can be viewed as an (undirected) graph by identifying two directed edges (x,y) and (y,x) with one edge $\{x,y\}$.

Let $X = \mathrm{Cay}(G,S)$ be a Cayley digraph. Then every element $g \in G$ induces naturally an automorphism $R(g)$ of X by mapping each vertex x to xg. The Cayley digraph $\mathrm{Cay}(G,S)$ is said to be *normal* if $R(G) = \{R(g)|g \in G\}$ is a normal subgroup of the automorphism group of X. In this paper we shall give a brief survey of recent results on automorphism groups of Cayley digraphs concentrating on the normality of Cayley digraphs.

Keywords: Cayley digraph, normal Cayley digraph, arc-transitive graph, half-arc-transitive graph.
2000 Mathematics Subject Classification: 05C25, 20B25.

1 INTRODUCTION

Throughout this paper graphs or digraphs (directed graphs) are finite and simple unless specified otherwise. For a (di)graph X, we denote by $V(X)$, $E(X)$ and $\mathrm{Aut}(X)$ the vertex set, the edge set and the automorphism group of X, respectively. A (di)graph is said to be *vertex-transitive* or *edge-transitive* if $\mathrm{Aut}(X)$ acts transitively on $V(X)$ or $E(X)$, respectively. Note that for an (undirected) graph X, each edge $\{u, v\}$ of X gives two ordered pairs (u, v) and (v, u), called *arcs* of X. Thus we sometimes, if necessary, view a graph X as a digraph.

Let G be a group and S a subset of G such that $1 \notin S$. The *Cayley digraph* $\mathrm{Cay}(G,S)$ on G with respect to S is defined as the directed graph with vertex set G and edge set $\{(g,sg) \mid g \in G, s \in S\}$. For a Cayley digraph $X = \mathrm{Cay}(G,S)$, we always call $\mid S \mid$ the *valency* of X for convenience. If S is symmetric, that is, if $S^{-1} = \{s^{-1} \mid s \in S\}$ is equal to S, then $\mathrm{Cay}(G,S)$ can be viewed as an undirected graph by identifying two oppositely directed edges with one undirected edge. We sometimes call a Cayley digraph $\mathrm{Cay}(G,S)$ a *Cayley graph* if S is symmetric, and say $\mathrm{Cay}(G,S)$ a directed Cayley graph to emphasize $S^{-1} \neq S$.

Let $X = \mathrm{Cay}(G,S)$ be a Cayley digraph. Consider the action of G on $V(X)$ by right multiplication. Then every element $g \in G$ induces naturally an automorphism $R(g)$ of X by mapping each vertex x to xg. Set $R(G) = \{R(g) \mid g \in G\}$. Then $R(G)$ is a subgroup of $\mathrm{Aut}(X)$ and $R(G) \cong G$. Thus X is a vertex-transitive digraph. Clearly, $R(G)$ acts regularly on vertices, that is, $R(G)$ is transitive on vertices and only the identity element of $R(G)$ fixes any given vertex. Further, it is well-known that a digraph Y is isomorphic to a Cayley digraph on some group G if and only if its automorphism group contains a subgroup isomorphic to G, acting regularly on the vertices of Y (see [5, Lemma 16.3]). Noting that $R(G)$ is regular on $V(X)$, it implies $\mathrm{Aut}(X) = R(G)\mathrm{Aut}(X)_1$.

For the case where $R(G) \trianglelefteq \mathrm{Aut}(X)$, we have the following concept, which was fist proposed by Xu [52].

Definition 1.1. *A Cayley* digraph $X = \mathrm{Cay}(G,S)$ *is said to be* normal *if* $R(G)$ *is a normal subgroup of* $\mathrm{Aut}(X)$.

It was conjectured in [52] that 'most' Cayley digraphs are normal. In the literatures, studying normality or, equivalently, determining automorphism groups of Cayley digraphs itself has been becoming an very active topic in the algebraic graph theory, which also play an important role in the investigation of various symmetry properties of digraphs. We need more concepts to start our survey on the works about normality of Cayley digraphs and its application to the symmetries of digraphs.

Let X be a graph. An *s-arc* in X is an ordered $(s+1)$-tuple $(v_0, v_1, \dots, v_s)$ of vertices such that v_{i-1} is adjacent to v_i for $1 \leq i \leq s$, and $v_{i-1} \neq v_{i+1}$ for $1 \leq i < s$; in other words, it is a directed walk of length s which never includes the reverse of an arc just crossed. A 1-arc is also called an *arc* simply. The graph X is said to be *s-arc-transitive* if $\mathrm{Aut}(X)$ is transitive on the vertex set and on the set of all s-arcs in X; and X is said to be *s-transitive* if it is s-arc-transitive but not $(s+1)$-arc-transitive. We also call a 1-arc-transitive graph an *arc-transitive* or *symmetric* graph. A subgroup of the automorphism group of an s-arc-transitive graph X is said to be *s-regular* if it acts regularly on the set of s-arcs of X. In particular, X is said to be *s-regular* if the automorphism group $\mathrm{Aut}(X)$ itself is s-regular. Thus, if a graph X is s-regular then $\mathrm{Aut}(X)$ is transitive on s-arcs and the only automorphism fixing an s-arc is the identity automorphism of X. Finally, the graph X is said to be *half-arc transitive* if it is vertex-transitive and edge-transitive but not arc-transitive.

In this paper, we denote by $\mathbb{Z}_n$ or D_n, respectively, the cyclic group or the dihedral group of order n, and by $\mathbb{Z}_p^m$ the elementary abelian p-group $\underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{m \text{ times}}$, where p is a prime and m is a positive integer.

2 THE NORMALITY OF CAYLEY DIGRAPHS

Let $X = \mathrm{Cay}(G,S)$ be a Cayley digraph. Let α be an automorphism of G. Then α induces a permutation on $V(X)$ naturally. It is easily shown that α induces an automorphism of the digraph X if and only if it preserves S, that is $S^\alpha = \{s^\alpha \mid s \in S\} = S$. Furthermore, $\mathrm{Aut}(G,S) = \{\alpha \in \mathrm{Aut}(G) \mid S^\alpha = S\}$ is a subgroup of $\mathrm{Aut}(G)$, and can be viewed as a subgroup of the stabilizer of the vertex 1 in $\mathrm{Aut}(X)$. It is easy to show that $N_{\mathrm{Aut}(X)}(R(G)) = R(G) \rtimes \mathrm{Aut}(G,S)$ (see [52], for example). Then $R(G) \trianglelefteq \mathrm{Aut}(X)$ implies $\mathrm{Aut}(X)_1 = \mathrm{Aut}(G,S)$, and the converse also holds. Thus we get a basic criteria for normal Cayley digraph.

Proposition 2.1 [52, Proposition 1.5]. *Let* $X = \mathrm{Cay}(G,S)$ *be a Cayley digraph on a finite group* G *with respect to* S. *Let* $A = \mathrm{Aut}(X)$ *and let* A_1 *be the stabilizer of* 1 *in* A. *Then* X *is normal if and only if* $A_1 = \mathrm{Aut}(G,S)$.

By Proposition 2.1, if $X = \mathrm{Cay}(G,S)$ is normal then $\mathrm{Aut}(X) = R(G) \rtimes \mathrm{Aut}(G,S)$, which also can be obtained from Godsil [25]. This implies that the automorphism group of a normal Cayley digraph is known and normal Cayley digraphs are just those which have the smallest possible full automorphism groups.

Note that being a normal Cayley digraph is not invariant under digraph isomorphisms, and so strictly depends upon which group the digraph is a Cayley digraph on. For example, the three-dimensional hypercube Q_3 is a Cayley graph on either the group $\mathbb{Z}_2^3$ or the group $\mathbb{Z}_4 \times \mathbb{Z}_2$, and the Cayley graph on the first group is normal, but the Cayley graph on the second group is not.

Let S and T be two subsets of G such that $1 \notin S$ and $1 \notin T$. If there is an $\alpha \in \mathrm{Aut}(G)$ such that $S^{\alpha} = T$, then S and T are said to be *equivalent*, denoted by $S \equiv T$. It is easy to see that if S and T are equivalent, then $\mathrm{Cay}(G, S)$ is normal if and only if $\mathrm{Cay}(G, T)$ is normal. Thus, to study the normality of Cayley digraphs on a group G, it suffices to deal with all non-equivalent subsets of G. Here we mention two results as examples.

Proposition 2.2 [21]. *Let G be a nonabelian group of order $2p^2$ for an odd prime p and S a two-element generating subset of G. Then $X = \mathrm{Cay}(G, S)$ is nonnormal if and only if*

$$G = \langle a, b, c \mid a^p = b^p = c^2 = 1, [a, b] = [a, c] = 1, c^{-1}bc = b^{-1}\rangle$$

and $S \equiv \{ca, cba^{-1}\}$; further, $\mathrm{Aut}(X) \cong R(G) \cdot (\mathbb{Z}_2 \times \mathbb{Z}_2)$.

Proposition 2.3 [58]. *Let $X = \mathrm{Cay}(G, S)$ be a connected cubic Cayley graph of order $4p$ for a prime p. Then either $R(G) \trianglelefteq \mathrm{Aut}(X)$, or one of the following happens:*

(1) *$G = \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, $S \equiv \{a, a^{-1}, b\}$, $\mathrm{Aut}(X) \cong \mathbb{Z}_2^3 \rtimes S_3$, and $X \cong Q_3$, the three-dimensional hypercube of order 8;*
(2) *$G = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-a}\rangle$, $S \equiv \{b, a, a^{-1}\}$ or $\{b, ab, a^2b\}$, and $X \cong Q_3$;*
(3) *$G = \langle a, b \mid a^{2p} = b^2 = 1, b^{-1}ab = a^{-1}\rangle$ for $p \geq 3$, $S \equiv \{b, ab, a^pb\}$ and $\mathrm{Aut}(X) \cong \mathbb{Z}_2^p \rtimes D_{2p}$*

However, for a finite group G we do not know in general whether there are two subsets S and T of G not containing the identity such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ and that $\mathrm{Cay}(G, S)$ is normal but $\mathrm{Cay}(G, T)$ is nonnormal. For this reason, the non-equivalent subsets corresponding to nonnormal (normal) Cayley digraphs are usually given when a classification of nonnormal (normal) Cayley digraphs on a given group is done.

In most situations, it is difficult to determine the normality of Cayley digraphs. In fact the only groups, for which the complete information about the normality of Cayley (di)graphs is available, are the cyclic groups of prime order (see the below theorem) and the groups of order a product of two primes (see the next section). It is well-known that every transitive permutation group of prime degree p is either 2-transitive or solvable with a regular normal Sylow p-subgroup (for example, see [7 Corollary 3.5B]). This implies the following proposition, which was also obtained in [1].

Theorem 2.4. *A Cayley digraph on a group of prime order p is normal if the digraph is neither the empty graph nor the complete graph of order p.*

Noting that Xu [52] reviewed the results about the normality of Cayley digraphs obtained before 1997, in what follows we shall mainly review the results obtained after 1997.

3 CAYLEY DIGRAPHS OF ORDER *pq*

This section is to collect several results on the normality of Cayley digraphs of order a product of two primes. For the convenience of statement, we need some graph notations.

Let X and Y be two digraphs. Denote by X^c the complement of X in the complete digraph K_m, where $m = \mid V(X) \mid$. The *lexicographic product* $X[Y]$ is defined as the digraph with vertex set $V(X[Y]) = V(X) \times V(Y)$ such that for any two vertices $u = (x_1, y_1)$ and $v = (x_2, y_2)$ in $V(X[Y])$, (u, v) is an edge in $X[Y]$ whenever $(x_1, x_2) \in E(X)$ or $x_1 = x_2$ and $(y_1, y_2) \in E(Y)$. Let $V(Y) = \{y_1, y_2, \ldots, y_n\}$. Then there is a natural embedding nX in $X[Y]$, where for $1 \leq i \leq n$, the ith copy of X is the subgraph induced on the vertex subset $\{(x, y_i) \mid x \in V(X)\}$ in $X[Y]$. The *deleted lexicographic product* $X[Y] - nX$ is the digraph obtained by deleting all the edges of (this natural embedding of) nX from $X[Y]$.

For the normality of Cayley digraphs on a group of order a prime square, Dobson and Witte [8] proved the following result which is a complete answer for Problem 3 posed by Xu in [52].

Theorem 3.1 [8, Corollary 3]. *Let p be a prime. Then a Cayley digraph $X = \mathrm{Cay}(G,S)$ on a group G of order p^2 is nonnormal if and only if X is isomorphic to one of the following digraphs:*

(1) *$X = K_{p^2}$, where $p \geq 3$ or $p = 2$ and $G = \mathbb{Z}_4$;*
(2) *$X = X_1[X_2]$, where X_1 and X_2 are Cayley digraphs on the cyclic group of order p, $p \geq 3$;*
(3) *X is a Cayley digraph on $\mathbb{Z}_p^2$ but not $\mathbb{Z}_{p^2}$, $p \geq 5$, with $S = \{(i,0),(0,j) \mid i,j \in \mathbb{Z}_p\}$ or the complement of this graph;*
(4) *X is a Cayley digraph on $\mathbb{Z}_p^2$ but not $\mathbb{Z}_{p^2}$, $p \geq 5$, with S satisfying the following properties, where $H = \{(0,i) \mid i \in \mathbb{Z}_p\}$,*
   (A) *$H \cap S = \emptyset$ or $H \cap S = H - \{(0,0)\}$,*
   (B) *for every coset $(a,0) + H \neq H$ of H, $((a,0) + H) \cap S = (a,b) + H$, $\emptyset$, $\{(a,0)\}$, or $((a,0) + H) - \{(a,0)\}$.*

The normality of Cayley digraphs on a group of order $2p$ was determined by Du, Wang and Xu [10]. For the convenience of statement, we need some notations. In Table 1. "Y" denotes any transitive digraph of order p; the graph $B(H(11))$ is the incidence graph of the doubly transitive Hadamard 2-$(11,5,2)$-design $H(11)$; and $PG(n-1,q)$ denotes the point-hyperplane incidence graph of the $(d-1)$-dimensional projective geometry $PG(n-1,q)$.

Proposition 3.2 [10, Theorem 1.6]. *All Cayley digraphs on groups of order twice a prime p are normal, except for the digraphs listed in Table* 1.

We now consider the normality of Cayley graphs of order pq. By Proposition 3.2, one may let $p > q \geq 3$. All vertex-primitive or edge-transitive Cayley graphs of order pq can be extracted from [2, 45, 46, 50, 51] and all vertex-primitive Cayley graphs of order pq are nonnormal (see [52, Theorem 2.12]), which can be read out from [46]. Furthermore, Lu and Xu [38] investigated the normality of imprimitive Cayley graphs of order pq, which answered the first part of Problem 2 posed in [52].

Table 1. Nonnormal Cayley digraphs X of groups G of order $2p$.

Row	Digraph X	Aut(X)	Group G	p	Remark
1	K_4	S_4	Z_4	2	
2	$4K_1$	S_4	Z_4	2	
3	$2pK_1$	S_{2p}	Z_{2p} and D_{2p}	$p > 2$	
4	pK_2	$Z_2 \wr S_p$	Z_{2p} and D_{2p}	$p > 2$	
5	$2Y,\ Y \neq pK_1$	$\mathrm{Aut}(Y) \wr Z_2$	Z_{2p} and D_{2p}	$p > 2$	For D_{2p}, $\mathrm{Aut}(Y) > Z_p$
6	$Y[2K_1],\ Y \neq pK_1$	$Z_2 \wr \mathrm{Aut}(Y)$	Z_{2p} and D_{2p}	$p > 2$	For D_{2p}, Y undirected
7	$Y[K_2],\ Y \neq pK_1$ and K_p	$Z_2 \wr \mathrm{Aut}(Y)$	Z_{2p} and D_{2p}	$p > 2$	For D_{2p}, Y undirected
8	K_{2p}	S_{2p}	Z_{2p} and D_{2p}	$p > 2$	
9	$K_2[Y],\ Y \neq K_p$	$\mathrm{Aut}(Y) \wr Z_2$	Z_{2p} and D_{2p}	$p > 2$	For D_{2p}, $\mathrm{Aut}(Y) > Z_p$
10	$K_{p,p} - pK_2$	$S_p \times Z_2$	Z_{2p} and D_{2p}	$p > 2$	
11	$(K_{p,p} - pK_2)^c$	$S_p \times Z_2$	Z_{2p} and D_{2p}	$p > 2$	
12	$B(H(11))$	$PGL(2,11)$	D_{2p}	11	
13	$K_{11,11} - B(H(11))$	$PGL(2,11)$	D_{2p}	11	
14	$(B(H(11)))^c$	$PGL(2,11)$	D_{2p}	11	
15	$(K_{11,11} - B(H(11)))^c$	$PGL(2,11)$	D_{2p}	11	
16	$B(PG(n-1,q))$	$P\Gamma L(n,q) \rtimes \mathbb{Z}_2$	D_{2p}	$\frac{q^n-1}{q-1}$	$n \geq 3$
17	$K_{p,p} - B(PG(n-1,q))$	$P\Gamma L(n,q) \rtimes \mathbb{Z}_2$	D_{2p}	$\frac{q^n-1}{q-1}$	$n \geq 3$
18	$(B(PG(n-1,q)))^c$	$P\Gamma L(n,q) \rtimes \mathbb{Z}_2$	D_{2p}	$\frac{q^n-1}{q-1}$	$n \geq 3$
19	$(K_{p,p} - B(PG(n-1,q)))^c$	$P\Gamma L(n,q) \rtimes \mathbb{Z}_2$	D_{2p}	$\frac{q^n-1}{q-1}$	$n \geq 3$

Let G be a finite group of order pq, where p, q are distinct primes. By elementary group theory, we know that $G \cong \mathbb{Z}_{pq}$ or $\mathbb{F}_{pq}$, where $\mathbb{F}_{pq}$ is the Frobenius group of order pq, that is,

$$\mathbb{F}_{pq} = \langle a, b \mid a^p = b^q = 1, b^a = b^r \rangle$$

for $r \not\equiv 1 (\bmod\ p)$, $r^q \equiv 1 (\bmod\ p)$ and $q \mid p - 1$.

By analyzing actions of the automorphism groups of Cayley graphs of order pq, Lu and Xu [38] constructs all possible imprimitive nonnormal Cayley graphs of order pq. The following result is a brief version of the main result [38, Theorem 3.1].

Proposition 3.3. *Assume that p and q are distinct primes with $p > q \geq 3$. Let X be a nonnormal Cayley graph on a group G with $\mid G \mid = pq$. Assume further that $A = \mathrm{Aut}(X)$ acts imprimitively on $V(X)$. Then one of the following happens.*

(1) *$X \cong Y_m[Y_n]$ or $(Y_m[Y_n])^c$, $G = \mathbb{Z}_{pq}$ or $\mathbb{F}_{pq}$, and $A = \mathrm{Aut}(Y_n) \wr \mathrm{Aut}(Y_m)$, where $\{m, n\} = \{p, q\}$, Y_p and Y_q are Cayley graphs of $\mathbb{Z}_p$ and $\mathbb{Z}_q$, respectively, such that one of them is connected and one of them is not complete.*
(2) *$A \geq \mathbb{Z}_q \times S_p$ and $G = \mathbb{Z}_{pq}$ or $\mathbb{F}_{pq}$.*
(3) *$q > 3$, $A = H \times S_q$, $p \mid\mid H \mid$ and $G = \mathbb{Z}_{pq}$ or $\mathbb{F}_{pq}$; further, $q \mid\mid H \mid$ if $G = \mathbb{F}_{pq}$.*
(4) *$(\mathrm{Aut}(X))' \cong \mathbb{Z}_{pq}$, $q^2 \mid\mid \mathrm{Aut}(X) \mid$ and $G = \mathbb{F}_{pq}$.*
(5) *$A = \mathrm{PSL}(2, 11)$ and $G = \mathbb{F}_{5 \cdot 11}$.*
(6) *$A = \mathrm{PSL}(3, 2)$ and $G = \mathbb{F}_{3 \cdot 7}$.*

To end the section, we would like to mention that all disconnected normal Cayley digraphs have been determined by Wang, Wang and Xu [48] (also see [52, Proposition 2.4 and 2.5])). For this reason, it suffices to consider the connected ones when one investigates the normality of Cayley digraphs.

4 MINIMAL CAYLEY DIGRAPHS

In this section we discuss mainly the normality of Cayley digraphs on abelian groups. Baik et al. [4] determined all nonnormal Cayley graphs with valences less than 5 which was reviewed by Xu [52, Theorem 2.12]. The following proposition gives all possible abelian groups on which there exist nonnormal Cayley graphs of valency 5, and for the corresponding subsets and the graphs, see Baik et al. [3, theorem 1.1] for details.

Proposition 4.1. *Let $X = \mathrm{Cay}(G, S)$ be a connected Cayley graph of valency 5 on an abelian group G with respect to S. If X is nonnormal then G is isomorphic to one of the groups: $\mathbb{Z}_{2m}$ $(m \geq 3)$, $\mathbb{Z}_{2m} \times \mathbb{Z}_2$ $(m \geq 2)$, $\mathbb{Z}_m \times \mathbb{Z}_4$ $(m \geq 3)$, $\mathbb{Z}_m \times \mathbb{Z}_6$ $(m \geq 3)$, $\mathbb{Z}_m \times \mathbb{Z}_2^2$ $(m \geq 2)$, $\mathbb{Z}_m \times \mathbb{Z}_4 \times \mathbb{Z}_2$ $(m \geq 3)$, $\mathbb{Z}_4 \times \mathbb{Z}_2^3$ or $\mathbb{Z}_2^4$.*

A generating set S of a group G is called *minimal* if S generates G but $S \backslash \{s\}$ cannot generate G for any $s \in S$. A Cayley digraph $\mathrm{Cay}(G, S)$ is *minimal* if S is a minimal generating set of G. Xu [52, Problem 6] asked whether $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, S \cup S^{-1})$ are normal for any minimal generating set S of G. Feng and Gao [17] prove the following proposition.

Proposition 4.2 [17, Theorem]. *Let G be a finite abelian group such that the Sylow 2-subgroup of G is cyclic. Let S be a minimal generating set of G. Then both $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, S \cup S^{-1})$ are normal.*

As for a special case of Proposition 4.2, if G is cyclic then $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, S \cup S^{-1})$ are normal, which was also proved by Huang and Meng [28, 29, 30]. Furthermore, Meng and Ying [42] determined all finite abelian groups whose Cayley digraph with respect to any given minimal generating subset is normal.

Theorem 4.3 [42, Theorem 3.4]. *Let G be a finite abelian group.*

(1) *If G is a 2-group then every minimal Cayley digraph on G is normal if and only if G has no direct factor $\mathbb{Z}_2 \times \mathbb{Z}_{2^m}$ $(m \geq 2)$.*
(2) *If G is not a 2-group then every minimal Cayley digraph on G is normal if and only if G has no direct factor $\mathbb{Z}_2 \times \mathbb{Z}_{2^m}$ $(m \geq 1)$.*

The following proposition gives all possible abelian groups on which there are nonnormal Cayley digraphs with valency 2 or 3, and for the corresponding subsets and the digraphs, see Xu, Zhang and Zhou [55, Theorem 1.1] for details.

Proposition 4.4. *Let G be a finite abelian group and let $X = \mathrm{Cay}(G,S)$ be a connected nonnormal digraph. If X has valency 2 then $G \cong \mathbb{Z}_{2n}$ $(n > 2)$ or $\mathbb{Z}_n \times \mathbb{Z}_2$ $(n > 2)$; if X has valency 3 then $G \cong \mathbb{Z}_{2n}$ $(n \geq 2)$, $\mathbb{Z}_n \times \mathbb{Z}_2$ $(n > 2)$, $\mathbb{Z}_{2n} \times \mathbb{Z}_m$ $(n > 2, m > 1)$ or $\mathbb{Z}_n \times \mathbb{Z}_2 \times \mathbb{Z}_m$ $(n > 2, m > 1)$.*

A digraph is said to be *strongly connected* if for any two vertices u and v there is a directed path from u to v in the digraph. Cayley digraphs on infinite cyclic groups were considered by Meng and Huang [43].

Proposition 4.5 [43, Theorem 1]. *Let $\mathbb{Z}$ be the infinite cyclic group and S a minimal generating subset of $\mathbb{Z}$ such that the Cayely digraph $\mathrm{Cay}(\mathbb{Z},S)$ is strongly connected. Then $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z},S)) = R(\mathbb{Z})$.*

At the end of this section we mention the normality of Cayley graph on the symmetric group S_n with respect to a minimal generating subset of involutions, which was first considered in Godsil and Royle [26].

Theorem 4.6 [15, Theorem 2.1]. *For any minimal generating set S of transpositions of S_n, the Cayley graph $\mathrm{Cay}(S_n,S)$ is normal.*

Many interconnection networks were constructed from those Cayley graphs $\mathrm{Cay}(S_n,S)$. Let $S_1 = \{(ii+1) \mid 1 \leq i \leq n-1\}$, $S_2 = \{(1\ i) \mid 2 \leq i \leq n\}$ and $S_3 = \{(ii+1) \mid 1 \leq i \leq n-1\} \cup (1\ n)$. The Cayley graphs $\mathrm{Cay}(S_n,S_1)$, $\mathrm{Cay}(S_n,S_2)$ and $\mathrm{Cay}(S_n,S_3)$ are called the *bubble-sort network BS_n*, the *star network ST_n*, and the *modified bubble-sort network MB_n* respectively (see [32]). Theorem 4.6 shows that the underlying graphs of those interconnection networks are normal Cayley graphs on S_n, so that their automorphism groups are known.

5 CAYLEY DIGRAPHS OF NONABELIAN SIMPLE GROUPS

This section is to review mainly results about the normality of Cayley digraphs on non-abelian simple groups. We first introduce two concepts.

For a group M, the *socle* of M is the product of all minimal normal subgroups of M, and M is called *almost simple* if its socle is a non-abelian simple group.

Let X be a graph and $M \leq \mathrm{Aut}(X)$. For an intransitive normal subgroup K of M we define the *quotient graph X_K* of X with respect to K as follows: the vertex set $V(X_K)$ is the set of K-orbits on $V(X)$, and two K-orbits B_1 and B_2 are adjacent in X_K if and only if there are $u_1 \in B_1$ and $u_2 \in B_2$ such that u_1 and u_2 are adjacent in X.

Table 2. The possibilities for G and T.

	G	T	m	$V(X_K)$
1	A_6	G	6	m^2
2	M_{12}	G or A_m	12	m^2
3	$Sp_4(q)$	G or A_m or	$\frac{q^2(q^2-1)}{2}$	m^2
	$q = 2^a > 2$	$Sp_{4r}(q_0)(q = q_0^r)$		
4		$Sp_{4r}(q_0)(q = q_0^r)$	$\frac{q^2(q^2-1)}{2}$	$2m^2$
5	$P\Omega_8^+(q)$	G or A_m or	$\frac{q^3(q^4-1)}{(2,q-1)}$	m^2
		$Sp_8(q_0)(\text{if } q = 2)$		

The following result, due to Fang, Praeger and Wang [12], gives a general description of the possibilities for the automorphism groups of connected Cayley graphs on a finite non-abelian simple group.

Theorem 5.1 [12, Theorem 1.1]. *Let G be a finite non-abelian simple group and $X = \mathrm{Cay}(G, S)$ a connected Cayley graph on G. Let M be a subgroup of $\mathrm{Aut}(X)$ containing $R(G) \rtimes \mathrm{Aut}(G, S)$. Then either $M = R(G) \rtimes \mathrm{Aut}(G, S)$ or one of the following holds.*

(1) *M is almost simple and $R(G) \leq \mathrm{soc}(M)$;*
(2) *$R(G) \rtimes \mathrm{Inn}(G) \leq M = (R(G) \rtimes \mathrm{Aut}(G, S)).2$ and S is a self-inverse union of G-conjugacy classes;*
(3) *there is intransitive normal subgroup K of M such that one of the following holds:*
  (a) *M/K is almost simple and $G \cong R(G)K/K \leq \mathrm{soc}(M/K)$;*
  (b) *$M/K = \mathrm{AGL}_3(2)$, $G = \mathrm{PSL}(2, 7)$ and $X_K \cong K_8$;*
  (c) *$\mathrm{soc}(M/K) \cong T \times T$, and $R(G)K/K \cong G$ is a diagonal subgroup of $\mathrm{soc}(M/K)$, where T and G are given in Table 2.*

For the case where $\mathrm{Cay}(G, S)$ is an edge-transitive cubic Cayley graph on a simple group, we may get more precise results.

A Cayley graph $X = \mathrm{Cay}(G, S)$ is called a *normal edge transitive* Cayley graph if the normalizer of $R(G)$ in $\mathrm{Aut}(X)$ is transitive on the edges of X.

Let X be a connected edge transitive cubic Cayley graph. Then X must be arc transitive. It follows from a result of Tutte that the order of the stabilizer $\mathrm{Aut}(X)_1$ is bounded by 48 (see [5], for example). Then this make us do something further. In fact, Praeger [44] proved that all connected normal edge-transitive cubic Cayley graphs on non-abelian simple groups are normal Cayley graphs. One may ask which connected arc transitive cubic Cayley graphs on non-abelian simple groups are not normal edge transitive, or equivalently among such Cayley graphs, which one is nonnormal? This was answered partially by Li [33], where it was showed that the only possibilities for connected nonnormal arc-transitive cubic Cayley graphs on nonabelian simple groups must arise from one of the groups A_5, $L_2(11)$, M_{11}, A_{11}, M_{23}, A_{23} and A_{47}. Further, on the basis of Li's work, X.G. Fang, J. Wang, S.J. Xu and M.Y. Xu [56, 57] recently proved the following result.

Theorem 5.2. *Let G be a finite nonabelian simple group and let $X = \mathrm{Cay}(G, S)$ be a connected arc-transitive cubic Cayley graph on G. Then X is normal or $G = A_{47}$. Furthermore, There are exactly two nonnormal cubic Cayley graphs on A_{47} which are 5-regular with automorphism groups isomorphic to A_{48}.*

Theorem 5.2 completes the job on the normality of arc-transitive cubic Cayley graphs on non-abelian simple groups. For the case where $X = \mathrm{Cay}(G, S)$ is not arc transitive or of valency more than 3, we have no such a lucky result by now. However, a lot of progresses have been made.

Table 3. Exceptional candidates.

s	G
$\frac{1}{2}$, 1	M_{12}, M_{22}, J_2, Suz A_{2^m-1} for $m \geq 3$ $\mathrm{PSL}_n(2^e)$, $\mathrm{PSU}_n(2^e)$ for $n \geq 4$; $\mathrm{PSp}_n(2^e)$ for $n \geq 6$ $E_6(2^e), E_7(2^e), {}^2E_6(2^e), {}^2G_2(2^e)$
2	$\mathrm{PSL}_2(11), M_{11}, M_{23}, A_{11}$
3	$\mathrm{PSL}_2(11)$, or A_{n-1} where $n = 2^r3^2$ for $r \in \{2, 3, 4\}$
4, 7	$\mathrm{PSL}_4(2)$, $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_3(9)$, $\mathrm{PSL}_3(27)$, $\mathrm{PSL}_4(3)$, $\mathrm{PSL}_5(3)$, $\mathrm{PSL}_6(3)$, $\mathrm{PSU}_4(3)$ A_{n-1} where $n = 2^r3^{s-1}$ for $r \in \{2, 3, 4\}$

Fang *et al.* [13] proved that the vast majority of connected cubic Cayley graphs on non-abelian simple groups are normal.

Theorem 5.3 [13, Theorem 1.1]. *Let G be one of the groups satisfying:*

(1) *G is a sporadic simple group and $G \neq M_{11}, M_{22}, M_{23}, J_2, Suz$; or*
(2) *$G = A_n$, where $n \notin \{5, 11, 23, 47\} \cup \{2^m - 1 \mid m \geq 3\}$; or*
(3) *G is a simple group of Lie type of odd characteristic with a possible exception $G \neq L_2(11)$; or*
(4) *$G = L_2(2^e)$, $L_3(2^e)$, $U_3(2^e)$, $PSp_4(2^e)$, $E_8(2^e)$, $F_4(2^e)$, ${}^2F_4(2e)'$, $G_2(2^e)$, or $Sz(2^e)$.*

Then every connected cubic Cayley graph $\mathrm{Cay}(G, S)$ *on G is normal, and* $\mathrm{Aut}(G, S) \leq S_3$.

For tetravalent Cayley graphs on nonabelian simple groups, we list here two results. With assumption of edge-transitivity, Fang, Li and Xu [14] proved the following result.

Theorem 5.4 [14, Theorem 1.1]. *Let G be a nonabelian simple group, and let $X = \mathrm{Cay}(G, S)$ be a connected edge-transitive graph of valency* 4. *Then either*

(1) $\mathrm{Aut}X = G \rtimes \mathrm{Aut}(G, S)$, $\mathrm{Aut}(G, S) = \mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2^2$, D_8, A_4, *or* S_4, *and further*
   (i) *X is half-arc-transitive if and only if* $\mathrm{Aut}(G, S) = \mathbb{Z}_2$;
   (ii) *X is* 1*-transitive if and only if* $\mathrm{Aut}(G, S) = \mathbb{Z}_4$, $\mathbb{Z}_2^2$, *or* D_8;
   (iii) *X is* 2*-transitive if and only if* $\mathrm{Aut}(G, S) = A_4$ *or* S_4; *or*
(2) $\mathrm{Aut}X \neq G \rtimes \mathrm{Aut}(G, S)$, *$X$ is s-transitive, and G is one of the groups given in Table* 3.

And without the assumption of edge-transitivity, Qu [47] proved the following result.

Proposition 5.5 [47]. *Let G be a nonabelian simple group, and let $X = \mathrm{Cay}(G, S)$ be a connected graph of valency* 4 *which is not edge-transitive. If S contains no* 2*-elements and X is nonnormal then G is one of the following groups: A_{2^m-1} or A_{2^m} $(m \geq 3)$, M_{12}, M_{22}, J_2,* Suz, $\mathrm{PSL}_2(7)$, $\mathrm{PSp}_4(3)$, $\mathrm{PSL}_n(2^e)$ *or* $\mathrm{PSU}_n(2^e)$ $(n \geq 3)$, $\mathrm{PSp}_n(2^e)$ $(n \geq 4)$, $P\Omega_n^+(2^e)$ $(n \geq 6)$, $P\Omega_n^-(2^e)$ $(n \geq 4)$, ${}^3D_4(2^e)$, $E_6(2^e)$, $E_7(2^e)$, ${}^2E_6(2^e)$.

Recently, Zhou and Feng [59] gives two sufficient conditions for nonnormal Cayley graphs of valency 5.

Lemma 5.6 [59, Theorem 3.1]. *Let G be a finite group and $S = \{s_1, s_2, s_3, s_4, s_5\}$ a* 5*-element subset of G with s_5 an involution and $S = S^{-1}$. Suppose that S contains at least two involutions and that there exists an involution h in $G \backslash S$ such that*

$$s_2 = hs_1,\ s_3 = s_1h,\ s_4 = s_2h,\ s_5 = s_5^h.$$

Then, the Cayley graph $\mathrm{Cay}(G, S)$ *on G is nonnormal.*

Lemma 5.7 [59, Theorem 3.2]. *Let G be a finite group and $S = \{s_1, s_2, s_3, s_4, s_5\}$ a 5-element subset of G with $1 \notin S$. Let $G = \langle S \rangle$ and $S = S^{-1}$. Suppose that s_1 is an involution with $\{1, s_1, s_2, s_3\}$ a subgroup of G and that $\{s_1s_4, s_1s_5\} = \{s_4s_1, s_5s_1\}$. Let $H = \langle s_1, s_4, s_5 \rangle$ with $s_2, s_3 \notin H$. Then, the Cayley graph* $\mathrm{Cay}(G, S)$ *is nonnormal when* $| G : H | \geq 4$.

With the help of above two lemmas, Zhou and Feng determined all nonnormal Cayley graphs of A_5 with valency 5. Then, combining a result of S.J. Xu and M.Y. Xu, we have the following theorem.

Theorem 5.8 [54, 59]. *All nonnormal Cayley graphs of A_5 with valency* 4 *or* 5 *are known.*

Zhou and Feng also constructed in [59] three infinite families of nonnormal Cayley graphs of valency 5 on $\mathrm{PSL}(2, p)$ and A_p, where p is a prime. Up to our best knowledge, besides these three infinite families, there are 6 known, up to equivalence, nonnormal Cayley graphs on nonabelian simple groups with valency no more than 5: two are cubic Cayley graphs on A_{47}, and the other four are tetravalent Cayley graphs on A_5. This suggests the following problem.

Problem 5.9. *Are there infinitely many connected nonnormal Cayley graphs of valency* 3 *or* 4 *on non-abelian simple groups.*

So far, in this section, we deal only with Cayley graphs. In the following up to the end of this section we consider the directed case. Recall that we say $\mathrm{Cay}(G, S)$ a directed Cayley graph of valency k if $S^{-1} \neq S$ and $| S | = k$. The following result given by Li [33] (see also [34]) shows that all connected directed Cayley graphs of valency 2 on $\mathrm{PSL}_2(q)$ are normal.

Proposition 5.10. *Let X be a connected directed Cayley graph of valency* 2 *on* $G = \mathrm{PSL}_2(q)$. *Then* $R(G) \trianglelefteq \mathrm{Aut}(X)$.

As a more general case, for nonabelian simple groups, Fang, Lu, Wang and Xu [11] proved that, with a list of exceptions, the connected directed Cayley graph of valency 2 are normal.

Theorem 5.11. *Let* $X = \mathrm{Cay}(G, S)$ *be a connected directed Cayley graph of valency* 2. *Assume that G is a nonabelian simple group except for*

A_5, A_6, A_{2^s-1} and A_{2^s} for $s \geq 3$; and
M_{11}, M_{12}, J_2, Suz; and
$\mathrm{PSL}_2(7)$, $\mathrm{PSU}_4(3)$*; and*
Simple groups of Lie type over fields of characteristic 2.

Then X is normal, and $\mathrm{Aut}(X) = R(G)$ *or* $R(G) \rtimes \mathbb{Z}_2$.

To end this section we consider edge-transitive cubic directed Cayley graphs.

Let $X = \mathrm{Cay}(G, S)$ be a Cayley digraph. We define an undirected graph $X^{(2)} := \mathrm{BC}(G, S)$, called a *bi-Cayley graph* of G, which has vertex set $V(X) \times \{0, 1\}$ such that $\{(x, 0), (y, 1)\} \in E(X^{(2)})$ if and only if $yx^{-1} \in S$. It is easily shown that $X^{(2)}$ is connected if and only if G is generated by SS^{-1}. For each $\sigma \in \mathrm{Aut}(X)$, define a bijection

$$(x, 0) \mapsto (x^\sigma, 0), \quad (x, 1) \mapsto (x^\sigma, 1), \quad \forall x \in V(X).$$

on $V(X^{(2)})$, which is in fact an automorphism of $X^{(2)}$. Further, we may view $\mathrm{Aut}(X)$ as a subgroup of $\mathrm{Aut}(X^{(2)})$ by this way. Then the edge-transitivity of X (as a directed graph) implies the edge-transitivity of $X^{(2)}$. See [36, 37] for more basic facts and applications of bi-Cayley graphs.

Now let $X = \mathrm{Cay}(G, S)$ be an edge-transitive directed Cayley graph with $G = \langle SS^{-1}\rangle$. Then $X^{(2)}$ is connected and $\mathrm{Aut}(X)$ acts transitively on its edge set. It follows from [27] that $\mid \mathrm{Aut}(X)_1 \mid$ is bounded by $3 \cdot 2^7$. Thus we have the following result, by routinely checking simple groups one by one, which is a revised version of [11, Theorem 1.2, 1.3].

Theorem 5.12 [11]. *Let G be a nonabelian simple group and let $X = \mathrm{Cay}(G, S)$ be an edge-transitive cubic directed Cayley graph with $G = \langle SS^{-1}\rangle$. If $R(G)$ is not normal in* $\mathrm{Aut}(X)$*, then $\mid G \mid \leq (3 \cdot 2^7)!$ and G is one of the following groups:*

A_n, $n = 5, 6, 7, 8, 9, 11, 15, 23, 31, 47, 63, 95, 127, 191, 383$*; and*
M_{11}, M_{12}, M_{22}, M_{23}, J_1, J_2*; and*
$\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSU}_3(3)$, $\mathrm{PSU}_4(3)$, $\mathrm{PSp}_4(3)$*; and*
$\mathrm{PSL}_2(2^3)$, $\mathrm{PSL}_2(2^4)$, $\mathrm{PSL}_2(2^5)$, $\mathrm{PSL}_2(2^6)$*; and*
$\mathrm{PSL}_3(2^2)$, $\mathrm{PSL}_3(2^3)$, $\mathrm{PSL}_3(2^4)$, $\mathrm{PSL}_4(4)$*; and*
$\mathrm{PSL}_5(2)$, $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_6(2)$, $\mathrm{PSL}_7(2)$*; and*
$\mathrm{PSU}_3(4)$, $\mathrm{PSU}_4(4)$, $\mathrm{PSU}_5(2)$, $\mathrm{PSp}_4(4)$, $\mathrm{Sp}_6(2)$, $\mathrm{P}\Omega_8^-(2)$ *and* ${}^2B_2(2^3)$.

6 CAYLEY DIGRAPHS OF SMALL VALENCIES ON p-GROUPS AND DIHEDRAL GROUPS

In this section we discuss the normality of Cayley digraphs with small valencies on p-groups and dihedral groups.

A finite p-group P is called a *regular p-group* if for any two elements x and y in P, there exist $c_1, c_2, \ldots, c_r$ in the derived group $\langle x, y\rangle'$ such that $(xy)^p = x^p y^p c_1^p c_2^p \cdots c_r^p$. First, Feng, Wang and Xu [22] considered the normality of directed Cayley graphs of valency 2 on regular p-groups.

Theorem 6.1. *Let $X = \mathrm{Cay}(G, S)$ be a 2-valent connected directed Cayley graph on a regular p-group G. Then one of the following happens:*

(1) $\mathrm{Aut}(X) = R(G) \rtimes \mathrm{Aut}(G, S)$*;*
(2) $X \cong C_{2^n}[2K_1]$ *for some $n > 1$,* $\mathrm{Aut}(X) \cong \mathbb{Z}_2 \wr \mathbb{Z}_{2^n}$*, and either $G = \mathbb{Z}_{2^{n+1}} = \langle a\rangle$ and $S \equiv \{a, a^{2^n+1}\}$, or $G = \mathbb{Z}_{2^n} \times \mathbb{Z}_2 = \langle a\rangle \times \langle b\rangle$ and $S \equiv \{a, ab\}$.*

Furthermore, the normality of Cayley graphs of valency 4 on a regular p-group was determined by Feng and Xu [23].

Theorem 6.2. *Let G be a regular p-group with $p \neq 2, 5$ and $X = \mathrm{Cay}(G, S)$ a connected tetravalent Cayley graph on G. Then we have* $\mathrm{Aut}(\mathrm{Cay}(G, S)) = R(G) \rtimes \mathrm{Aut}(G, S)$.

Not that a regular 2-group is abelian (see [31, III. Theorem 10.3]) and the nonnormal connected Cayley graph of valency 4 on abelian groups are classified in [4]. Clearly, $\mathbb{Z}_5$ is a regular 5-group and the tetravalent Cayley graph on $\mathbb{Z}_5$ is the complete graph K_5, which is nonnormal on $\mathbb{Z}_5$. In fact, by using regular coverings of K_5 (for a method see [39]), one may construct infinitely many tetravalent Cayley graphs on 5-groups that are nonnormal. By Huppert [31, III. Theorem 10.2], a p-group of order p^n with $n \leq p$ is regular. The following corollary is straightforward from Theorem 6.2.

Corollary 6.3. *Let G be a p-group of order p^n with $n \leq p$. Then all connected tetravalent Cayley graph on G are normal except for $p = 5$.*

Together with the normality of Cayley graphs of valency 4 on abelian groups obtained in [4], one has the following by Feng et al. [18, 24].

Theorem 6.4. *Let G be a p-group with p an odd prime and let $X = \mathrm{Cay}(G, S)$ be a tetravalent connected Cayley graph. Then*

(1) *X is normal if G has nilpotent class* 2*;*
(2) *X is normal if G has order* p^3.

A proof of Theorem 6.4 (2) was also given in [53] with the help of the finite simple group classification and the Hall-Higman's theorem, which implies a classification of tetravalent half-arc-transitive graphs of order p^3 for odd prime p. However, the proof of Theorem 6.4 provided in [18, 24] are independent from the finite simple group classification and the Hall-Higman's theorem.

The following example shows that Theorem 6.4 is not true if G has nilpotent 3 or G has order p^4.

Example 6.5 [18]. Let $G = \langle a, b, c \mid a^9 = b^3 = c^3 = 1, [a, b] = a^3, [a, c] = b, [b, c] = 1\rangle$ and $S = \{a, ac, a^{-1}, (ac)^{-1}\}$. Then G has nilpotent class 3 and $X = \mathrm{Cay}(G, S)$ is nonnormal. Moreover if we set $A = \mathrm{Aut}(X)$ and $A_1^* = \{\alpha \in A_1 \mid s^\alpha = s, \ \ \forall s \in S\}$, then $A_1^* \cong \mathrm{Aut}(G, S) \cong \mathbb{Z}_2$ and $A_1/A_1^* \cong D_8$.

Note that the Cayley graph in Example 6.5 is symmetric. For half-arc-transitive graphs of valency 4 on groups of order p^4, we have the following theorem given by Feng, Kwak, Xu and Zhou [20].

Theorem 6.6. *Let X be a connected tetravalent half-arc-transitive graph of order p^4 for a prime p. Then $p \geq 3$ and X is a normal Cayley graph on a non-abelian group G of order p^4.*

Note that there exist connected tetravalent half-arc-transitive graphs whose stabilizers are not isomorphic to $\mathbb{Z}_2$ (see [6, 40, 41] for example). Since every tetravalent vertex transitive graph with an odd prime power must be a Cayley graph (see [16]), Theorems 6.4 and 6.6 suggest the following problem.

Problem 6.7. *Does there exist a connected tetravalent half-arc-transitive Cayley graph with order an odd-prime power which is nonnormal?*

By the way, as a more general case, the automorphism groups of edge-transitive tetravalent Cayley graphs of odd order were considered in [35], where a description of the automorphism groups of such graphs and a lot of nonnormal examples were given.

At the end of this paper we would like to mention two results about symmetric Cayley graphs with small valencies on the dihedral groups. One may deduce the following theorem from [9] and [19].

Theorem 6.8. *Let $D_{2n} = \langle a, b \mid a^2 = b^n = 1, a^{-1}ba = b^{-1}\rangle$ be the dihedral group of order* $2n$ *and let $X = \mathrm{Cay}(D_{2n}, S)$ be a connected symmetric cubic Cayley graph. Assume that X is normal. Then X is* 1*- or* 2*-regular. Furthermore, X is* 2*-regular if and only if $X \cong K_4$ and X is* 1*-regular if and only if S is equivalent to $\{a, ab, ab^k\}$ for $n \geq 13$, $4 \leq k < n$, and $k^2 - k + 1 \equiv 0 (\mathrm{mod}\ n)$.*

For Cayley graphs of valency 4 on dihedral groups, Wang and Xu [49] proved the following.

Theorem 6.9. *Let $D_{2n} = \langle a, b \mid a^2 = b^n = 1, a^{-1}ba = b^{-1}\rangle$ be the dihedral group of order* $2n$ *$(n > 6)$ and let $X = \mathrm{Cay}(D_{2n}, S)$ be a* 1*-regular Cayley graph of valency* 4*. Then X is normal, unless $n = 2m$, $m \geq 4$ is even, and $X \cong \mathrm{Cay}(G, \{a, a^{-1}, a^i b, a^{-i} b\})$, where $2 \leq i \leq m - 2$, and $i^2 = \pm 1 (\mathrm{mod}\ m)$. Moreover, if $i^2 = -1 (\mathrm{mod}\ m)$ then $m = 2 (\mathrm{mod}\ 4)$, and the vertex-stabilizer is isomorphic to $\mathbb{Z}_4$; while if $i^2 = 1 (\mathrm{mod}\ m)$ then $m = 0 (\mathrm{mod}\ 4)$, and the vertex-stabilizer is isomorphic to $\mathbb{Z}_2^2$.*

REFERENCES

[1] B. Alspach, Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree, *J. Combin. Theory*, **15**(1973), 12–17.

[2] B. Alspach and M.Y. Xu, 1/2-transitive graphs of order $3p$, *Journal of Algebraic Combinatorics*, **3**(1994), 347–355.

[3] Y.G. Baik, Y.-Q. Feng and H.S. Sim, The normality of Cayley graphs of finite Abelian groups with valency 5, *Systems Science and Mathematical Sciences*, **13**(2000), 425–431.

[4] Y.G. Baik, Y.-Q. Feng, H.S. Sim and M.Y. Xu, On the normality of Cayley graphs of Abelian groups, *Algebra Colloquium*, **5**(1998), 297–304.

[5] N. Biggs, Algebraic Graph Theory (second edition), Cambridge University Press, Cambridge, 1993.

[6] M.D.E. Conder and D. Marušič, A tetravalent half-arc-transitive with non-abelian vertex stabilizer, *J. Combin. Theory B*, **88**(2003), 67–76.

[7] J.D. Dixon and B. Mortimer, Permutation Groups, New York: Springer-Verlag, 1996, 97–97.

[8] E. Dobson and D. Witte, Transitive permutation groups of prime-squared degree, *J. Algebraic Combin.*, **16**(2002), 43–69.

[9] S.F. Du, Y.-Q. Feng, J.H. Kwak and M.Y. Xu, Cubic Cayley graphs on Dihedral groups, *Mathematical Analysis and Applications*, **7**(2004), 224–234.

[10] S.F. Du, R.J. Wang and M.Y. Xu, On the normality of Cayley digraphs of order twice a prime, *Australasian Journal of Combinatorics*, **18**(1998), 227–234.

[11] X.G. Fang, Z.P. Lu, J. Wang and M.Y. Xu, Cayley digraphs of finite simple groups of small out-valency, *Commun. Algebra*, **32**(2004), 1201–1211.

[12] X.G. Fang, C.E. Praeger and J. Wang, On the automorphism groups of Cayley graphs of finite simple groups, *J. London Math Soc.*, **66**(2002), 563–578.

[13] X.G. Fang, C.H. Li, J. Wang and M.Y. Xu, On cubic Cayley graphs of finite simple groups, *Discrete Mathematics*, **244**(2002), 67–75.

[14] X.G. Fang, C.H. Li and M.Y. Xu, On finite edge-transitive Cayley graphs of valency 4, *Europ. J. Combin.*, **25**(2004), 1107–1116.

[15] Y.-Q. Feng, Automorphism groups of Cayley graphs on symmetric groups with generating transposition sets, *J. Combin. Theory B*, **96**(2006), 67–72.

[16] Y.-Q. Feng, On vertex-transitive graphs of odd prime-power order, *Discrete Mathematics*, **248**(2002), 265–269.

[17] Y.-Q. Feng and T.P. Gao, Automorphism groups and isomorphisms of Cayley digraphs of abelian groups, *Australasian Journal of Combinatorics*, **16**(1997), 183–187.

[18] Y.-Q. Feng, J.H. Kwak and R.J. Wang, Automorphism groups of 4-valent connected Cayley graphs of p-groups, *Chin. Ann. Math.*, **22B**(2001), 281–286.

[19] Y.-Q. Feng, J.H. Kwak and M.Y. Xu, s-Regular cubic Cayley graphs on abelian or dihedral groups, Institute of Mathematics and School of Mathematical Sciences, Research Report No. 53, 2000.

[20] Y.-Q. Feng, J.H. Kwak, M.Y. Xu and J.-X. Zhou, Tetravalent half-arc-transitive graphs of order p^4, *Europ. J. Combin.*, **29**(2008), 555–567.

[21] Y.-Q. Feng, D.J. Wang and J.L. Chen, A family of nonnormal Cayley digraphs, *Acta Mathematica Sinica, English Series*, **17**(2001), 147–152.

[22] Y.-Q. Feng, R.J. Wang and M.Y. Xu, Automorphism groups of 2-valent connected Cayley digraphs on regular p-groups, *Graphs and Combinatorics*, **18**(2002), 253–257.

[23] Y.-Q. Feng and M.Y. Xu, Automorphism groups of tetravalent Cayley graphs on regular p-groups, *Discrete Math.*, **305**(2005), 354–360.

[24] Y.-Q. Feng and M.Y. Xu, Normality of tetravalent Cayley graphs of odd prime-cube order and its application, *Acta Mathematica Sinica, English Series*, **21**(2005), 903–912.

[25] C.D. Godsil, On the full automorphism group of a graph, *Combinatorica*, **1**(1981), 243–256.

[26] C.D. Godsil, G. Royle, Algebraic graph theory, Springer-Verlag, New York, 2001.

[27] D.M. Goldschmidt, Automorphisms of trivalent graphs, *Ann. Math.*, **111**(1980), 377–406.

[28] Q.X. Huang and J.X. Meng, Isomorphisms of circulant digraphs, *Appl. Math.—JCU*, **9B**(1994), 405–409.

[29] Q.X. Huang and J.X. Meng, Automorphism groups of Cayley digraphs, in *Combinatorics, Graph Theory, Algorithms and Applications*, edited by Y. Alavi, D.R. Lick and Jiuqiang Liu, World Scientific, Singapore, 1994; pp. 77–81.

[30] Q.X. Huang and J.X. Meng, On the isomorphisms and automorphism groups of circulants, *Graphs & Combin.*, **12**(1996), 179–187.

[31] B. Huppert, Endliche gruppen I, Springer-Verlag, Berlin, 1979.

[32] S. Lakshmivarahan, J.S. Jwo and S.K. Dhall, Symmetry in interconnection networks based on Cayley graphs of permutation groups: a survey, *Parallel Comput.*, **19**(1993), 361–407.

[33] C.H. Li, Isomorphisms of finite Cayley graphs, Ph.D. Thesis, The University of Western Australia, 1966.

[34] C.H. Li, On isomorphisms of connected Cayley graphs III, *Bull. Austral. Math. Soc.*, **58**(1998), 137–145.

[35] C.H. Li, Z.P. Lu and H. Zhang, Tetravalent edge-transitive Cayley graphs with odd number of vertices, *J. Combin. Theory B*, **96**(2006), 164–181.

[36] Z.P. Lu, On the automorphism groups of biCayley graphs, *Beijing Daxue Xuebao*, **39**(2003), no. 1, 1–5.

[37] Z.P. Lu, C.Q. Wang and M.Y Xu, Semisymmetric cubic graphs constructed from bi-Cayley graphs of A_n, *Ars Combin.*, **80**(2006), 177–187.

[38] Z.P. Lu and M.Y. Xu, On the normality of Cayley graphs of order pq, *Australasian Journal of Combinatorics*, **27** (2003), 81–93.

[39] A. Malnič, Group actions, coverings and lifts of automorphisms, *Discrete Mathematics*, **182**(1998), 203–218.

[40] A. Malnič and D. Marušič, Constructing 4-valent 1/2-transitive graphs with a non-abelian automorphism group, *J. Combin. Theory B*, **75**(1999), 46–55.

[41] A. Malnič and D. Marušič, Constructing $\frac{1}{2}$-arc-transitive graphs of valency 4 and vertex stabilizer $\mathbb{Z}_2 \times \mathbb{Z}_2$, *Discrete Math.*, **245**(2002), 203–216.

[42] J.X. Meng and B. Ying, Normal minimal Cayley digraphsf of abelian groups, *Europ. J. Combinatorics*, **21**(2000), 523–528.

[43] J.X. Meng and Q.X. Huang, The automorphism groups of minimal infinite circulant digraphs, *Europ. J. Combin.*, **18**(1997), 425–429.

[44] C.E. Praeger, Finite normal edge-transitive graphs, *Bull. Austral. Math. Soc.*, **60**(1999), 207–220.

[45] C.E. Praeger, R.J. Wang and M.Y. Xu, Symmetric graphs of order a product of two distinct primes, *J. Combin. Theory Ser. B*, **58**(1993), 299–318.

[46] C.E. Praeger and M.Y. Xu, Vertex primitive graphs of order a product of two distinct primes, *J. Combin. Theory Ser. B*, **59**(1993), 245–266.

[47] H.P. Qu, On symmetry of Cayley graphs of finite simple groups of valency 4, Ph.D. Thesis, Peking University, 2001.

[48] C.Q. Wang, D.J. Wang and M.Y. Xu, On normal Cayley graphs of finite groups, *Science in China A*, **28**(1998), 131–139.

[49] C.Q. Wang and M.Y. Xu, Non-normal one-regular and 4-valent Cayley graphs of dihedral groups D_{2n}, *Europ. J. Combin.*, **27**(2006), 750–766.

[50] R.J. Wang, $\frac{1}{2}$-transitive graphs of order a product of two distinct primes, *Communications in Algebra*, **22**(1994), 915–927.

[51] R.J. Wang and M.Y. Xu, A classification of symmetric graphs of order $3p$, *J. Combin. Theory Ser. B*, **58**(1993), 197–216.

[52] M.Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Mathematics*, **182**(1998), 309–319.

[53] M.Y. Xu, Half-transitive graphs of prime-cube order, *J. Algebraic Combinatorics*, **1**(1992), 275–292.

[54] M.Y. Xu and S.J. Xu, Symmetry properties of Cayley graphs of small valencies on the alternating group A_5, *Science in China A*, **47**(2004), 593–604.

[55] M.Y. Xu, Q.H. Zhang and J.X. Zhou, On the normality of Cayley digraphs on abelian groups (Chinese), *Systems Science and Mathematical Sciences*, **25**(2005), 700–710.

[56] S.J. Xu, X.G. Fang, J. Wang and M.Y. Xu, On cubic s-arc transitive Cayley graphs of finite simple groups, *Europ. J. Combinatorics*, **26**(2005), 133–143.

[57] S.J. Xu, X.G. Fang, J. Wang and M.Y. Xu, 5-Arc transitive cubic Cayley graphs on finite simple groups, *Europ. J. Combinatorics*, **28**(2007), 1023–1036.

[58] C.X. Zhou and Y.-Q. Feng, Automorphism groups of connected cubic Cayley graphs of order $4p$, *Algebra Colloquium*, **14**(2007), 351–359.

[59] J.X. Zhou and Y.-Q. Feng, Two sufficient conditions for non-normal Cayley graphs and their applications, *Science in China A*, **50**(2007), 201–216.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Symmetrical covers, decompositions and factorisations of graphs

Michael Giudici, Cai Heng Li & Cheryl E. Praeger
School of Mathematics and Statistics, The University of Western Australia Crawley, Australia

ABSTRACT: This paper introduces three new types of combinatorial structures associated with group actions, namely symmetrical covers, symmetrical decompositions, and symmetrical factorisations of graphs. These structures are related to and generalise various combinatorial objects, such as 2-designs, regular maps, near-polygonal graphs, and linear spaces. General theory is developed for each of these structures, pertinent examples and constructions are given, and a number of open research problems are posed.

1 INTRODUCTION TO THE CONCEPTS

In this introductory section we fix our notation and introduce the concepts of cover, decomposition and factorisation of a graph and explain when we regard such configurations as symmetrical. The objective of this chapter is to develop the general theory of symmetrical covers, decompositions and factorisations of graphs. We will mainly concentrate on the arc-symmetrical case.

A graph $\Gamma = (V, E)$ consists of a vertex set V and a subset E of unordered pairs of vertices called edges. Its automorphism group, denoted $\mathsf{Aut}(\Gamma)$, is the subgroup of all permutations of V that preserve E.

Let $\Gamma = (V, E)$ be a graph, and let $P_1, \ldots, P_k$ with $k \geq 2$ be subsets of the edge set E such that $E = P_1 \cup P_2 \cup \cdots \cup P_k$. Then $\mathcal{P} = \{P_1, \ldots, P_k\}$ is called a *cover* of Γ, and the P_i are called the *parts* of $\mathcal{P}$. A cover $\mathcal{P}$ of Γ is called a λ*-uniform cover* if each edge of Γ is contained in a constant number λ of the P_i. We usually identify a part P_i with its induced subgraph $[P_i] = (V_i, P_i)$ of Γ where V_i is the set of vertices of Γ which lie on an edge in P_i.

The well known *cycle double cover* conjecture for graphs (see [17, 18]) asserts that every 2-edge connected graph has a 2-uniform cover by cycles. The λ-uniform covers of the complete graph K_n with parts isomorphic to K_k correspond to the 2-(n, k, λ) *designs* (see for example [13]). The vertices of K_n correspond to the points of the design, while each block of the design is the set of vertices in some part of the cover. Since each edge lies in λ parts, it follows that each pair of points lies in λ blocks.

A 1-uniform cover, that is, a cover such that every edge of Γ is contained in precisely one part is called a *decomposition* of Γ. Under the correspondence described in the previous paragraph, decompositions of a complete graph with parts isomorphic to K_k correspond to *linear spaces* with line size k. This is discussed further in Section 4.2. A decomposition is called a *factorisation* if each part is a spanning subgraph. (By spanning, we mean that for every vertex v of Γ there is an edge $\{v, w\}$ in the subgraph.)

For a decomposition $\mathcal{P} = \{P_1, P_2, \ldots, P_k\}$ of a graph Γ, if the subgraphs induced by each of the P_i are all isomorphic to Σ, then the decomposition is called an *isomorphic decomposition*, and Σ is called a *divisor* of Γ. An isomorphic decomposition of a graph is called an *isomorphic factorisation* if it is a factorisation, and in this case the divisors are called *factors*. Decompositions of graphs have been widely studied, see for example [3, 13], as have isomorphic factorisations, for example [11, 12].

Let $\mathcal{P}$ be a cover of Γ and let $G \leqslant \mathsf{Aut}(\Gamma)$. If G preserves $\mathcal{P}$ and the permutation group $G^{\mathcal{P}}$ induced on $\mathcal{P}$ is transitive then we say that the cover $(\Gamma, \mathcal{P})$ is *G-transitive*. If further

Table 1. Possibilities for X and xxx.

X	V	E	A
xxx	vertex	edge	arc

$\mathcal{P}$ is a decomposition or a factorisation of Γ, then Γ is called a *G-transitive decomposition* or a *G-transitive factorisation*, respectively. By definition, a transitive cover, decomposition or factorisation is an isomorphic cover, decomposition or factorisation, respectively. Symmetries of decompositions have been studied in [30, 33]. In particular, Robinson conjectured that every finite group occurs as $G^{\mathcal{P}}$ where $(\Gamma, \mathcal{P})$ is an isomorphic factorisation of a complete graph Γ and G is the largest group of automorphisms of Γ preserving $\mathcal{P}$. He showed [30, Proposition 3] that every finite group does occur as a subgroup of some $G^{\mathcal{P}}$. To our knowledge this conjecture is still open.

In this paper, transitivity is required not only on the set of parts, divisors, or factors, but also on the graphs: namely on their vertices or edges or arcs. For any graph Γ we denote by $V\Gamma$, $E\Gamma$, $A\Gamma$ the set of vertices, edges, and arcs respectively.

Definition 1.1. Let Γ be a graph, and let $\mathcal{P}$ be a G-transitive cover, decomposition, or factorisation, of Γ, where $G \leq \mathsf{Aut}\Gamma$. Let G_P be the stabiliser in G of the part $P \in \mathcal{P}$ and let X, xxx be as in one of the columns of Table 1. If G is transitive on $X\Gamma$ and G_P is transitive on XP, then $(\Gamma, \mathcal{P})$ is called G-xxx-*symmetrical*.

We remark that there are $3 \times 3 = 9$ different objects defined in this definition; for example, if Γ is G-arc-transitive and P is G_P-arc-transitive, then $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical cover, decomposition or factorisation. We see in Lemma 4.4 that if $(\Gamma, \mathcal{P})$ is a G-transitive decomposition and Γ is G-arc-transitive (respectively G-edge-transitive) then $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical (respectively G-edge-symmetrical) decomposition. The following simple examples show that neither implication is true for covers.

Example 1.2. Let $\Gamma = C_6$ with vertices labelled by the elements of $\mathbb{Z}_6$ and x adjacent to $x \pm 1$ (mod 6).

(1) Let

$$P_1 = \{\{0,1\},\{1,2\},\{2,3\},\{3,4\}\}$$
$$P_2 = \{\{2,3\},\{3,4\},\{4,5\},\{5,0\}\}$$
$$P_3 = \{\{4,5\},\{5,0\},\{0,1\},\{1,2\}\}$$

and $\mathcal{P} = \{P_1, P_2, P_3\}$. Then $(\Gamma, \mathcal{P})$ is a 2-uniform cover which is invariant under the group $G = D_6$ (the dihedral group of order 6). Now G acts transitively on $\mathcal{P}$ and on the set of edges of Γ. However, $G_{P_1} \cong C_2$ is not transitive on the edges of P_1. Hence $(\Gamma, \mathcal{P})$ is not G-edge-symmetrical.

(2) Let

$$P_1 = \{\{0,1\},\{1,2\},\{2,3\},\{3,4\}\}$$

and let $\mathcal{P} = P_1^{C_6}$. Then $|\mathcal{P}| = 6$ and is preserved by $G = D_{12}$ and $(\Gamma, \mathcal{P})$ is a G-transitive, 4-uniform cover. However, the group G acts transitively on the set of arcs of Γ while $G_{P_1} \cong C_2$ is not transitive on the arcs of P_1. Hence $(\Gamma, \mathcal{P})$ is not G-arc-symmetrical.

Arc-symmetrical covers of graphs with no isolated vertices are both edge-symmetrical and vertex-symmetrical. Conversely, it is a consequence of Lemma 4.4 (see Remark 4.5) that if $(\Gamma, \mathcal{P})$ is a G-edge-symmetrical decomposition and G acts arc-transitively on Γ then $(\Gamma, \mathcal{P})$ is G-arc-symmetrical. Similarly, if $(\Gamma, \mathcal{P})$ is a G-vertex-symmetrical decomposition and G acts edge-transitively (respectively arc-transitively) on Γ, then $(\Gamma, \mathcal{P})$ is G-edge-symmetrical (respectively G-arc-symmetrical). We see in Examples 3.4 and 3.16 that the same is not true for covers.

In the literature, various special cases of symmetrical covers, decompositions and factorisations have been studied. Arc-symmetrical 1-factorisations of complete graphs are classified by Cameron and Korchmáros in [6]. Arc-symmetrical 1-factorisations of arc-transitive graphs are addressed in [10] where a characterisation of those for 2-arc-transitive graphs is given. Arc-symmetrical decompositions of complete graphs are studied in [31], and arc-symmetrical decompositions of rank three graphs are investigated in [1]. The G-arc-symmetrical decompositions of Johnson graphs where G acts primitively on the set of divisors of the decomposition are classified in [8].

If $(\Gamma, \mathcal{P})$ is a G-transitive decomposition and the kernel M of the action of G on $\mathcal{P}$ is vertex-transitive, then $(\Gamma, \mathcal{P})$ is called a *(G, M)-homogeneous factorisation*. In particular, homogeneous factorisations are vertex-symmetrical. The study of homogeneous factorisations was initiated by the second and third authors who introduced in [21] homogeneous factorisations of complete graphs. General homogeneous factorisations were introduced and investigated in [14] and studied further in [15, 16].

The next section gives some fundamental notions and results on permutation groups that underpin an investigation of these symmetrical configurations. This is followed by three sections addressing basic examples and theory for covers, decompositions and factorisations respectively. In the final section we discuss the behaviour of covers and decompositions when we pass to the quotient graph.

2 SOME FUNDAMENTALS CONCERNING PERMUTATION GROUPS

In this section we introduce some permutation group notions needed later. The reader is referred to [19] for more details.

Given a permutation group G acting on a set Ω and $\alpha \in \Omega$, we let $G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$, the stabiliser in G of α. Let $B = \{\alpha_1, \ldots, \alpha_k\} \subseteq \Omega$. For $g \in G$, $B^g = \{\alpha^g \mid \alpha \in B\}$ and the *setwise stabiliser* of B in G is $G_B = \{g \in G \mid B^g = B\}$. The *pointwise stabiliser* of B in G is $G_{(B)} = \{g \in G \mid \alpha_1^g = \alpha_1, \alpha_2^g = \alpha_2, \ldots, \alpha_k^g = \alpha_k\}$ and is also denoted by $G_{\alpha_1,\alpha_2,\ldots,\alpha_k}$. The following lemma will be particularly useful.

Lemma 2.1 [9, Ex 1.4.1]. *Let G be a transitive subgroup of $\mathsf{Sym}(\Omega)$ and $H \leqslant G$. Then $G = HG_\alpha$ if and only if H is transitive on Ω.*

Let G be a transitive subgroup of $\mathsf{Sym}(\Omega)$. A partition $\mathcal{B} = \{B_1, \ldots, B_k\}$ of Ω is called a *system of imprimitivity* and its elements are called *blocks of imprimitivity*, if for each $g \in G$ and $B_i \in \mathcal{B}$, the image $B_i^g \in \mathcal{B}$. Trivial blocks of imprimitivity exist for any transitive group G, and are the singleton subsets $\{\alpha\}$ $(\alpha \in \Omega)$ and the whole set Ω. All other blocks of imprimitivity are called nontrivial and a transitive group G is said to be *imprimitive* if there exists a nontrivial block of imprimitivity. Given $\alpha \in \Omega$, there is a one-to-one correspondence between the subgroups H with $G_\alpha \leqslant H \leqslant G$ and the blocks of imprimitivity B containing α, given by $B = \alpha^H$ and $H = G_B$. See for example [9, Theorem 1.5A]. In particular, note that the stabiliser in G of a block of imprimitivity B is transitive on B. We say that G is *primitive* if it has no nontrivial systems of imprimitivity. It follows from the correspondence between blocks and overgroups of G_α that a transitive group G on Ω is primitive if and only if G_α is maximal in G for some $\alpha \in \Omega$.

Every nontrivial normal subgroup of a primitive group is transitive, for otherwise, the set of orbits of an intransitive normal subgroup forms a system of imprimitivity. We say that a permutation group is *quasiprimitive* if every nontrivial normal subgroup is transitive. Thus every primitive group is quasiprimitive. However, not every quasiprimitive group is primitive. For example, the right multiplication action of a nonabelian simple group on the set of right cosets of a nonmaximal subgroup is quasiprimitive but not primitive.

Given two graphs Γ, Σ we define the *cartesian product* of Γ and Σ to be the graph denoted by $\Gamma\Box\Sigma$ with vertex set $V\Gamma \times V\Sigma$ and $\{(u_1, u_2), (v_1, v_2)\}$ is an edge if and only if either $u_1 = v_1$ and $\{u_2, v_2\} \in E\Sigma$, or $\{u_1, v_1\} \in E\Gamma$ and $u_2 = v_2$. If $G \leqslant \mathsf{Aut}(\Gamma)$ and $H \leqslant \mathsf{Aut}(\Sigma)$ then $G \times H \leqslant \mathsf{Aut}(\Gamma\Box\Sigma)$. The cartesian product of graphs is associative and hence the cartesian product $\Gamma_1\Box\Gamma_2\Box \cdots \Box\Gamma_t$ for graphs $\Gamma_1, \Gamma_2, \ldots , \Gamma_t$ is well defined for any $t \geq 2$.

3 TRANSITIVE COVERS AND SYMMETRICAL COVERS

Our first lemma shows that many covers of edge-transitive graphs are uniform.

Lemma 3.1. *Let Γ be a G-edge-transitive graph and $\mathcal{P}$ be a cover of Γ which is G-invariant. Then $(\Gamma, \mathcal{P})$ is a uniform cover.*

Proof. Let $\{u, v\}$ be an edge of Γ and suppose that $\{u, v\}$ is contained in precisely λ parts of $\mathcal{P}$. Since G is edge-transitive and $\mathcal{P}$ is G-invariant, λ is independent of the choice of $\{u, v\}$. Thus $\mathcal{P}$ is a λ-uniform cover. □

In fact every edge-transitive graph has many transitive covers. Here by a subgraph Σ of a graph Γ we mean any graph (U, E_U) where $U \subseteq V$ and $E_U \subseteq E \cap (U \times U)$. Also, for a subset $P \subseteq E$, the edge-induced subgraph $[P]$ is the subgraph (V_P, P) where V_P is the subset of vertices incident with at least one edge of P.

Lemma 3.2. *An edge-transitive graph Γ has a transitive cover with parts Σ if and only if Γ has a subgraph isomorphic to Σ.*

Proof. Let Σ be a subgraph of Γ and $G \leqslant \mathsf{Aut}(\Gamma)$ be edge-transitive. Let $P = E\Sigma$, and let $\mathcal{P} = P^G$. Then by definition, $(\Gamma, \mathcal{P})$ is a G-transitive cover with parts isomorphic to Σ. □

Each edge-intransitive subgroup of an edge-transitive group gives rise to edge-symmetrical uniform covers and the parameters λ can be expressed group theoretically.

Lemma 3.3. *Let $\Gamma = (V, E)$ be a connected G-edge-transitive graph and let $H < G$ such that H is intransitive on $E\Gamma$. Let P be an H-orbit in $E\Gamma$ and $\mathcal{P} = P^G$. Then $(\Gamma, \mathcal{P})$ is a G-edge-symmetrical λ-uniform cover with*

$$\lambda = \frac{|G_{\{v,w\}} : H_{\{v,w\}}|}{|G_P : H|}$$

where $\{v, w\} \in P$. Moreover, if Γ is G-arc-transitive and for each $\{v, w\} \in P$ there exists $g \in H$ such that $(v, w)^g = (w, v)$, then $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical cover.

Proof. By definition, $H \leqslant G_P$ and the edge-induced subgraph $[P]$ is H-edge-transitive. Since G is edge-transitive, every edge of Γ occurs in some image of P and so $\mathcal{P}$ is a G-transitive cover. Then by Lemma 3.1, $(\Gamma, \mathcal{P})$ is a λ-uniform cover for some λ and since $[P]$ is H-edge-transitive $(\Gamma, \mathcal{P})$ is G-edge-symmetrical. Moreover, $G_P = HG_{\{v,w\},P}$, so $|P| = |G_P : G_{\{v,w\},P}| = |H : H_{\{v,w\}}|$. Since $\mathcal{P}$ is a λ-uniform cover, we have

$$|H : H_{\{v,w\}}||G : G_P| = |P||\mathcal{P}| = \lambda|E| = \lambda|G : G_{\{v,w\}}| = \frac{\lambda|G : G_P||G_P : H||H : H_{\{v,w\}}|}{|G_{\{v,w\}} : H_{\{v,w\}}|}.$$

Hence $\lambda = |G_{\{v,w\}} : H_{\{v,w\}}|/|G_P : H|$. □

As noted in the introduction, every G-arc-symmetrical cover of a graph with no isolated vertices is G-edge-symmetrical and G-vertex-symmetrical. The following is an example of a G-edge-symmetrical cover of a G-arc-transitive graph which is not G-arc-symmetrical. In particular, it shows that for an arc-transitive graph, spinning an edge will not necessarily give an arc-symmetrical cover. Moreover, it is an example of the construction underlying Lemma 3.2, and if we take H to be a subgroup C_{11} it also illustrates Lemma 3.3.

Example 3.4. Let $\Gamma = K_{11}$ and $G = M_{11}$. Then Γ is G-arc-transitive. Let Σ be an 11-cycle in Γ. Since $M_{11} \cap D_{22} = C_{11}$, it follows that $G_\Sigma = C_{11}$ which is edge-transitive and vertex-transitive on Σ, but not arc-transitive. Let $P = E\Sigma$ and $\mathcal{P} = P^G$. Then $(\Gamma, \mathcal{P})$ is a G-edge-symmetrical and G-vertex-symmetrical cover which is not G-arc-symmetrical.

We are often interested in λ-covers for small values of λ, so we propose the following problems.

Problem 3.5.

(i) For small values of λ, characterise the arc-transitive graphs that have an arc-symmetrical λ-uniform cover.

(ii) For a given arc-transitive graph Γ, find the smallest value of λ such that Γ has an arc-symmetrical λ-uniform cover.

To illustrate the theory, we will present briefly some examples of symmetrical covers of some well known graphs, and examples of symmetrical covers with given specified parts.

3.1 *Covers of complete graphs*

Lemma 3.3 has the following corollary.

Corollary 3.6. *For an edge-transitive graph Σ on m vertices, a complete graph K_n with $n \geq m$ has an edge-symmetrical cover with parts isomorphic to Σ.*

Lemma 3.3 and Corollary 3.6 lead to the following illustrative examples.

Example 3.7. Let $\Gamma = K_n$, a complete graph with n vertices.

(i) Let $G = \mathsf{Aut}\Gamma = S_n$, acting arc-transitively on Γ. Let P be a complete subgraph of Γ with m vertices, where $m < n$. Then $G_P = S_m \times S_{n-m}$, and acts arc-transitively on P. Let $\mathcal{P}$ be the set of all complete subgraphs with m vertices. Since G is m-transitive on $V\Gamma$, G is transitive on $\mathcal{P}$. Thus $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical cover of K_n. Further, $\mathcal{P}$ is an $\binom{n-2}{m-2}$-uniform cover.

(ii) Let $n = q + 1 = p^d + 1$ with p prime, and let $G = \mathrm{PGL}(2, q)$. Let P be a 3-cycle of Γ. Then $G_P = S_3$. Let $\mathcal{P}$ be the set of all 3-cycles of Γ. Since G is 3-transitive on $V\Gamma$, the pair $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical cover. It is an $(n-2)$-uniform cover.

(iii) Let $n \geq 10$ and $G = \mathsf{Aut}\Gamma = S_n$. Let $H \cong S_5$ be a subgroup of G acting transitively on a subset $\Delta \subset \Omega$ of size 10. Then there exist two vertices $v, w \in \Delta$ such that the induced subgraph $\Sigma := [\{v, w\}^H]$ is a Petersen graph. Let $\mathcal{P} = \Sigma^G$. Then $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical λ-uniform cover with $\lambda = (n-2)!/4(n-10)!$ and parts the Petersen graph.

(iv) Let $n = q + 1$ with $q = 3^f$ with f even. Let $G = \mathrm{PSL}(2, q)$ and $H \leqslant G$ such that $H \cong A_5$. Then G is arc-transitive on Γ and by [7, Lemma 11], H has an orbit Δ on vertices of size 10. There exist two vertices $v, w \in \Delta$ such that the induced subgraph $\Sigma := [\{v, w\}^H]$ is a Petersen graph. Let $\mathcal{P} = \Sigma^G$. Then $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical λ-uniform cover with $\lambda = \frac{q-1}{4}$. Note in particular, that when $q = 9$ then $\lambda = 2$.

3.2 *Covers for complete multipartite graphs*

For integers $m, n \geq 2$, a complete m-partite graph with part size n is denoted by $K_{m[n]} = K_{n,n,\ldots,n}$. The following corollary to Lemma 3.3 for complete multipartite graphs is analogous to Corollary 3.6 for complete graphs.

Corollary 3.8. *Let Σ be an H-edge-transitive graph such that $V\Sigma$ has an H-invariant partition $\mathcal{B}$ with block size b and $|\mathcal{B}| = l$. Then for each $m \geq l$ and $n \geq b$, $K_{m[n]}$ has an edge-symmetrical cover with parts isomorphic to Σ.*

Here are some examples.

Example 3.9. Let $\Gamma = K_{m[n]}$, and let $G = \mathsf{Aut}\Gamma = S_n \operatorname{wr} S_m$.

(i) For $m = 2$, let $\mathcal{P}$ be the set of all induced subgraphs of Γ which are isomorphic to $K_{i,i}$ for $i < n$. For $P \in \mathcal{P}$, $H := (S_i \times S_{n-i}) \operatorname{wr} S_2$, acts arc-transitively on P. Further, G is transitive on $\mathcal{P}$, and $(\Gamma, \mathcal{P})$ is a G-arc symmetrical λ-uniform cover, where $\lambda = \binom{n-1}{i-1}^2$.

(ii) For $m \geq 3$, let $\mathcal{P}$ be the set of all induced subgraphs of Γ that are isomorphic to K_m. Let $P \in \mathcal{P}$. Then $G_P = S_{n-1} \operatorname{wr} S_m$ acts arc-transitively on P, and $(\Gamma, \mathcal{P})$ is a G-transitive n^{m-2}-uniform cover. Taking $m = 3$ and $G = S_n \operatorname{wr} S_3$, shows that the complete tri-partite graph $K_{n,n,n}$ is G-arc transitive and has a G-arc-symmetrical n-uniform 3-cycle cover.

3.3 *Covers involving cliques*

For $n > k$, the Johnson graph $J(n,k)$ is the graph with V the set of k-element subsets of an n-set with two subsets adjacent if they have $k-1$ points in common. The valency of $J(n,k)$ is $k(n-k)$ and the group $G = S_n$ acts arc-transitively on $J(n,k)$. For an edge $\{v, w\}$, we have $G_v = S_k \times S_{n-k}$, and $G_{vw} = S_{k-1} \times S_{n-k-1}$.

Example 3.10. Let $\Gamma = J(n,k)$ and $G = S_n$. Let ℓ satisfy $1 \leq \ell < k$ and let I be the set of ℓ-element subsets of the n-set. For each $A \in I$, let $\Gamma_A = (V_A, E_A)$ where V_A consists of all the k-element subsets containing A, and E_A is the subset of E joining elements of V_A. Then $\Gamma_A \cong J(n-\ell, k-\ell)$, and each edge $\{B, C\}$ of Γ is an edge of each of the $\binom{k-1}{\ell}$ graphs Γ_A such that $A \subseteq B \cap C$. The stabiliser G_A of Γ_A induces $S_{n-\ell}$ on Γ_A. Thus $\mathcal{G} = \{\Gamma_A \mid |A| = \ell\}$ is an edge-symmetrical uniform cover with $\lambda = \binom{k-1}{l}$ and hence is a factorisation if $\ell = k-1$. In this latter case the factors $J(n-k+1, 1) \cong K_{n-k+1}$ are maximal cliques of Γ.

The previous example was pointed out to us by Michael Orrison who uses the case $l = k-1$ in [25] for the analysis of unranked data. He also noticed that it is a special case of clique covers of graphs, that is, covers in which the parts are cliques (complete subgraphs). These arise naturally for edge-transitive graphs as follows. Let Γ be a G-edge transitive graph and let A be a maximal clique. Let $\mathcal{G} = A^G = \{A^g | g \in G\}$. Then $(\Gamma, \mathcal{G})$ is a uniform cover which is G-transitive. There are some graphs for which each edge lies in exactly one clique in the G-class of cliques $\mathcal{G}$. For these graphs $\mathcal{G}$ is a G-edge-symmetrical decomposition (see Lemma 4.4).

3.4 *Cycle covers, near polygonal graphs and rotary maps*

Each finite arc-transitive graph of valency at least three contains cycles. The next example shows that such graphs have edge-symmetrical cycle covers. The method presented here has been used in [23] for constructing polygonal graphs and we discuss this below.

Construction 3.11. Let Γ be a regular graph of valency at least 3, and $G \leq \mathsf{Aut}\Gamma$ be such that Γ is G-arc transitive. Then there exists a set $\mathcal{P}$ of cycles such that $(\Gamma, \mathcal{P})$ is a G-edge-symmetrical cycle cover. The set $\mathcal{P}$ is constructed as follows: For a pair of adjacent vertices v and w, let $g \in G \backslash G_v$

such that $v^g = w$ and $w^g \neq v$. Then the set of images of (v, w) under $\langle g \rangle$ forms a cycle C say. Let $\mathcal{P} = C^G$.

The fact that the partition $\mathcal{P}$ produced in Construction 3.11 is a G-edge-symmetrical cover of Γ follows from [23, Lemmas 1.1 and 2.2], and further, if G_C^C is dihedral, then $\mathcal{P}$ is a G-arc-symmetrical cover.

Example 3.12. Let $\Gamma = K_4$, the complete graph on 4 vertices, and let $G = \mathsf{Aut}\Gamma = S_4$. Let (v, w) be an arc. Let $\mathcal{P}$ be a cover of Γ produced by Construction 3.11. If $g \in G$ is of order 3, then $\mathcal{P}$ contains 4 triangles while if $g \in G$ is of order 4, then $\mathcal{P}$ contains 3 cycles of length 4. In both cases $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical 2-uniform cycle cover.

A 2-*arc* in a graph Γ is a triple (u, v, w) such that $u \neq w$ and both (u, v) and (v, w) are arcs. Following [27], a graph Γ is called a *near-polygonal graph* if there is a collection $\mathcal{C}$ of m-cycles in Γ such that each 2-arc of Γ is contained in exactly one cycle in $\mathcal{C}$. Suppose that Γ is such a graph of valency k and that $G \leqslant \mathsf{Aut}(\Gamma)$ preserves $\mathcal{C}$ and is transitive on the set of 2-arcs of Γ. Then G_{vw} is transitive on $\Gamma(v)\backslash\{w\}$ and for each of the $k-1$ vertices $u \in \Gamma(v)\backslash\{w\}$, the 2-arc (u, v, w) lies in a unique cycle of $\mathcal{C}$. Moreover, these cycles are pairwise distinct, by definition of $\mathcal{C}$, and they are the only cycles of $\mathcal{C}$ containing (w, v) since each such cycle must contain (u, v, w) for some $u \in \Gamma(v)\backslash\{w\}$. Thus the edge $\{v, w\}$ lies in exactly $k-1$ cycles in $\mathcal{C}$, that is, $\mathcal{C}$ is a $(k-1)$-uniform cycle cover and is G-arc-symmetrical. Examples of infinite families of near-polygonal graphs can be found in [23, 27, 28]. It is shown in [23] that each 2-arc-regular graph (that is, $\mathsf{Aut}(\Gamma)$ is regular on the 2-arcs of Γ) is a near-polygonal graph, so each 2-arc-regular graph of valency k has an arc-symmetrical $(k-1)$-uniform cycle cover. In particular, 2-arc-regular cubic graphs have a 2-uniform cycle cover.

A *map* on a surface (2-manifold) is a 2-complex of the surface. The 0-cells, 1-cells and 2-cells of the 2-complex are called vertices, edges and faces of the map, respectively. Incidence between these objects is defined by inclusion. A map $\mathcal{M}$ may be viewed as a 2-cell embedding of the underlying graph Γ into the supporting surface. A vertex-edge incident pair is called a *dart*, and a pairwise incident vertex-edge-face triple is called a *flag*. A permutation of flags of a map $\mathcal{M}$ preserving the incidence relation is an *automorphism* of $\mathcal{M}$, and the set of all automorphisms of $\mathcal{M}$ forms the map automorphism group $\mathsf{Aut}\mathcal{M}$. A map $\mathcal{M}$ is said to be *rotary* or *regular* if $\mathsf{Aut}\mathcal{M}$ acts transitively on the darts or on the flags of $\mathcal{M}$, respectively. Further, a rotary map is called *chiral* if it is not regular.

Example 3.13. Let $\mathcal{M}$ be a map with underlying graph Γ, and let $G = \mathsf{Aut}\mathcal{M}$. Let $\mathcal{P}$ be the set of cycles which are boundaries of faces of $\mathcal{M}$. Then $\mathcal{P}$ is a 2-uniform cycle cover of the underlying graph Γ. If $\mathcal{M}$ is regular, then $\mathcal{P}$ is a G-arc-symmetrical cycle cover; if $\mathcal{M}$ is chiral, then $\mathcal{P}$ is a G-edge-symmetrical but not G-arc-symmetrical cover.

3.5 *Vertex-symmetrical covers*

First we note that not every vertex-symmetrical cover is a uniform cover, as seen in the following example.

Example 3.14. Let $\Gamma \cong K_2 \square K_4$ be the graph with vertex set such that $\{1, 2\} \times \{1, 2, 3, 4\}$ and (u_1, v_1) is adjacent to (u_2, v_2) if and only if $u_1 = u_2$ or $v_1 = v_2$. We saw in Example 3.12, that K_4 has an S_4-arc-symmetrical 2-uniform cover $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ consisting of four 3-cycles. For each $P_i \in \mathcal{P}$, let Q_i be the set of edges $\{(u_1, v_1), (u_2, v_2)\}$ such that $v_1 = v_2$, or $u_1 = u_2$ and $\{v_1, v_2\} \in P_i$. Then $\mathcal{Q} = \{Q_1, Q_2, Q_3, Q_4\}$ is a cover of Γ with edges of the form $\{(u_1, v), (u_2, v)\}$ lying in all four parts while edges of the form $\{(u, v_1), (u, v_2)\}$ lie in precisely two parts. The group $G = S_2 \times S_4$ is vertex-transitive on Γ, preserves $\mathcal{Q}$ and $G^{\mathcal{Q}}$ is transitive. Moreover, for $Q \in \mathcal{Q}$, $G_Q = S_2 \times S_3$ is transitive on the vertices in Q and so $\mathcal{Q}$ is a G-vertex-symmetrical cover.

We have the following general construction of vertex-symmetrical covers.

Construction 3.15. Let $\Gamma = (V, E)$ be a G-vertex-transitive graph. Let $H < G$ and let V_0 be an orbit of H on vertices. Suppose that there exists an H-invariant nonempty subset $P \neq E$ of the edge set of the induced subgraph $[V_0]$ such that P contains an edge from each G-orbit on E, and let $\mathcal{P} = P^G$. Then each edge of Γ lies in some P^g. Also, as V_0 is an H-orbit and P is H-invariant, each vertex of V_0 lies in some edge of P. Thus $V_P = V_0$ and so $H \leqslant G_P$ is transitive on VP. Hence $(\Gamma, \mathcal{P})$ is a G-vertex-symmetrical cover.

Every G-arc-symmetrical cover is G-vertex-symmetrical and Example 3.14 shows that the converse is not true in general. Moreover, the following example shows that even if Γ is G-arc-transitive, a G-vertex-symmetrical cover is not necessarily G-edge-symmetrical.

Example 3.16. Let $\Gamma = K_{12}$ and $G = \mathrm{PSL}(2, 11)$. Then Γ is G-arc-transitive. Moreover, there exists a set V_0 of 5 vertices such that $G_{V_0} \cong C_5$. Let P be the complete graph on V_0 and $\mathcal{P} = P^G$. Then as seen in Construction 3.15, $(\Gamma, \mathcal{P})$ is a G-vertex-symmetrical cover. Since G_{V_0} is not edge-transitive on P, $(\Gamma, \mathcal{P})$ is not G-edge-symmetrical.

We have already seen in Section 1 that uniform covers correspond to 2-designs. This leads to the following lemma.

Lemma 3.17. *A uniform cover $(\Gamma, \mathcal{P})$ of a complete graph $\Gamma = (V, E)$ with complete subgraph parts is G-vertex-symmetrical if and only if $(V, \mathcal{P})$ is a G-flag-transitive 2-design.*

4 TRANSITIVE DECOMPOSITIONS

By definition, an xxx-symmetrical decomposition is an xxx-symmetrical 1-uniform cover for each xxx $\in$ {vertex, edge, arc}. Any G-arc-transitive graph has a G-arc-symmetrical decomposition with each divisor consisting of a single edge. Such a decomposition is called *trivial*. We have the following existence criterion for nontrivial transitive decompositions of edge-transitive graphs.

Lemma 4.1. *Let Γ be a G-edge-transitive graph. Then Γ has a non-trivial G-transitive decomposition if and only if G acts on $E\Gamma$ imprimitively. More precisely, a subgraph Σ of Γ is a divisor of a G-transitive decomposition if and only if $E\Sigma$ is a block of imprimitivity for G acting on $E\Gamma$.*

Proof. By definition a partition $\mathcal{P}$ of $E\Gamma$ forms a G-transitive decomposition of Γ precisely if $\mathcal{P}$ is G-invariant, that is to say, $\mathcal{P}$ is a system of imprimitivity for G on $E\Gamma$. □

This leads to the following general construction.

Construction 4.2. Let Γ be a G-edge-transitive graph. Suppose that $\{v, w\}$ is an edge of Γ and $G_{\{v,w\}} < H < G$. Let $P = \{v, w\}^H$. Then $\mathcal{P} = P^G$ is a G-transitive decomposition of Γ.

In fact, every transitive decomposition of an edge-transitive graph arises in this way.

Lemma 4.3. *Let $(\Gamma, \mathcal{P})$ be a G-transitive decomposition with G acting edge-transitively on Γ. Then $(\Gamma, \mathcal{P})$ arises from Construction 4.2 using $H = G_P$, where P is the divisor of $\mathcal{P}$ containing $\{v, w\}$.*

Proof. By Lemma 4.1, P is a block of imprimitivity for G on $E\Gamma$. Thus $G_{\{v,w\}} < G_P$ and $P = \{v, w\}^{G_P}$. □

We further note that when studying transitive decompositions, if G acts imprimitively on $\mathcal{P}$ then there is a partition $\mathcal{Q}$ of $E\Gamma$ refined by $\mathcal{P}$ such that G acts primitively on $\mathcal{Q}$. Moreover, $(\Gamma, \mathcal{Q})$

is also a G-transitive decomposition. For some families of graphs the most reasonable approach is to study G-transitive decompositions $(\Gamma, \mathcal{Q})$ such that $G^{\mathcal{Q}}$ is primitive. For example, this was done for the Johnson graphs in [8] giving a classification of such decompositions.

4.1 *Edge-symmetrical and arc-symmetrical decompositions*

First we observe that in the edge-transitive and arc-transitive cases, transitive decompositions are symmetrical decompositions.

Lemma 4.4. *Let $(\Gamma, \mathcal{P})$ be a G-transitive decomposition. If G is edge-transitive on Γ then $(\Gamma, \mathcal{P})$ is G-edge-symmetrical; if G is arc-transitive on Γ then $(\Gamma, \mathcal{P})$ is G-arc-symmetrical.*

Proof. If G is edge-transitive on Γ, Lemma 4.1 implies that $\mathcal{P}$ is a system of imprimitivity for G on $E\Gamma$. Thus for $P \in \mathcal{P}$, G_P is transitive on P and so $(\Gamma, \mathcal{P})$ is a G-edge-symmetrical decomposition. Moreover, if G is also arc-transitive then $\mathcal{P}$ is a system of imprimitivity for G on $A\Gamma$ and it follows that $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical decomposition. □

Remark 4.5. Since G-vertex-symmetrical decompositions are G-transitive decompositions it follows that G-vertex-symmetrical decompositions of G-edge-transitive graphs (respectively G-arc-transitive graphs) are also G-edge-symmetrical (respectively G-arc-symmetrical). Similarly, G-edge-symmetrical decompositions of G-arc-transitive graphs are G-arc-symmetrical.

By Lemmas 4.4 and 4.3, all edge-symmetrical decompositions and arc-symmetrical decomposition arise from Construction 4.2.

We give two examples of arc-symmetrical decompositions to illustrate how Construction 4.2 may be applied to two important families of graphs.

Example 4.6. Let Γ be the Petersen graph, and let $G = A_5$. Let $\{u, v\}$ be an edge of Γ. Then $G_{\{u,v\}} = C_2^2 < A_4 < G$. Hence letting $H = A_4$ we obtain a G-arc-symmetrical decomposition of Γ. Each part consists of three disjoint edges.

This example generalises as follows. Let $\Gamma = O_k$, an odd graph of degree k, that is the graph with vertex set the set of all k-subsets of a $(2k+1)$-set such that two k-sets are adjacent if and only if they are disjoint. Then $G = S_{2k+1} \leq \mathsf{Aut}\Gamma$, and acts transitively on the set of arcs of Γ. The graph Γ has $\binom{2k+1}{k}$ vertices, and is of valency $k+1$, so Γ has $\binom{2k+1}{k}(k+1)/2$ edges. The group $G = S_{2k+1}$ is imprimitive on $E\Gamma$. For two adjacent vertices v, w, the vertex stabiliser $G_v = S_{k+1} \times S_k$, and the edge stabiliser satisfies $G_{\{v,w\}} = (S_k \times S_k) \cdot 2 < H := S_{2k}$. Let $P = \{(v, w)^g \mid g \in H\}$, and let $\mathcal{P} = P^G$. Then $(\Gamma, \mathcal{P})$ is a G-transitive decomposition. The graph $[P]$ induced by P has vertices all k-sets not containing i where i is the unique point not in $v \cup w$ and two vertices are adjacent if and only if they are disjoint. Hence $[P]$ consists of $\binom{2k}{k}/2$ disjoint edges.

Example 4.7. Let $\Gamma = \mathsf{H}(d, n) = K_n \Box K_n \Box \cdots \Box K_n = K_n^{\Box d}$ and $G = S_n \operatorname{wr} S_d$. Then Γ can be decomposed into edge disjoint maximal cliques K_n, giving a G-arc-symmetrical decomposition as follows: vertices $v = (1, \ldots, 1)$ and $w = (2, 1. \ldots, 1)$ are adjacent and $G_{\{v,w\}} = (S_{n-2} \cdot 2) \times (S_{n-1} \operatorname{wr} S_{d-1}) < H := S_n \times (S_{n-1} \operatorname{wr} S_{d-1})$. Let $P = \{v, w\}^H$. Then $[P] \cong K_n$ and $\mathcal{P} = P^G$ is a G-arc-symmetrical decomposition.

4.2 *Link with linear spaces*

We now consider decomposing complete graphs into complete subgraphs.

A *linear space* $(\Omega, \mathcal{L})$ is an incidence geometry with point set Ω and line set $\mathcal{L}$ where each line is a subset of Ω, $|\mathcal{L}| \geq 2$, and each pair of points lies on exactly one line. For a linear space $(\Omega, \mathcal{L})$

with $n = |\Omega|$, let $\Gamma \cong K_n$ be its point graph, that is, the complete graph with vertex set Ω, and let $\mathcal{P}$ be the set of subgraphs of Γ such that $P \in \mathcal{P}$ if and only if P is the complete graph whose vertex set consists of all points on some line. Then $(\Gamma, \mathcal{P})$ is a decomposition of Γ. Moreover,

(i) $(\Omega, \mathcal{L})$ is G-line transitive if and only if $(\Gamma, \mathcal{P})$ is G-transitive. See [26].
(ii) $(\Omega, \mathcal{L})$ is G-flag-transitive if and only if $(\Gamma, \mathcal{P})$ is G-vertex-symmetrical.
(iii) G acts 2-transitively on the points of $(\Omega, \mathcal{L})$ if and only if $(\Gamma, \mathcal{P})$ is G-arc-symmetrical.

The linear spaces in (iii), with a group of automorphisms acting 2-transitively on points, were determined by Kantor [19] while all flag-transitive linear spaces for which G is not a 1-dimensional affine group were classified in [5] and subsequent papers. Thus vertex-symmetrical decompositions of complete graphs with complete divisors are essentially known. Moreover, the arc-symmetrical decompositions of complete graphs with arbitrary divisors were characterised in [31], extending the classification in [6] for the case where the divisors are 1-factors. Sibley's characterisation has been made more explicit both in [20] for homogeneous factorisations of K_n, and in [1] to provide input decompositions for a series of general decomposition constructions for products and cartesian products of complete graphs.

4.3 *Vertex-symmetrical decompositions*

Now we consider vertex-symmetrical decompositions of vertex-transitive graphs. Let Γ be a G-vertex-transitive graph. If Γ is disconnected, then the set of connected components forms a G-vertex-symmetrical decomposition of Γ. Moreover, since the connected components are isomorphic (because Γ is G-vertex-transitive), each G-vertex-symmetrical decomposition $(\Gamma_0, \mathcal{P}_0)$ of a connected component of Γ, where $G_0 = G_{\Gamma_0}$, leads to the G-vertex-symmetrical decomposition $(\Gamma, \mathcal{P}_0^G)$ of Γ. The next example illustrates that not all vertex-symmetrical decompositions of disconnected graphs arise in this way. Nevertheless we will confine our further discussion to the case where Γ is connected.

Example 4.8. Let Γ be the vertex disjoint union of the two 3-cycles $\{1,2\}, \{2,3\}, \{3,1\}$ and $\{4,5\}, \{5,6\}, \{6,4\}$, and let $G = S_3 \times S_2 \leqslant \mathsf{Aut}(\Gamma)$ acting transitively on $V\Gamma$. Let $P = \{\{1,2\}, \{4,5\}\}$ and $\mathcal{P} = P^G$. Then $G_P = \langle (1,2)(4,5) \rangle \times S_2$ and so $(\Gamma, \mathcal{P})$ is a G-vertex-symmetrical decomposition.

If Γ is G-edge-transitive, then a G-vertex-symmetrical decomposition of Γ is also a G-edge-symmetrical decomposition and hence arises from Construction 4.2. We give below a general construction for G-vertex-symmetrical decompositions of connected graphs when G is not edge-transitive.

Construction 4.9. Let Γ be a connected G-vertex-transitive graph with G intransitive on edges, and let $E_1, E_2, \ldots, E_r$ be the orbits of G acting on the edge set $E\Gamma$. Then each induced subgraph $[E_i]$ is a G-edge-transitive spanning subgraph of Γ. Assume that each $[E_i]$ has a G-vertex-symmetrical decomposition $\mathcal{P}_i = \{P_{i1}, P_{i2}, \ldots, P_{ik}\}$ such that for each $i, j \in \{1, \ldots, r\}$ and $s \in \{1, \ldots, k\}$ we have $VP_{is} = VP_{js}$. Let $P_j = P_{1j} \cup P_{2j} \cup \cdots \cup P_{rj}$, and $\mathcal{P} = \{P_1, P_2, \ldots, P_k\}$. Note that for each j, $VP_j = VP_{1j}$ and so $G_{P_j} = G_{P_{1j}}$ is transitive on VP_j. Hence $(\Gamma, \mathcal{P})$ is a G-vertex-symmetrical decomposition.

Lemma 4.10. *Let $(\Gamma, \mathcal{P})$ be a G-vertex-symmetrical decomposition of a connected graph Γ with G intransitive on edges. Then $(\Gamma, \mathcal{P})$ can be obtained from Construction 4.9.*

Proof. Let $E_1, \ldots, E_r$ be the orbits of G on $E\Gamma$. Since G is vertex-transitive, each $[E_i]$ is a spanning subgraph of Γ. Let $\mathcal{P} = \{P_1, \ldots, P_k\}$ and for each $i \in \{1, \ldots, r\}$ and $s \in \{1, \ldots, k\}$ let $Q_{is} = E_i \cap P_s$. Then for $i \in \{1, \ldots, r\}$, $\mathcal{Q}_i = \{Q_{is} \mid s \in \{1, \ldots, k\}\}$ is a G-transitive decomposition of $[E_i]$. Moreover, for each $s \in \{1, \ldots, k\}$, $G_{Q_{is}} = G_{P_s}$. Since $(\Gamma, \mathcal{P})$ is G-vertex-symmetrical, for each $s \in \{1, \dots, k\}$, G_{P_s} is transitive on VP_s. It follows, that for each $i \in \{1, \dots, r\}$, $VQ_{is} = VP_s$ and $G_{Q_{is}}$ is transitive on VQ_{is}. Thus $([E_i], \mathcal{Q}_i)$ is a G-vertex-symmetrical decomposition. Hence $\mathcal{P}$ may be obtained from Construction 4.9. □

A natural problem in this area is the following.

Problem 4.11. Characterise the vertex-transitive graphs which arise as vertex-symmetrical divisors of a complete graph.

5 TRANSITIVE FACTORISATIONS

Let $(\Gamma, \mathcal{P})$ be a factorisation with $\mathcal{P} = \{P_1, \dots, P_k\}$. For $v \in V\Gamma$ and each $i \in \{1, \dots, k\}$ we can define $P_i(v) = \{w \in \Gamma(v) \mid \{v, w\} \in \mathcal{P}\}$ and $\mathcal{P}(v) = \{P_1(v), \dots, P_k(v)\}$. Since $\mathcal{P}$ is a partition of $E\Gamma$, it follows that $\mathcal{P}(v)$ is a partition of $\Gamma(v)$ and as each P_i is a spanning subgraph of Γ, each $P_i(v)$ is nonempty. If $G \leqslant \mathsf{Aut}(\Gamma)$ preserves $\mathcal{P}$ then G_v preserves $\mathcal{P}(v)$.

This local correspondence allows us to see that transitive factorisations of graphs are naturally connected to group factorisations. This fact can be used very effectively to study transitive factorisations for various classes of graphs or classes of groups.

Lemma 5.1. *Let Γ be a G-arc-transitive graph, and let $(\Gamma, \mathcal{P})$ be a G-transitive factorisation of Γ. Then for $P \in \mathcal{P}$ and $v \in V\Gamma$, $G = G_v G_P$, G_P is vertex-transitive on Γ and G_v is transitive on $\mathcal{P}$.*

Proof. Since G_v acts transitively on $\Gamma(v)$, it follows that G_v is transitive on $\mathcal{P}(v)$ and hence also on $\mathcal{P}$. Thus by Lemma 2.1, $G = G_v G_P$ and so again by Lemma 2.1, G_P acts transitively on $V\Gamma$. □

The following lemma follows immediately from Lemma 5.1 and implies that G_P has index at most a subdegree of G.

Lemma 5.2. *If $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical factorisation and $H = G_P$ for some $P \in \mathcal{P}$, then $|G : H| = |G_v : H_v|$ divides the valency of Γ.*

We now give two general constructions and show that all symmetrical factorisations arise from them.

Construction 5.3. (Edge-symmetrical and arc-symmetrical factorisations) Let $\Gamma = (V, E)$ be a G-edge-transitive graph. Assume that there is a subgroup H containing $G_{\{v,w\}}$ for some edge $\{v, w\}$, such that either $G = HG_v = HG_w$, or $HG_v = HG_w$ is an index two subgroup of G. Let $P = \{v, w\}^H$, and let $\mathcal{P} = P^G$. If $G = HG_v$ and Γ is G-vertex-transitive, then by Lemma 2.1, Γ is H-vertex-transitive and so $[P]$ is a spanning subgraph containing the edge $\{v, w\}$. On the other hand, if $G = HG_v = HG_w$ and Γ is not G-vertex-transitive, or if $HG_v = HG_w$ is an index two subgroup of G, then Γ is bipartite and H is transitive on each bipartite half. Again $[P]$ is a spanning subgraph. In all these cases, since $G_{\{v,w\}} < H < G$, $\mathcal{P}$ is a system of imprimitivity for G on E and so $(\Gamma, \mathcal{P})$ is a G-edge-symmetrical factorisation. Moreover, if Γ is G-arc-transitive, then $G_{\{v,w\}}$ contains an element interchanging v and w, and hence so does H. Thus H is arc-transitive on $[P]$ and so $(\Gamma, \mathcal{P})$ is a G-arc-symmetrical factorisation.

The following example shows that edge-symmetrical factorisations exist with $G = HG_v$ and G either vertex-transitive or vertex-intransitive, and also with $HG_v = HG_w$ an index two subgroup of G. Note that for arc-symmetrical factorisations only the case $G = HG_v$ and G-vertex-transitive occurs as Γ is both G- and H-vertex-transitive in this case.

Example 5.4. Let $\Gamma = C_6$ with vertices labelled by the elements of $\mathbb{Z}_6$ and x adjacent to $x \pm 1$ (mod 6), and let $h = (0,1,2,3,4,5)$, $g = (1,5)(2,4) \in \mathsf{Aut}(\Gamma)$. Let $v = 0$ and $w = 1$ so that $\{v,w\} \in E\Gamma$.

(1) Let $G = \langle g,h\rangle = \mathsf{Aut}(\Gamma) \cong D_{12}$. Then $G_v = \langle g\rangle$ and $G_{\{v,w\}} = \langle (0,1)(2,5)(3,4)\rangle \cong C_2$. Let $H = \langle G_{\{v,w\}}, h^2\rangle \cong D_6$. Then $G = G_vH$ and so we can use Construction 5.3 to obtain a G-edge-symmetrical factorisation. In particular, $P = \{v,w\}^H = \{\{0,1\},\{2,3\},\{4,5\}\}$ and $\mathcal{P} = P^G$. Moreover, $(\Gamma,\mathcal{P})$ is G-arc-symmetrical.
(2) Let $G = \langle h\rangle \cong C_6$. Then $G_v = G_w = 1 = G_{\{v,w\}}$. Let $H = \langle h^2\rangle \cong C_3$. Then $HG_v = HG_w$ has index two in G and so we can use Construction 5.3 to obtain a G-edge-symmetrical factorisation. We again have $P = \{v,w\}^H = \{\{0,1\},\{2,3\},\{4,5\}\}$.
(3) Let $G = \langle h^2, g\rangle \cong D_6$ which is vertex-intransitive. Then $G_v = \langle g\rangle$ and $G_{\{v,w\}} = 1$. Let $H = \langle h^2\rangle$. Then $G = G_vH$ and so we can again use Construction 5.3 to obtain a G-edge-symmetrical factorisation. Once again $P = \{v,w\}^H = \{\{0,1\},\{2,3\},\{4,5\}\}$.

Lemma 5.5. *Let $(\Gamma,\mathcal{P})$ be a G-edge-symmetrical factorisation. Then $(\Gamma,\mathcal{P})$ arises from Construction 5.3 using $H = G_P$ for $P \in \mathcal{P}$.*

Proof. By Lemma 4.1, $\mathcal{P}$ is a block system of the G-action on E. Thus $H = G_P$ contains the edge stabiliser $G_{\{v,w\}}$ and $P = \{v,w\}^H$. Since H is transitive on the edges of the factor P, either Γ is H-vertex-transitive, or Γ is bipartite and H has two orbits on $V\Gamma$, these being the two bipartite halves. It follows from Lemma 2.1 that in the first case $G = HG_v$. In the second case, the stabiliser G^+ in G of each bipartite half has index at most two in G and Lemma 2.1 implies that $G^+ = HG_v = HG_w$. Thus $(\Gamma,\mathcal{P})$ arises from Construction 5.3 □

Note that if $(\Gamma,\mathcal{P})$ is a G-arc-symmetrical factorisation then it is also G-edge-symmetrical and hence by Lemma 5.5 arises from Construction 5.3.

If $(\Gamma,\mathcal{P})$ is a G-vertex-symmetrical factorisation with G transitive on $E\Gamma$, then $(\Gamma,\mathcal{P})$ is an edge-symmetrical factorisation. We have the following general construction in the edge-intransitive case.

Construction 5.6. (Vertex-symmetrical factorisations) Let $\Gamma = (V,E)$ be a G-vertex-transitive graph and let $E_1,\ldots,E_r$ be the G-orbits on E. Suppose there is a subgroup H such that $G = HG_v$ for some vertex v and for each orbit E_i of G on E there exists $\{v_i,w_i\} \in E_i$ such that $G_{\{v_i,w_i\}} \leqslant H$. Let $P = \{\{v_1,w_1\},\ldots,\{v_r,w_r\}\}^H$ and $\mathcal{P} = P^G$. Since $G = HG_v$, Γ is H-vertex-transitive and so $[P]$ is a spanning subgraph containing each edge $\{v_i,w_i\}$. Also, since $G_{\{v_i,w_i\}} < H < G$ for each i, the partition $\mathcal{P}_i = \{P_j \cap E_i \mid P_j \in \mathcal{P}\}$ is a system of imprimitivity for G on E_i. Moreover, the action of G on $\mathcal{P}_i$ is equivalent to the action of G on the set of right cosets of H and hence $G^{\mathcal{P}_i} \cong G^{\mathcal{P}_j}$ for all $i \neq j$. Thus $\mathcal{P}$ is indeed a factorisation of Γ and so $(\Gamma,\mathcal{P})$ is a G-vertex-symmetrical factorisation.

Example 5.7. Let Γ be the graph with vertices labelled by the elements of $\mathbb{Z}_8$ and x adjacent to $x \pm 1, x \pm 3$ (mod 8). Let $G = D_{16} \leqslant \mathsf{Aut}(\Gamma)$. Then G has two orbits E_1, E_2 on the set of edges of Γ, with E_1 being the 8-cycle with adjacency $x \sim x \pm 1$ (mod 8) and E_2 the 8-cycle with adjacency $x \sim x \pm 3$ (mod 8). Now $\{0,1\} \in E_1$ and $\{3,6\} \in E_2$. Moreover, $G_{\{0,1\}} = G_{\{3,6\}} = \langle (0,1)(2,7)(3,6)(4,5)\rangle$. Now $G = G_0H$ where $H = \langle (0,1)(2,7)(3,6)(4,5), (0,2,4,6)(1,3,5,7)\rangle$ and H contains $G_{\{0,1\}} = G_{\{3,6\}}$. Thus we can use Construction 5.6 to find a G-vertex-symmetrical factorisation. The part $\mathcal{P} = \{\{0,1\},\{3,6\}\}^H$ gives $[P] = 2C_4$ with components $(0,1,4,5)$ and $(2,3,6,7)$.

Lemma 5.8. *Let $(\Gamma,\mathcal{P})$ be a G-vertex-symmetrical factorisation. Then $(\Gamma,\mathcal{P})$ arises from Construction 5.6 using $H = G_P$ for $P \in \mathcal{P}$.*

Proof. Suppose that $(\Gamma, \mathcal{P})$ is a G-vertex-symmetrical factorisation and let $P \in \mathcal{P}$ contain the edge $\{v, w\}$. Then the subgraph P is spanning, and $H = G_P$ is transitive on V. Hence $G = HG_v$. Let $E_1, \ldots, E_r$ be the G-orbits on E. For $i \in \{1, \ldots, r\}$, we have $\mathcal{P} \cap E_i := \{P_j \cap E_i \mid P_j \in \mathcal{P}\}$ is a G-edge-symmetrical factorisation of the induced subgraph $[E_i]$. By Lemma 4.1, $P \cap E_i$ is a block of imprimitivity for G acting on E_i, and so the block stabiliser $G_{P \cap E_i} = H$ properly contains $G_{\{v_i, w_i\}}$ for some edge $\{v_i, w_i\} \in E_i$. Moreover, $P \cap E_i = \{v_i, w_i\}^H$ and $P = \{\{v_1, w_1\}, \ldots, \{v_r, w_r\}\}$. Hence $(\Gamma, \mathcal{P})$ is as obtained by Construction 5.6. □

5.1 *A link between transitive covers and homogeneous factorisations*

There is an interesting situation that arises for G-transitive covers $(\Gamma, \mathcal{P})$ for vertex-quasiprimitive groups G. These are permutation groups G for which all nontrivial normal subgroups are vertex-transitive. We propose the general study of G-transitive uniform covers $(\Gamma, \mathcal{P})$ where G is arc-transitive and vertex-quasiprimitive.

Construction 5.9. For a cover $(\Gamma, \mathcal{P})$ define the following family $\mathcal{Q}(\mathcal{P})$ of sets as follows: For each $e \in E\Gamma$, let $\mathcal{P}_e = \{P \in \mathcal{P} \mid e \in P\}$ and let $Q_e = \cap_{P \in \mathcal{P}_e} P$. Then define $\mathcal{Q}(\mathcal{P}) = \{Q_e \mid e \in E\Gamma\}$.

Lemma 5.10. *If $(\Gamma, \mathcal{P})$ is a G-transitive λ-uniform cover such that the kernel $N = G_{(\mathcal{P})}$ is vertex-transitive and Γ is G-edge-transitive, then $(\Gamma, \mathcal{Q}(\mathcal{P}))$ is a (G, N)-homogeneous factorisation.*

(Homogeneous factorisations were defined at the end of Section 1.)

Proof. Let $\mathcal{Q} = \mathcal{Q}(\mathcal{P})$, and let $e \in E\Gamma$. Since $e \in Q_e$ and N fixes Q_e setwise, it follows that Q_e is a spanning subgraph. Now G preserves $\mathcal{Q}$ and since G is edge-transitive, it follows that G acts transitively on $\mathcal{Q}$. Moreover, for each $e \in E\Gamma$, there is a unique part of $\mathcal{Q}$, namely Q_e, which contains e. Hence $(\Gamma, \mathcal{Q})$ is a (G, N)-homogeneous factorisation. □

This link can sometimes occur rather naturally and we demonstrate this phenomenon in the next lemma.

Lemma 5.11. *Let $(\Gamma, \mathcal{P})$ be a (G, M)-homogeneous factorisation such that G is 2-transitive on $\mathcal{P}$. Let $\mathcal{R} = \{P_i \cup P_j \mid i \neq j, P_i, P_j \in \mathcal{P}\}$. Then $(\Gamma, \mathcal{R})$ is a G-transitive $(|\mathcal{P}| - 1)$-uniform cover. Moreover, the homogeneous factorisation obtained from $(\Gamma, \mathcal{R})$ using Construction 5.9 is $(\Gamma, \mathcal{P})$.*

Proof. Since G is 2-transitive on $\mathcal{P}$, it acts transitively on $\mathcal{R}$. Moreover, as each edge lies in a unique element of $\mathcal{P}$, it lies in precisely $|\mathcal{P}| - 1$ elements of $\mathcal{R}$. Thus $(\Gamma, \mathcal{R})$ is a G-transitive $(|\mathcal{P}| - 1)$-uniform cover. Given an edge e of Γ, if P is the unique part of $\mathcal{P}$ containing e, then P is the intersection of all the parts of $\mathcal{R}$ containing e. Hence $(\Gamma, \mathcal{P})$ is the homogeneous factorisation obtained from $(\Gamma, \mathcal{R})$ using Construction 5.9. □

An explicit example of a homogeneous factorisation satisfying the conditions of Lemma 5.11 is $G = \mathrm{AGL}(d, q)$, $\Gamma = K_{q^d}$, with $\mathcal{P}$ the partition of edges into parallel classes. Application of Construction 5.9 arises most naturally when the group G involved is quasiprimitive on vertices.

Lemma 5.12. *Let $(\Gamma, \mathcal{P})$ be a G-transitive uniform cover of a G-edge-transitive, G-vertex-quasiprimitive graph Γ. Then either*

(1) *G acts faithfully on $\mathcal{P}$, or*
(2) *Construction 5.9 yields a (G, N)-homogeneous factorisation $(\Gamma, \mathcal{Q})$ with $N = G_{(\mathcal{P})}$.*

Proof. Let N be the kernel of the action of G on $\mathcal{P}$. If $N = 1$ then G acts faithfully on $\mathcal{P}$ and we have case (1). On the other hand, if $N \neq 1$, since Γ is G-vertex-quasiprimitive, N is transitive on $V\Gamma$. Hence Construction 5.9 yields a (G, N)-homogeneous factorisation $(\Gamma, \mathcal{Q})$. □

6 QUOTIENTS

In this final section we discuss the behaviour of covers and decompositions when we pass to a quotient graph. Let Γ be a G-arc-transitive connected graph and $\mathcal{B}$ a G-invariant partition of $V\Gamma$. The *quotient graph* $\Gamma_{\mathcal{B}}$ is the graph with vertex set $\mathcal{B}$ such that two blocks B_1, B_2 are adjacent if and only if there exist $v \in B_1$ and $w \in B_2$ such that v and w are adjacent in Γ. The quotient $\Gamma_{\mathcal{B}}$ has no loops and is connected, and G acts arc-transitively (see [29]). If the G-invariant partition $\mathcal{B}$ is the set of orbits of a normal subgroup N of G then we denote $\Gamma_{\mathcal{B}}$ by Γ_N and $\mathcal{P}_{\mathcal{B}}$ by $\mathcal{P}_N$.

We say that Γ *covers* the quotient graph $\Gamma_{\mathcal{B}}$ if the subgraph of Γ induced between two adjacent blocks is a perfect matching, that is, given two adjacent blocks B_1, B_2, for all $v \in B_1$, we have $|\Gamma(v) \cap B_2| = 1$. This is an unfortunate re-use of the term 'cover'. However, both uses of this word are standard in the graph theory literature. The context should make it clear which one is intended.

Given a cover $\mathcal{P}$ of Γ (as in Section 1), for each $P \in \mathcal{P}$ let $P_{\mathcal{B}}$ be the set of all arcs (B, C) of $\Gamma_{\mathcal{B}}$ such that there exists $u \in B$ and $v \in C$ with $(u, v) \in P$. This allows us to define $\mathcal{P}_{\mathcal{B}} = \{P_{\mathcal{B}} \mid P \in \mathcal{P}\}$. If the G-invariant partition $\mathcal{B}$ is the set of orbits of a normal subgroup N of G then we denote $\Gamma_{\mathcal{B}}$ by Γ_N and $\mathcal{P}_{\mathcal{B}}$ by $\mathcal{P}_N$.

The following lemma records properties of $(\Gamma, \mathcal{P})$ that are inherited by $(\Gamma_{\mathcal{B}}, \mathcal{P}_{\mathcal{B}})$. Case (c) involves the condition that Γ covers it quotient graph Γ_N, a condition that always holds if Γ is G-locally primitive, see our comments after Theorem 6.2 below.

Lemma 6.1. *Let Γ be a G-arc-transitive connected graph and let $\mathcal{B}$ be a G-invariant partition of $V\Gamma$.*

(*a*) *If $\mathcal{P}$ is a cover of Γ then $\mathcal{P}_{\mathcal{B}}$ is a cover of $\Gamma_{\mathcal{B}}$.*
(*b*) *If $(\Gamma, \mathcal{P})$ is a G-transitive λ-uniform cover, then $(\Gamma_{\mathcal{B}}, \mathcal{P}_{\mathcal{B}})$ is a G-transitive μ-uniform cover for some $\mu \geq \lambda$.*
(*c*) *Let N be a normal subgroup of G which acts trivially on $\mathcal{P}$ and has at least three orbits on vertices, and suppose that Γ covers Γ_N. Then $(\Gamma_N, \mathcal{P}_N)$ is a (G/N)-transitive λ-uniform cover, and for each $P \in \mathcal{P}$, P covers P_N.*

Proof.

(a) Let (B, C) be an arc of $\Gamma_{\mathcal{B}}$. As noted above there are no loops in $\Gamma_{\mathcal{B}}$, and so there exists $(u, v) \in A\Gamma$ such that $u \in B$ and $v \in C$. Since $\mathcal{P}$ is a cover of Γ, there exists $P \in \mathcal{P}$ such that $(u, v) \in P$. Hence $(B, C) \in P_{\mathcal{B}}$ and so $\mathcal{P}_{\mathcal{B}}$ is a cover of $\Gamma_{\mathcal{B}}$.
(b) As noted above G acts arc-transitively on $\Gamma_{\mathcal{B}}$. Since $\mathcal{P}$ is G-invariant it follows from the definition of $\mathcal{P}_{\mathcal{B}}$ that $\mathcal{P}_{\mathcal{B}}$ is also G-invariant, and since G is transitive on $\mathcal{P}$ it is also transitive on $\mathcal{P}_{\mathcal{B}}$. Thus by part (a), $(\Gamma_{\mathcal{B}}, \mathcal{P}_{\mathcal{B}})$ is a G-transitive μ-uniform cover for some μ. Since an arc (u, v) with $u \in B$ and $v \in C$ is contained in λ parts of $\mathcal{P}$, it follows that $\mu \geq \lambda$.
(c) Let (B, C) be an arc of Γ_N. Since Γ is a cover of Γ_N, the subgraph induced between B and C is a complete matching and N acts transitively on the set of arcs from B to C. Thus if $P_1, \ldots, P_\lambda$ are the λ parts of $\mathcal{P}$ containing the arc (u, v) with $u \in B$ and $v \in C$, then all arcs from B to C are contained in each $P_1, \ldots, P_\lambda$. Thus (B, C) is contained in precisely λ parts of $\mathcal{P}_N$ and so $(\Gamma_N, \mathcal{P}_N)$ is a (G/N)-transitive λ-uniform cover. Moreover, if $P \in \mathcal{P}$ contains an arc joining some (B, C) then since N acts transitively on B and fixes P, for each $b \in B$, there exists $c \in C$ such that $(b, c) \in P$. Since Γ covers Γ_N, c is unique and hence P covers P_N. □

Let $(\Gamma, \mathcal{P})$ be a G-transitive factorisation and let M be the kernel of the action of G on $\mathcal{P}$. Recall that if M is vertex-transitive, then $(\Gamma, \mathcal{P})$ is a (G, M)-homogeneous factorisation. If Γ is bipartite and both G and M fix the two parts of the bipartition and act transitively on both, then $(\Gamma, \mathcal{P})$ is called a *(G, M)-bihomogeneous factorisation*. In either of these cases if we replace $\mathcal{P}$ by a G-invariant partition of $E\Gamma$ refined by $\mathcal{P}$ the kernel will also be transitive on $V\Gamma$, or in the second case will have at most two vertex-orbits. We have a useful result about quotients for G-transitive decompositions $(\Gamma, \mathcal{P})$ in the case where G is primitive on $\mathcal{P}$, a property that may be obtained by replacing $\mathcal{P}$ with a maximal invariant partition refined by $\mathcal{P}$. For a bipartite graph Γ which is G-vertex-transitive, we denote by G^+ the index two subgroup of G which fixes setwise each of the two bipartite halves.

We have the following theorem.

Theorem 6.2. *Let $(\Gamma, \mathcal{P})$ be a G-transitive decomposition of the G-arc-transitive connected graph Γ. Suppose that G acts primitively on $\mathcal{P}$ and let N be the kernel of the action of G on $\mathcal{P}$. Then one of the following holds.*

(1) $(\Gamma, \mathcal{P})$ *is a (G,N)-homogeneous factorisation.*
(2) $(\Gamma, \mathcal{P})$ *is a (G^+,N)-bihomogeneous factorisation.*
(3) $(\Gamma_N, \mathcal{P}_N)$ *is a (G/N)-transitive decomposition with G/N faithful on $\mathcal{P}_N$.*
(4) *N has at least three vertex orbits and Γ does not cover Γ_N.*

Proof. If N is vertex-transitive then we are clearly in the first case. If N has two orbits on $V\Gamma$, then Γ is bipartite with the two N-orbits being the two parts of the bipartition. Since $G^{\mathcal{P}}$ is primitive, it follows that G^+ acts transitively on $\mathcal{P}$ and so $(\Gamma, \mathcal{P})$ is a (G^+,N)-bihomogeneous factorisation.

Suppose now that N has at least three orbits on vertices. If Γ is a cover of Γ_N, then Lemma 6.1(c) implies that $(\Gamma_N, \mathcal{P}_N)$ is a (G/N)-transitive decomposition. Since N is the kernel of the action of G on $\mathcal{P}$, G/N is faithful on $\mathcal{P}_N$. □

When Γ is G-locally primitive, [29] implies that Γ is a cover of Γ_N, so case (4) of Theorem 6.2 does not arise in this case. Thus Theorem 6.2 suggests that for G-locally primitive graphs important G-transitive decompositions to study are those for which G acts faithfully on the decomposition.

Problem 6.3. Study G-transitive decompositions of families of G-locally primitive graphs.

REFERENCES

[1] J. Bamberg, G. Pearce and C. E. Praeger, Transitive decompositions of graph products: rank 3 product action type, J. Group Theory, 11 (2008), 185–228.

[2] A. Bonisoli, M. Buratti and G. Mazzuoccolo, Doubly transitive 2-factorisations, *J. Combin. Des.* 15 (2007), 120–132.

[3] J. Bosák, Decompositions of Graphs, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1990.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.* 24 3/4 (1997), 235–265. Also see the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma/.

[5] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, J. Saxl, Linear spaces with flag-transitive automorphism groups. *Geom. Dedicata* 36 (1990), 89–94.

[6] P. J. Cameron and G. Korchmáros, One-factorizations of complete graphs with a doubly transitive automorphism group. *Bull. London Math. Soc.* 25 (1993), 1–6.

[7] P. J. Cameron, G. R. Omidi and B. Tayeh-Rezaie, 3-Designs from $\mathrm{PGL}(2,q)$, Electron. *J. Combin.* 13 (2006) #R50.

[8] A. Devillers, M. Giudici, C. H. Li and C. E. Praeger, Primitive decompositions of Johnson graphs, *J. Combin. Theory, Series A*, to appear.

[9] J. D. Dixon and B. Mortimer, Permutation groups. Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996.

[10] X. G. Fang, C. H. Li and J. Wang, On transitive 1-factorizations of arc-transitive graphs, *J. Combin. Theory Series A*, 114 (2007), 692–703.

[11] F. Harary, R. W. Robinson and N. C. Wormald, Isomorphic factorisations. I. Complete graphs, *Trans. Amer. Math. Soc.* 242 (1978), pp. 243–260.

[12] F. Harary and R. W. Robinson, Isomorphic factorisations X: unsolved problems, *J. Graph Theory* 9 (1985), pp. 67–86.

[13] K. Heinrich, Graph decompositions and designs, in: The CRC Handbook of Combinatorial Designs, Charles J. Colbourn and Jeffrey H. Dinitz, (Editors), CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1996, pp. 361–366.

[14] M. Giudici, C. H. Li, P. Potočnik and C. E. Praeger, Homogeneous factorisations of graphs and digraphs, *European J. Combin*. 27 (2006), 11–37.

[15] M. Giudici, C. H. Li, P. Potočnik and C. E. Praeger, Homogeneous factorisations of complete multipartite graphs, *Discrete Math*. 307 (2007), 415–431.

[16] M. Giudici, C. H. Li, P. Potočnik and C. E. Praeger, Homogeneous factorisations of graph products, to appear in *Discrete Math*.

[17] C. Greenhill, The cycle double cover conjecture, *Austral. Math. Soc. Gaz*. 32 (2005), 169–172.

[18] F. Jaeger, A survey on the cycle double cover conjecture, in: Cycles in graphs, B. Alspach and C. D. Godsil (Editors) Annals of Discrete Math. 27 North-Holland Amsterdam 1985, 1–12.

[19] W. M. Kantor, Homogeneous designs and geometric lattices. *J. Comb. Theory* (A) 38 (1985), 66–74.

[20] C. H. Li, T. K. Lim and C. E. Praeger, Homogeneous factorisations of complete graphs with edge-transitive factors, *J. Alg. Combin.*, doi: 10.1007/s10801-008-0127-2. Published on-line February 27, 2008.

[21] C. H. Li and C. E. Praeger, On partitioning the orbitals of a transitive permutation group, *Trans. Amer. Math. Soc*. 355 (2003), 637–653.

[22] C. H. Li, C. E. Praeger, A. Venkatesh, and S. Zhou, Finite locally-quasiprimitive graphs, *Discrete Math.* 246 (2002), 197–218.

[23] C. H. Li and A. Seress, Symmetrical path-cycle covers of a graph and polygonal graphs, *J. Combin. Theory Series* A 114 (2007), 35–51.

[24] T. K. Lim, Edge-transitive homogeneous factorisations of complete graphs, Ph.D. Thesis, The University of Western Australia, 2003.

[25] D. K. Maslen, M. E. Orrison and D. N. Rockmore, Computing isotypic projections with the Lanczos iteration, SIAM *J. Matrix Anal. Appl*. 25 (2004), 784–803.

[26] G. Pearce, Transitive decompositions of graphs and their links with geometry and origami, submitted.

[27] M. Perkel, Near-polygonal graphs. *Ars Combin*. 26A (1988), 149–170.

[28] M. Perkel and C. E. Praeger, Polygonal graphs: new families and an approach to their analysis, *Congr. Numer*. 124 (1997), 161–173.

[29] C. E. Praeger, Imprimitive symmetric graphs, *Ars Combin*. 19A (1985), 149–163.

[30] R. W. Robinson, Isomorphic factorisations. VI. Automorphisms. in: Combinatorial mathematics, VI (Proc. Sixth Austral. Conf., Univ. New England, Armidale, 1978), pp. 127–136, Lecture Notes in Math., 748, Springer, Berlin, 1979.

[31] T. Sibley, On classifying finite edge colored graphs with two transitive automorphism groups, *J. Combin. Theory Series* B 90 (2004), 121–138.

[32] R. M. Wilson, Decompositions of complete graphs into subgraphs isomorphic to a given graph, *Proc. 5th British Comb. Conf.* (1975), 647–659.

[33] B. Zelinka, The decomposition of a complete graph according to a given group, *Mat. Časopis Sloven. Akad. Vied*. 17 (1967), 234–239.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Complete bipartite maps, factorisable groups and generalised Fermat curves

Gareth A. Jones
School of Mathematics, University of Southampton, Southampton, UK

1 INTRODUCTION

This paper is based on a talk given at the Com^{2}MaC Conference on Applications of Group Theory to Combinatorics, July 2007. It is a brief survey of recent progress on the combinatorial problem of classifying the orientably regular embeddings of complete bipartite graphs. The motivation for this problem comes from two main areas, topological graph theory and arithmetic algebraic geometry, while the techniques required to solve it come from a third area, finite group theory—specifically the theories of factorisable groups and of finite solvable groups.

The first part of this paper is mainly combinatorial and group-theoretic, discussing the classification problem and the methods used to solve it. Much of this work was done by the author in collaboration with Shao-Fei Du, Jin Ho Kwak, Roman Nedela and Martin Škoviera. I will also briefly mention an alternative approach to this problem, developed by Jin Ho Kwak and Young Soo Kwon, and its connection with skew-morphisms, introduced by Robert Jajcay and Jozef Širáň. The second part of this paper is rather more wide-ranging, involving the links between this problem and other topics such as Riemann surfaces, algebraic geometry and Galois theory. Again, much of this was collaborative work, this time involving Antoine Coste, Manfred Streit and Jürgen Wolfart. I am grateful to all these colleagues for their valuable input over many years, and also to Com^{2}MaC for the invitation and the financial support which enabled this talk to be given.

2 MOTIVATION FROM TOPOLOGICAL GRAPH THEORY

One of the main general problems of topological graph theory is to find all the orientably regular embeddings of a given class of arc-transitive finite graphs $\mathcal{G}$. These are maps $\mathcal{M}$ on compact orientable surfaces $\mathcal{S}$, such that the faces (connected components of $\mathcal{S}\backslash\mathcal{G}$) are simply connected; $\mathcal{M}$ is *orientably regular* (often abbreviated to *regular*) if the group $\mathrm{Aut}^+\mathcal{M}$ of orientation-preserving automorphisms of $\mathcal{M}$ acts transitively on the arcs (directed edges) of $\mathcal{G}$. One can generalise this problem by considering orientation-reversing automorphisms or non-orientable surfaces (see §13 and [1, 2]), but for simplicity we will generally avoid these cases here.

This problem has been solved for several classes of graphs, such as complete graphs K_n by James and Jones [3], n-cubes Q_n for odd n by Du, Kwak and Nedela [4], and Johnson graphs $J(n,m)$ by Jones [5], but there many interesting cases still open, such as Q_n for even n, shown by Kwon [6] to be much harder than the case where n is odd.

3 COMPLETE BIPARTITE GRAPHS

In this paper we take $\mathcal{G}$ to be the *complete bipartite graph $K_{n,n}$*: this has $2n$ vertices, partitioned into two sets of size n, coloured black and white respectively, and it has n^2 edges, one between each pair of black and white vertices. The automorphism group $\mathrm{Aut}\,\mathcal{G}$ is isomorphic to the wreath product

$S_n \wr S_2$, an extension of a normal subgroup $S_n \times S_n$ (with the factors independently permuting the black and the white vertices) by a complement S_2 transposing these two sets. This group acts transitively on arcs of the graph, so it is conceivable that the graph has orientably regular embeddings. (This is not always the case: each complete graph K_n has an arc-transitive automorphism group S_n, but Biggs [7] showed that only those for which n is a prime power have orientably regular embeddings.)

By contrast with the complete graphs, every graph $K_{n,n}$ has at least one orientably regular embedding. This is the *standard embedding* of $K_{n,n}$, described by Biggs and White in [8, §5.6.7] as a Cayley map for the group $\mathbf{Z}_{2n}$ with respect to the generators $1, 3, \ldots, 2n-1$ taken in that cyclic order. Thus the vertices are the elements of $\mathbf{Z}_{2n}$, coloured black or white as they are even or odd, and each vertex v is joined by edges to the vertices $v+1, v+3, \ldots, v-1$ in that cyclic order around v. This determines an orientably regular map $\mathcal{M}$ with n faces, all $2n$-gons, so $\mathcal{M}$ has Euler characteristic

$$\chi = 2n - n^2 + n = 3n - n^2$$

and hence has genus

$$g = 1 - \frac{\chi}{2} = \frac{(n-1)(n-2)}{2}.$$

The orientation-preserving automorphism group $\mathrm{Aut}^+\mathcal{M}$ is a wreath product $C_n \wr S_2$, with the direct factors of the normal subgroup $C_n \times C_n$ acting independently on the black and the white vertices by translations $v \mapsto v + a$, a even, and a complement S_2 transposing them, for instance by $v \mapsto v + 1$.

As an example, when $n = 3$ we obtain the torus map $\{6, 3\}_{1,1}$ in [9, §8.4].

4 MOTIVATION FROM THE THEORY OF DESSINS D'ENFANTS

According to Grothendieck's theory of *dessins d'enfants* [10], explained in more detail later in this paper, a compact Riemann surface $\mathcal{X}$ is defined (as an algebraic curve) over an algebraic number field if and only if its complex structure is obtained, in a canonical way, from an embedding of a bipartite graph in $\mathcal{X}$. The most symmetric examples correspond to orientably regular embeddings of bipartite graphs, and the most symmetric of these are the complete bipartite graphs $K_{n,n}$.

A classic example is the nth degree *Fermat curve* $\mathcal{F}_n$, defined as a projective variety by the equation

$$x^n + y^n = z^n.$$

This is defined over the rational field $\mathbf{Q}$, and as a Riemann surface it carries an embedding of $K_{n,n}$: the black and white vertices are the points with $x = 0$ and $y = 0$, and the edges are formed by the points $[x, y, z]$ with $(x/z)^n$ (and hence $(y/z)^n$) in the unit interval $[0, 1] \subset \mathbf{R}$. The resulting map $\mathcal{M}$ is isomorphic to the standard embedding of $K_{n,n}$: the base group $C_n \times C_n$ of $\mathrm{Aut}^+\mathcal{M}$ is obtained by multiplying x and y by nth roots of 1, and a complement by transposing x and y.

5 THE PROBLEMS

Motivated by the ideas in §§2–4, we study the following problems:

(a) find all the orientably regular embeddings of the graphs $K_{n,n}$;
(b) understand the corresponding algebraic curves $\mathcal{X}$, which we call the *generalised Fermat curves*.

The first significant result concerning Problem (a) was obtained by Nedela, Škoviera and Zlatoš [11]:

Theorem 1. *If n is prime the standard embedding is the only orientably regular embedding of $K_{n,n}$.* □

The proof of Theorem 1 uses directly combinatorial methods, but further progress requires other techniques. Kwak and Kwon [1, 2, 12] have had considerable success, in the orientable and non-orientable cases, by using permutations to represent embeddings of $K_{n,n}$ (see §14). An alternative approach, outlined here, is to convert Problem (a) into a purely group-theoretic problem, and then to apply results and techniques from that field. This approach, in joint work with Du, Kwak, Nedela and Škoviera, has given a complete solution to Problem (a), while partial results for Problem (b) have been obtained with Coste, Streit and Wolfart.

6 ISOBICYCLIC GROUPS

Let $\mathcal{M}$ be an orientably regular embedding of $K_{n,n}$. Then $\mathrm{Aut}^+\mathcal{M}$ has a subgroup $\mathrm{Aut}_0^+\mathcal{M}$ of index 2 preserving both surface-orientation and vertex-colours. The following is easy to prove (see [13], for instance):

Lemma 2. *A group G arises as $\mathrm{Aut}_0^+\mathcal{M}$ for some orientably regular embedding $\mathcal{M}$ of $K_{n,n}$ if and only if*

(i) *$G = XY$ with $X = \langle x\rangle$ and $Y = \langle y\rangle$ both cyclic subgroups of order n,*
(ii) *$X \cap Y = 1$,*
(iii) *there is an automorphism α of G transposing x and y.*

Then the isomorphism classes of orientably regular embeddings of $K_{n,n}$ associated with G correspond to the orbits of Aut *G on such pairs x, y in G.* □

If G satisfies (i), (ii) and (iii) we say it is *n-isobicyclic* (or simply *isobicyclic*), and we call (G, x, y) an *n-isobicyclic triple*. If $G = \mathrm{Aut}_0^+\mathcal{M}$ for some $\mathcal{M}$ then x and y are rotations of $\mathcal{M}$ around a black vertex v and a white vertex w, sending each incident edge to the next one by following the orientation around that vertex; the automorphism α is induced by conjugation by the half-turn in $\mathrm{Aut}^+\mathcal{M}$ reversing the edge vw. Conversely, if G is isobicyclic then one can identify the edges of $\mathcal{M}$ with the elements of G, and the black and white vertices with the cosets of X and Y, successive powers of x and y determining the local orientation around each vertex.

Condition (i) implies that each element of G has the form x^iy^j for some i and j, and condition (ii) implies that this factorisation is unique, so $|G| = |X|.|Y| = n^2$. For the standard embedding we have $G = X \times Y \cong C_n \times C_n$, but in general neither X nor Y need be a normal subgroup of G.

7 A UNIQUENESS RESULT

Lemma 2 allows one to construct non-standard embeddings of $K_{n,n}$ for certain values of n by finding appropriate isobicyclic groups $G \ncong C_n \times C_n$. There are simple examples of these when $n = p^e$ for some prime p with $e \geq 2$, and also when $n = pq$ for primes p and q with $p \equiv 1 \bmod (q)$. In a sense to be explained more fully in §10, all non-standard embeddings are generalisations of these.

The discovery of these simple examples gave rise to a uniqueness result. Let $\nu(n)$ denote the number of orientably regular embeddings of $K_{n,n}$, up to orientation-preserving isomorphism. The existence of the standard embedding implies that $\nu(n) \geq 1$ for all n, and Theorem 1 shows that $\nu(n) = 1$ whenever n is prime, whereas the non-standard examples mentioned above show that $\nu(n) > 1$ for certain other values of n. Lemma 2 allows one to characterise those n for which $\nu(n) = 1$, those for which the standard embedding is the only regular orientable embedding of $K_{n,n}$.

Define a positive integer n to be *singular* if $\gcd(n, \phi(n)) = 1$, where ϕ is Euler's function. Equivalently, n is a product of distinct primes, with no pair p, q of prime factors satisfying $p \equiv 1 \mod (q)$. Thus every prime number is singular, as are infinitely many composite numbers such as $3 \times 5 = 15, 3 \times 5 \times 17 = 255, 3 \times 5 \times 17 \times 23 = 5865$ and so on. Indeed, it follows easily from the Chinese Remainder Theorem and Dirichlet's Theorem on primes in arithmetic progressions that any such sequence of odd singular integers, each dividing the next, can be continued indefinitely.

Using Lemma 2, Nedela, Škoviera and the author [13] proved:

Theorem 3. $\nu(n) = 1$ *if and only if n is singular.* □

The existence of non-standard embeddings whenever n is nonsingular follows immediately from the basic examples mentioned above, together with the following straightforward result:

Lemma 4. *If (G_i, x_i, y_i) is an n_i-isobicyclic triple for each $i = 1, \ldots, k$, where $n_1, \ldots, n_k$ are mutually coprime, then (G, x, y) is an n-isobicyclic triple where $G = G_1 \times \cdots \times G_k$, $x = (x_i)$, $y = (y_i)$ and $n = n_1 \ldots n_k$.* □

If $\mathcal{M}_i$ is the orientably regular embedding of K_{n_i,n_i} corresponding to the triple (G_i, x_i, y_i), we denote by $\mathcal{M}_1 \times \cdots \times \mathcal{M}_k$ the orientably regular embedding of $K_{n,n}$ corresponding to (G, x, y), called the *cartesian product* of the embeddings $\mathcal{M}_i$.

The converse part of Theorem 3, namely the uniqueness of the standard embedding when n is singular, depends on an argument showing that in any isobicyclic group G, the subgroups X and Y contain normal subgroups X_p and Y_p of G of order p for some prime p dividing n. One can then argue by induction, regarding G as an extension of $X_p \times Y_p$ by the group $G/(X_p \times Y_p)$, which is also isobicyclic.

The singular integers are also those for which there is only one group of order n, namely C_n. This result is due to Burnside [14, Exercise 575]; the proofs are similar but independent of each other.

In 1947 Erdős [15] proved that the proportion of integers $n \leq N$ which are singular is asymptotic to

$$\frac{e^{-\gamma}}{\log \log \log N}$$

as $N \to \infty$, where γ is Euler's constant. This estimate approaches 0 as $N \to \infty$, but it does so very slowly!

8 PRIME POWER EMBEDDINGS

In the 1950s and 1960s, several mathematicians such as Douglas, Huppert, Itô, Rédei and Wielandt studied groups with factorisations $G = XY$, in many cases proving that if X and Y satisfy certain conditions, such as being cyclic, abelian, nilpotent, etc, then G satisfies certain correspondingly weaker conditions, such as being metabelian, solvable, etc. A typical result, due to Huppert [16] is:

Proposition 5. *If $G = XY$ where X and Y are cyclic groups and G is a p-group for some odd prime p, then G is metacyclic.* □

A metacyclic group is one which has a cyclic normal subgroup with a cyclic quotient. If $n = p^e$ for some odd prime p, so that the group $G = \mathrm{Aut}_0^+\mathcal{M}$ has order p^{2e}, then Lemma 2(i) implies that G satisfies the conditions of Proposition 5, so G is metacyclic. Using this, together with some p-group calculations exploiting the other parts of Lemma 2, Nedela, Škoviera and the author [17] were able to classify the orientably regular embeddings of $K_{n,n}$ for odd prime powers n:

Theorem 6. *If $n = p^e$ for some odd prime p then there are p^{e-1} orientably regular embeddings $\mathcal{M} = \mathcal{M}_{f,u}$ of $K_{n,n}$. They correspond to the groups*

$$\mathrm{Aut}_0^+\mathcal{M} = G = G_f := \langle g, h \mid g^n = h^n = 1, h^g = h^{1+p^f}\rangle$$

for $f = 1, 2, \ldots, e$, with $x = g^u, y = g^u h$ for some $u = 1, \ldots, p^{e-f}$ coprime to p. There are $\phi(p^{e-f})$ maps $\mathcal{M}_{f,u}$ associated with each G_f. These maps all have type $\{2n, n\}$ and genus $(n-1)(n-2)/2$. □

For instance, taking $f = e$, so that $h^g = h$ and hence $G \cong C_n \times C_n$, gives the standard embedding $\mathcal{M}_{e,1}$. Proposition 5 fails for $p = 2$, and in this case Du, Kwak, Nedela, Škoviera and the author have proved the following analogue of Theorem 6:

Theorem 7. *If $n = 2^e$ then the orientably regular embeddings of $K_{n,n}$ are*

(i) *the 2^{e-2} analogues for $p = 2$ of the maps $\mathcal{M}_{f,u}$ in Theorem 5 with $f = 2, \ldots, e$, for which $G = G_f$ is metabelian, and*

(ii) *one extra map when $e = 2$, and four for each $e \geq 3$, all with non-metabelian groups G.* □

Note that when $p = 2$ there are no analogues of the maps with $f = 1$ in Theorem 6. The exceptional map for $n = 4$ is the torus map $\{4, 4\}_{2,2}$ in the notation of [9, §8.3], and those for $n = 2^e \geq 8$ are branched coverings of $\{4, 4\}_{2,2}$, of type $\{n, n\}$ and genus $(n^2-4n+2)/2$. The proof of Theorem 7 uses the same p-group techniques as Theorem 6 in the cases where G is metacyclic [18], and uses induction on e to deal with the non-metacyclic exceptional cases [19].

9 CLASSIFYING ALL COMPLETE BIPARTITE MAPS

Theorems 6 and 7 describe the orientably regular embeddings $\mathcal{M}$ of $K_{n,n}$ for all prime powers n. The following result of Wielandt [20] allows one to extend these classifications to all n:

Proposition 8. *Let $G = XY$ where X and Y are finite cyclic groups, and let $p_1 > \cdots > p_k$ be the primes dividing $|G|$. Then G has a Sylow tower, that is, a series of normal subgroups*

$$1 < P_1 < P_1P_2 < \cdots < P_1 \ldots P_k = G \qquad (9.1)$$

where each P_i is a Sylow p_i-subgroup of G. □

In our case, $|G| = n^2$, so the primes p_i dividing $|G|$ are those dividing n. If

$$n = p_1^{e_1} \ldots p_k^{e_k}$$

then one can show that each P_i is $p_i^{e_i}$-isobicyclic, so it is one of the groups described in Theorem 6 or Theorem 7. The possibilities for the quotients

$$P_1 \ldots P_i / P_1 \ldots P_{i-1} \cong P_i$$

in the series (9.1) are therefore known, so one can try to reconstruct G. The argument is by induction on k, regarding G as an extension of a normal subgroup P_1 by an $\overline{n}$-isobicyclic group $\overline{G} = G/P_1$, where $\overline{n} = p_2^{e_2} \dots p_k^{e_k}$. Since P_1 and $\overline{G}$ have coprime orders, this extension is split, by the Schur-Zassenhaus Theorem, so it is sufficient to determine how $P_2, \dots, P_k$ can act by conjugation on P_1 to give an n-isobicyclic group G. Proposition 8 implies that G is solvable (in fact it is metabelian [21]), so one can also apply Hall's extension of Sylow's Theorems from single primes to sets of primes, valid for all finite solvable groups [22]. The main result is that the maps are all formed from the prime power maps in Theorems 6 and 7 by two simple constructions: the first is the cartesian product, given by Lemma 4, and the second is given by the following straightforward result.

Lemma 9. *Let (S,x,y) be an s-isobicyclic triple, let $T = C_t \times C_t$ with s and t coprime, and let G be the semidirect product $T : S$ of T by S where x and y act by conjugation on the normal subgroup T as matrices $\left(\begin{smallmatrix}\lambda & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 0 & \lambda\end{smallmatrix}\right)$ in $GL_n(\mathbf{Z}_t)$ for some unit $\lambda \in \mathbf{Z}_t^*$. Then G is n-isobicyclic where $n = st$.* □

If $\mathcal{S}$ and $\mathcal{T}$ (the standard embedding of $K_{t,t}$) are the orientably regular embeddings of $K_{s,s}$ and $K_{t,t}$ corresponding to S and T, we call the orientably regular embedding of $K_{n,n}$ corresponding to G in Lemma 9 a *semidirect product* or *abelian covering* $\mathcal{T} : \mathcal{S}$ of $\mathcal{S}$ by $\mathcal{T}$.

The classification is as follows, with the full proof in [23]:

Theorem 10. *For each $n \geq 1$, the orientably regular embeddings of $K_{n,n}$ are the maps of the form $\mathcal{M} = \mathcal{T} : \mathcal{S}$, where*

(i) *$n = st$ with s and t coprime,*
(ii) *$\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_k$ with each $\mathcal{S}_i$ an orientably regular embedding of K_{n_i,n_i}, where $s = n_1 \dots n_k$ with $n_1, \dots, n_k$ mutually coprime prime powers,*
(iii) *$\mathcal{T}$ is the standard embedding of $K_{t,t}$.*

Then $\mathrm{Aut}_0^+ \mathcal{M} \cong T : (S_1 \times \cdots \times S_k)$ *where T ($\cong C_t \times C_t$) and S_i are the isobicyclic groups corresponding to $\mathcal{T}$ and $\mathcal{S}_i$.* □

Since each n_i is a prime power, the embeddings $\mathcal{S}_i$ are all as described in Theorems 6 and 7 for odd and even n_i. Then $\mathcal{M}$ is completely determined by

- the factorisation $n = st$ of n,
- the choice of the embeddings $\mathcal{S}_i$, and
- the eigenvalue $\lambda \in \mathbf{Z}_t^*$ which determines the action of S on T in Lemma 9.

Given this information one can determine the type and the genus of $\mathcal{M}$ by computing the order m of xy in G: the faces are all $2m$-gons, so the type is $\{2m, n\}$; since there are n^2/m faces the Euler characteristic is $2n - n^2 + n^2/m$, so the genus is

$$1 - n + \frac{n^2}{2} - \frac{n^2}{2m}.$$

10 ENUMERATION

Theorem 10 and the comments following it allow one to determine the number $\nu(n)$ of orientably regular embeddings of $K_{n,n}$ for each n. The result is a rather complicated formula, which agrees with earlier results obtained in special cases, for instance when n is a prime power (§8) or a product of two primes [12], and also with a computer search for $n \leq 100$.

Let Π denote the set of all prime numbers, and let $\to$ denote the binary relation on Π defined by $q \to p$ if and only if q divides $p - 1$; one can regard Π as a directed graph, with this relation defining the set of arcs of Π. Given an integer $f \geq 1$, and an arc $q \to p$ of Π, define $f_{q,p} = \min\{f, r(q,p)\}$ where $r = r(q,p)$ is defined by $q^r \parallel p - 1$ (so q^r is the highest power of q dividing $p - 1$).

For each integer $n \geq 1$, let Π_n denote the set of primes dividing n, regarded as a subgraph of Π by restricting the relation $\to$ to Π_n. We say that $\rightharpoonup$ is a *short subrelation* of $\to$ on Π_n if $\rightharpoonup$ is a subrelation of $\to$ on Π_n (i.e. if $q \rightharpoonup p$ implies that $p, q \in \Pi_n$ with $q \mid p-1$) and there is no triple p, q, r in Π_n with $r \rightharpoonup q \rightharpoonup p$; equivalently, $\rightharpoonup$ defines a directed subgraph Γ of Π_n which is *short*, written $\Gamma \preceq \Pi_n$, in the sense that it contains no directed paths of length greater than 1. For each short subgraph $\Gamma \preceq \Pi_n$, corresponding to a short subrelation $\rightharpoonup$, define

$$N(\Gamma) = \{p \in \Pi_n \mid q \rightharpoonup p \ \text{ for no } q \in \Pi_n\},$$

the set of nonterminal vertices in Γ.

Theorem 11. *If n is odd, with prime power factorisation $\prod_q q^{e_q}$, then the number $\nu(n)$ of orientably regular embeddings of $K_{n,n}$ is given by*

$$\nu(n) = \sum_{\Gamma \preceq \Pi_n} \left(\prod_{q \in N(\Gamma)} \left(\sum_{f=1}^{e_q} \left(\phi(q^{e_q - f}) \prod_{q \rightharpoonup p} (q^{f_{q,p}} - 1) \right) \right) \right). \qquad \square$$

Here an arc $q \rightharpoonup p$ in Γ denotes that in the Sylow tower (9.1), a Sylow q-subgroup Q of G has a nontrivial action by conjugation on a Sylow p-subgroup P; this implies that $q \mid p-1$, and that no Sylow r-subgroup can act nontrivially on Q, so summing over all short subgraphs Γ of Π_n accounts for all choices of such sets of pairs p and q. For each such choice, we consider the nonterminal vertices q and count the $\phi(q^{e_q - f})$ possible Sylow q-subgroups Q for each value of the parameter f in Theorem 6, together with the $q^{f_{q,p}} - 1$ nontrivial actions of each Q on the Sylow p-subgroup P, to obtain the number of embeddings in Theorem 10.

11 DIGRESSION ON THE RANDOM GRAPH

Let us modify the construction of Π in §10 and consider the graph Π' whose vertices are all the odd primes, with an undirected edge between p and q whenever $q \mid p-1$. It is a simple consequence of the Chinese Remainder Theorem and Dirichlet's Theorem on primes in arithmetic progressions that for each disjoint pair U and V of finite sets of vertices of Π' there is a vertex adjacent to every vertex in U and to no vertex in V. Any countably infinite graph with this property is isomorphic to the *random graph* or *universal graph* R studied by Erdős and Rényi [24] and constructed by Rado [25], so $\Pi' \cong R$. Further properties of this remarkable graph are discussed in [26, §5.1] and [27, §9.6]: for instance, given any countably infinite set of vertices, if pairs of them are chosen at random to be edges, each with probability $\frac{1}{2}$, then the resulting graph is isomorphic to R with probability 1.

12 ENUMERATION FOR n EVEN

Returning to the problem of enumerating the orientably regular embeddings of $K_{n,n}$, the situation is rather more complicated for even n because of the exceptional embeddings corresponding to powers of 2 in Theorem 7. Suppose that $2^{e_2} \parallel n$, with $e_2 \geq 1$. Then the techniques discussed earlier give:

Theorem 12.

(a) *If $1 \leq e_2 \leq 2$, so that $2 \parallel n$ or $2^2 \parallel n$, then*

$$\nu(n) = \sum_{\Gamma \preceq \Pi_n} \left(\prod_{q \in N(\Gamma)} \left(\sum_{f=1}^{e_q} \left(\phi(q^{e_q - f}) \prod_{q \rightharpoonup p} (q^{f_{q,p}} - 1) \right) \right) \right).$$

(b) *If n is divisible by* 8 *then*

$$\nu(n) = \sum_{\Gamma \preceq \Pi_n} \left(\left(\sum_{f=2}^{e_2} \left(\phi(2^{e_2-f}) \prod_{2 \rightharpoonup p} (2^{f_{2,p}} - 1) \right) + 4 \right) \right.$$
$$\left. \times \prod_{2 \neq q \in N(\Gamma)} \left(\sum_{f=1}^{e_q} \left(\phi(q^{e_q-f}) \prod_{q \rightharpoonup p} (q^{f_{q,p}} - 1) \right) \right) \right). \qquad \square$$

An equivalent version of the formula in Theorem 12(b) is:

$$\nu(n) = \sum_{\Gamma \preceq \Pi_n} \left(\prod_{q \in N(\Gamma)} \left(\sum_{f=1}^{e_q} \left(\phi(q^{e_q-f}) \prod_{q \rightharpoonup p} (q^{f_{q,p}} - 1) \right) \right) \right)$$
$$+ (4 - 2^{e_2-2}) \sum_{\Gamma \preceq \Pi_n} \left(\prod_{2 \neq q \in N(\Gamma)} \left(\sum_{f=1}^{e_q} \left(\phi(q^{e_q-f}) \prod_{q \rightharpoonup p} (q^{f_{q,p}} - 1) \right) \right) \right).$$

The following table gives the values of $\nu(n)$ obtained from Theorems 11 and 12 for all $n \leq 120$. According to Nedela [28], Fujisaki used a computer search, based on the Kwak-Kwon permutation method (see [12] and §14), to evaluate $\nu(n)$ for all $n \leq 100$. The above values of $\nu(n)$ agree with all of his in this range, except in the case $n = 90$, where Fujisaki's reported value $\nu(90) = 6$ appears to be a typographic error. (It is easy to construct eight non-isomorphic orientably regular embeddings of $K_{n,n}$ in this case.) The initial evidence provided by Fujisaki's search was of considerable value in showing that the approach used to prove Theorem 10 was correct.

Table 1. Values of $\nu(n)$ for $1 \leq n \leq 120$.

n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$
1	1	21	3	41	1	61	1	81	27	101	1
2	1	22	2	42	8	62	2	82	2	102	4
3	1	23	1	43	1	63	9	83	1	103	1
4	2	24	12	44	4	64	20	84	16	104	16
5	1	25	5	45	3	65	1	85	1	105	3
6	2	26	2	46	2	66	4	86	2	106	2
7	1	27	9	47	1	67	1	87	1	107	1
8	6	28	4	48	16	68	6	88	12	108	20
9	3	29	1	49	7	69	1	89	1	109	1
10	2	30	4	50	6	70	4	90	8	110	12
11	1	31	1	51	1	71	1	91	1	111	3
12	4	32	12	52	6	72	24	92	4	112	16
13	1	33	1	53	1	73	1	93	3	113	1
14	2	34	2	54	10	74	2	94	2	114	8
15	1	35	1	55	5	75	5	95	1	115	1
16	8	36	8	56	12	76	4	96	24	116	6
17	1	37	1	57	3	77	1	97	1	117	9
18	4	38	2	58	2	78	8	98	8	118	2
19	1	39	3	59	1	79	1	99	3	119	1
20	6	40	16	60	12	80	24	100	14	120	32

13 REFLEXIBILITY AND PETRIE DUALITY

An orientably regular map is *reflexible* if it has an automorphism reversing the surface-orientation. In the case of an orientably regular embedding of $K_{n,n}$, this is equivalent to the existence of an automorphism of G inverting x and y. The methods described in §9 and §10 can be used to classify the reflexible embeddings of $K_{n,n}$, and in particular we find that the number $\rho(n)$ of them is given by

$$\rho(n) = \begin{cases} 1 & \text{if } e_2 = 0, \\ 2^r & \text{if } e_2 = 1, \\ 2^{r+1} & \text{if } e_2 = 2, \\ 3.2^{r+1} & \text{if } e_2 \geq 3, \end{cases}$$

where $2^{e_2} \parallel n$ and n is divisible by r distinct odd primes. This agrees with an enumeration obtained earlier by Kwak and Kwon [1], using their method based on permutations (see §14).

These reflexible embeddings are *regular*, meaning that the full automorphism group Aut $\mathcal{M}$ acts transitively (and hence regularly) on flags consisting of incident vertex-edge-face triples. Kwak and Kwon [2] have proved that $K_{n,n}$ has a regular embedding in a non-orientable surface if and only if $e_2 = 1$ and $p \equiv \pm 1 \bmod (8)$ for each odd prime p dividing n, in which case the number of such embeddings is 2^r.

The *Petrie dual* $\mathrm{P}(\mathcal{M})$ of a map $\mathcal{M}$ has the same embedded graph as $\mathcal{M}$, but has new faces, bounded by the Petrie polygons (closed zig-zag paths) of $\mathcal{M}$, so that $\mathrm{Aut}\,\mathcal{M} = \mathrm{Aut}\,\mathrm{P}(\mathcal{M})$. If $\mathcal{M}$ is an orientably regular embedding of $K_{n,n}$ then $\mathrm{P}(\mathcal{M})$ is an orientable embedding of $K_{n,n}$; if it is orientably regular, then $\mathcal{M}$ must be reflexible, in which case $\mathrm{P}(\mathcal{M})$ is obtained from $\mathcal{M}$ by inverting either x or y. We say that $\mathcal{M}$ is *self-Petrie* if $\mathcal{M} \cong \mathrm{P}(\mathcal{M})$; the methods discussed here allow one to classify the self-Petrie embeddings of $K_{n,n}$, and to show that the number of them is

$$\sigma(n) = \begin{cases} 1 & \text{if } e_2 = 0, \\ 2^r & \text{if } e_2 = 1, \\ 2^{r+1} & \text{if } e_2 = 2, \\ 2^{r+2} & \text{if } e_2 \geq 3, \end{cases}$$

where e_2 and r are as above. As in the case of reflexibility, this agrees with an enumeration obtained earlier by Kwak and Kwon [1].

14 THE PERMUTATION METHOD OF KWAK AND KWON

This section briefly explains the method developed by Kwak and Kwon [1, 12], which uses permutations to study orientably regular embeddings of $K_{n,n}$. They systematically label the vertices, so that such maps correspond bijectively to permutations of the labels satisfying certain properties.

If $\mathcal{M}$ is an orientably regular embedding of $K_{n,n}$ then let a pair of black and white vertices v and w be labelled 0 and $0'$. The automorphism x defined in §6 fixes v and permutes the white vertices in a cycle of length n; the white vertices other than w can be labelled $1', 2', \ldots, (n-1)'$ so that x induces the permutation $(0', 1', \ldots, (n-1)')$ of these labels. The black vertices other than v can then be labelled $1, 2, \ldots, n-1$ so that the half-turn a which transposes v and w induces the permutation

$$\lambda = (0, 0')(1, 1') \ldots (n-1, (n-1)')$$

of the labels. It follows that x induces a permutation

$$\rho_\sigma = \sigma(0', 1', \ldots, (n-1)') = (0', 1', \ldots, (n-1)')\sigma$$

of the set of $2n$ labels, where σ is a permutation of $\{0, 1, \ldots, n-1\}$ fixing 0, which is uniquely determined by $\mathcal{M}$. Since $y = x^a$ we also obtain the permutation ρ_σ^λ of the $2n$ labels representing y by transposing pairs of labels i and i' in the permutation ρ_σ. The analogue of Lemma 2 states that a permutation σ of $\{0, 1, \ldots, n-1\}$ fixing 0 corresponds to an orientably regular embedding $\mathcal{M}$ of $K_{n,n}$ if and only if the subgroup $\langle \rho_\sigma, \lambda \rangle$ of S_{2n} generated by ρ_σ and λ has order $2n^2$, or equivalently the subgroup $\langle \rho_\sigma, \rho_\sigma^\lambda \rangle$ of $S_n \times S_n \leq S_{2n}$ has order n^2; in this case $\mathcal{M}$ is unique, and these two subgroups correspond to $\mathrm{Aut}^+\mathcal{M}$ and to $G = \mathrm{Aut}_0^+\mathcal{M}$ in our earlier notation. In particular the number $\nu(n)$ of such embeddings $\mathcal{M}$ is equal to the number of such permutations σ. For instance, the standard embedding corresponds to the identity permutation.

This approach allows embeddings $\mathcal{M}$ to be studied and enumerated in terms of combinatorial properties of the corresponding permutations σ, which must have order dividing n. For instance, if n is prime then since σ has a fixed point it must be the identity, so we immediately obtain a proof of Theorem 1. Kwak and Kwon have used this method in [12] to enumerate orientably regular embeddings of $K_{n,n}$ when n is a product of two primes (not necessarily distinct), and in [1] to obtain the enumerations of reflexible and of self-Petrie embeddings mentioned in §13. An extension of this method in [2] also gives the enumeration of non-orientable regular embeddings mentioned there.

15 COMPLETE BIPARTITE MAPS AND SKEW-MORPHISMS

There is a link between the group-theoretic and the permutational approaches to complete bipartite maps through skew-morphisms, which were introduced by Jajcay and Širáň [29] to characterise orientably regular Cayley maps.

A permutation ϕ of order r of the elements of a group G is called a *skew-morphism* of G with respect to a power-function $\pi : G \to \mathbf{Z}_r$ if ϕ fixes the identity element and

$$\phi(gh) = \phi(g)\phi^{\pi(g)}(h)$$

for all $g, h \in G$, where $\phi^{\pi(g)}$ denotes ϕ iterated $\pi(g)$ times. Thus ϕ is an automorphism if $\pi(g) = 1$ for all $g \in G$. Jajcay and Širáň proved that a Cayley map is orientably regular if and only if the cyclic permutation of the generators defining the map extends to a skew-morphism of the group. (This represents the permutation of the vertices induced by rotating the map around the identity element, each incident edge sent to the next edge according to the local orientation.) For instance, in the construction of the standard embedding of $K_{n,n}$ in §3 as a Cayley map over $\mathbf{Z}_{2n}$, we have

$$\phi(g) = \begin{cases} g & \text{if } g \text{ is even,} \\ g+2 & \text{if } g \text{ is odd,} \end{cases}$$

with

$$\pi(g) = \begin{cases} 1 & \text{if } g \text{ is even,} \\ -1 & \text{if } g \text{ is odd.} \end{cases}$$

Now let $G = \mathrm{Aut}_0^+\mathcal{M}$ for some orientably regular embedding $\mathcal{M}$ of $K_{n,n}$. By Lemma 2 we have $G = XY$, so taking inverses gives $G = YX$, and hence there are functions $\phi, \psi : \mathbf{Z}_n \to \mathbf{Z}_n$ such that

$$xy^i = y^{\phi(i)}y^{\psi(i)}$$

for all i. Representing x and y as permutations σ and $\rho = (0, 1, \ldots, n-1)$ of the black vertices, as in §14, we therefore have

$$\sigma\rho^i = \rho^{\phi(i)}\sigma^{\psi(i)}$$

for all i. This implies that

$$\sigma(i+j) = \sigma\rho^i(j) = \rho^{\phi(i)}\sigma^{\psi(i)}(j) = \phi(i) + \sigma^{\psi(i)}(j)$$

for all i and j. Putting $j = 0$ and using the fact that σ fixes 0 we see that $\phi = \sigma$, so

$$\sigma(i+j) = \sigma(i) + \sigma^{\psi(i)}(j)$$

for all i and j, which shows that σ is a skew-morphism of the additive group $\mathbf{Z}_n$ with respect to the power function ψ.

Skew-morphisms thus describe the permutations σ used in the permutational approach, and also control the general lack of commutativity of X and Y in the group-theoretic approach. A good understanding of skew-morphisms might help to strengthen the connections between these two approaches.

The second part of this paper considers connections between the preceding work and other areas of mathematics. See [30], [31] or [32] for more details.

16 RIEMANN SURFACES AND ALGEBRAIC CURVES

A *Riemann surface* is a surface $\mathcal{X}$ (always assumed here to be connected) which is covered by subsets homeomorphic to open subsets of the complex plane $\mathbf{C}$, giving local complex coordinates on $\mathcal{X}$. We require that whenever such subsets overlap, the resulting change of coordinates functions are analytic, thus allowing the usual operations of complex analysis to be performed on $\mathcal{X}$ in a consistent way.

Example 1. The *Riemann sphere* $\hat{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$, also known in algebraic geometry as the *complex projective line*, has complex coordinates z and $1/z$ on its open subsets $\mathbf{C}$ and $\hat{\mathbf{C}} \setminus \{0\}$, with the change of coordinate function $z \mapsto 1/z$ analytic on $\mathbf{C} \setminus \{0\}$.

The Riemann sphere is compact. Indeed, Riemann proved that a Riemann surface is compact if and only if it corresponds to an algebraic curve over $\mathbf{C}$, that is, it is defined, as an algebraic variety, by a finite set of polynomial equations with complex coefficients. This gives us very powerful 'dictionary' between the concepts of complex analysis and algebraic geometry, when applied to compact Riemann surfaces.

Example 2. If Λ is a lattice in $\mathbf{C}$ (that is, an additive subgroup generated by two elements which are linearly independent over $\mathbf{R}$), then $\mathbf{C}/\Lambda$ is a compact Riemann surface of genus 1, known as a *torus*. Equivalently, it can also be regarded as an *elliptic curve*

$$y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in \mathbf{C} \setminus \{0, 1\}$. Elliptic curves, and their associated elliptic functions and integrals, have a history going back over 200 years; they have recently achieved prominence in providing the proof of Fermat's Last Theorem, and in forming the basis for powerful cryptographic systems.

17 BELYĬ'S THEOREM

It is of considerable interest to know which compact Riemann surfaces can be defined (as algebraic curves) over specific subfields $F \subseteq \mathbf{C}$. This is straightforward for $F = \mathbf{R}$, whereas very little is known about the case $F = \mathbf{Q}$ (the recently-proved Taniyama-Shimura Conjecture, part of which led Wiles to a proof of Fermat's Last Theorem, gives a necessary condition for an elliptic curve to be defined over the rationals). Here we consider the case where F is the field of algebraic numbers, that is, the algebraic closure

$$\overline{\mathbf{Q}} = \{z \in \mathbf{C} \mid f(z) = 0 \text{ for some non-zero } f(t) \in \mathbf{Q}[t]\}$$

of $\mathbf{Q}$ in $\mathbf{C}$. As part of an investigation into the Inverse Galois Problem (Hilbert's conjecture that every finite group is the Galois group of an algebraic number field), Belyĭ [33] characterised Riemann surfaces defined over $\overline{\mathbf{Q}}$ in terms of the branching of meromorphic functions.

If $\beta : \mathcal{X} \to \hat{\mathbf{C}}$ is a non-constant meromorphic function (analytic apart from poles of finite order), then it is a d-sheeted branched covering of $\hat{\mathbf{C}}$ for some finite $d = \deg(\beta)$, meaning that $|\beta^{-1}(w)| = d$ for all but finitely many points $w \in \hat{\mathbf{C}}$, so that a small neighbourhood N of w is covered by d disjoint open sets in $\mathcal{X}$, each mapped homeomorphically onto N. At the finitely many exceptional points w we have $1 \leq |\beta^{-1}(w)| < d$, with some of the d sheets of the covering coming together over w; these are the *branch points* of β on $\hat{\mathbf{C}}$. Belyĭ's Theorem states:

Theorem 13. *A compact Riemann surface $\mathcal{X}$ is defined (as an algebraic curve) over the field $\overline{\mathbf{Q}}$ of algebraic numbers if and only if there is a non-constant meromorphic function $\beta : \mathcal{X} \to \hat{\mathbf{C}}$ which is branched over at most three points in $\hat{\mathbf{C}}$.* □

Such a function β is called a *Belyĭ function*, and $(\mathcal{X}, \beta)$ is called a *Belyĭ pair*. The automorphisms of the Riemann surface $\hat{\mathbf{C}}$ are the Möbius transformations $w \mapsto (aw+b)/(cw+d)$ where $a, b, c, d \in \mathbf{C}$ and $ad - bc \neq 0$, forming the group $PGL_2(\mathbf{C})$; this group acts triply transitively on $\hat{\mathbf{C}}$, so by composing β with a Möbius transformation we may assume that β is unbranched outside $\{0, 1, \infty\}$.

Belyĭ proved that his condition is necessary by giving an ingenious algorithm for constructing β (see [32] for a more efficient one), but his proof of sufficiency was simply a two-line reference to Weil's Rigidity Theorem. In fact, a completely satisfactory proof of this part of the theorem did not appear until 25 years later; this was provided by Koeck [34], building on earlier work by Wolfart [35].

Example 3. Let $\mathcal{X}$ be the nth degree Fermat curve $\mathcal{F}_n$, defined over $\mathbf{Q} \subset \overline{\mathbf{Q}}$ as a projective algebraic curve of genus $(n-1)(n-2)/2$ by the equation $x^n + y^n = z^n$. As a Belyĭ function we can take $\beta : [x, y, z] \mapsto w = (x/z)^n$. It is straightforward to verify that $\deg(\beta) = n^2$, with $|\beta^{-1}(w)| = n$ at the branch points $w = 0, 1$ and ∞.

Let $\mathcal{B}_1$ be the trivial bipartite map on the sphere $\hat{\mathbf{C}}$, with black and white vertices at 0 and 1 and an edge along the unit interval $I = [0, 1]$. If $(\mathcal{X}, \beta)$ is a Belyĭ pair then $\mathcal{B} = \beta^{-1}(\mathcal{B}_1)$ is a bipartite map on $\mathcal{X}$. The cyclic permutations of the edges around the black and white vertices and the faces give the branching data for β over $0, 1$ and ∞, so $\mathcal{B}$ can be regarded as a combinatorial picture of β. Conversely, any bipartite map on a compact oriented surface $\mathcal{S}$ can be described by such permutations, so by Riemann's Existence Theorem it determines a unique complex structure on $\mathcal{S}$, making $\mathcal{S}$ into a compact Riemann surface $\mathcal{X}$ and hence an algebraic curve. This is the basis of Grothendieck's theory of *dessins d'enfants*, or children's drawings [10], in which apparently simple sketches can encode very complicated mathematical phenomena.

Example 4. If $(\mathcal{X}, \beta)$ is as in Example 3 then $\mathcal{B}$ is the standard embedding of $K_{n,n}$ on $\mathcal{F}_n$, as in §4.

Any compact oriented bipartite map $\mathcal{B}$ corresponds to a Belyĭ pair $(\mathcal{X}, \beta)$, and the finitely many coefficients of the polynomials and rational functions defining $\mathcal{X}$ and β are all algebraic numbers, so the subfield of $\mathbf{C}$ they generate is a finite extension of $\mathbf{Q}$, that is, an algebraic number field. Determining such a field of definition for a given map $\mathcal{B}$ is an interesting but difficult problem, though it is a little easier if there is some symmetry involved. One of the few cases where explicit results are known involves the orientably regular embeddings of $K_{n,n}$ discussed in §8, where $n = p^e$ for some prime p. The exceptional maps in Theorem 7 for $p = 2$ correspond to curves defined over $\mathbf{Q}$, so let us ignore them and consider the algebraic curves $\mathcal{X}_{f,u}$ corresponding to the maps $\mathcal{M}_{f,u}$ with metacyclic groups $G = G_{f,u}$ in Theorems 6 and 7. Let $\eta = \exp(2\pi i/p^{e-f})$, so that $\mathbf{Q}(\eta)$ is a cyclotomic field. Streit, Wolfart and the author [36] have recently proved:

Theorem 14. *For each prime power $n = p^e$ and each $f \leq e$, the $\phi(p^{e-f})$ curves $\mathcal{X}_{f,u}$ are all defined over $\mathbf{Q}(\eta)$.* □

Finding explicit equations for the curves $\mathcal{X}_{f,u}$ is harder, and has been achieved only when $f \geq e/2$. These are the cases where G_f is 'close to abelian', and in particular has several large abelian normal subgroups which can be used to construct the field of rational functions on the curve from its Galois group G_f, and hence to obtain the defining equations [36].

Theorem 15. *If p is odd and $f \geq e/2$ then an affine model of $\mathcal{X}_{f,u}$ in $\mathbf{C}^3$ is given by the equations*

$$v^n = w^{p^{e-f}}(w^{p^{e-f}} - 1) \quad \textit{and} \quad z^{p^f} = w^{-r}. \prod_{k=0}^{p^{e-f}-1} (w - \eta^{uk})^{ak},$$

where r and a are integers given by

$$r = \frac{(1+p^f)^{p^{e-f}} - 1}{p^e} \quad \textit{and} \quad a = p^{2f-e}.$$

The Belyĭ function $\beta : \mathcal{X}_{f,u} \to \hat{\mathbf{C}}$ corresponding to $\mathcal{M}_{f,u}$ is given by

$$(v, w, z) \mapsto 1 - w^{p^{e-f}}.$$ □

(There are similar results for $\mathcal{X}_{f,u}$ in the case $p = 2$.)

19 GALOIS THEORY

The *absolute Galois group* $\mathbf{\Gamma}$ is the Galois group $\mathrm{Gal}\,\overline{\mathbf{Q}}/\mathbf{Q}$ of $\overline{\mathbf{Q}}$. Now $\overline{\mathbf{Q}}$ is the union of the Galois (finite normal) extensions K of $\mathbf{Q}$ in $\mathbf{C}$, i.e. the splitting fields of polynomials in $\mathbf{Q}[t]$. These have finite Galois groups $G_K = \mathrm{Gal}\,K/\mathbf{Q}$, and given any inclusion $K \subseteq L$ between them, restriction of automorphisms gives an epimorphism $G_L \to G_K$. It follows that $\mathbf{\Gamma}$ is the projective limit $\lim_{\leftarrow} G_K$ of this system of finite groups, that is, $\mathbf{\Gamma}$ is a profinite group: it can be identified with the subgroup of the cartesian product $\prod_K G_K$ consisting of those elements whose coordinates are compatible with the restriction homomorphisms. The discrete topology on the groups G_K induces a compact topology on $\mathbf{\Gamma}$, the *Krull topology*, with respect to which $\mathbf{\Gamma}$ is a topological group, homeomorphic to a Cantor set. In the Galois correspondence between fields and groups, the subfields of $\overline{\mathbf{Q}}$ correspond to the closed subgroups of $\mathbf{\Gamma}$.

The group $\mathbf{\Gamma}$ has a natural action on Belyĭ pairs, by acting on the coefficients of the polynomials and rational functions defining them, so it has an induced action on the corresponding bipartite maps. As shown in [37], this action preserves such properties as the numbers and valencies of vertices and faces, the genus and the orientation-preserving automorphism group. Nevertheless, this action is faithful on isomorphism classes of bipartite maps, even when restricted to those of a given genus.

It is therefore of interest to determine the orbits of $\mathbf{\Gamma}$ on bipartite maps. As with the related question of fields of definition, this is a difficult problem, with relatively few explicit results. In the situation in Theorem 14, where the curves $\mathcal{X}_{f,u}$ are all defined over the cyclotomic field $\mathbf{Q}(\eta)$, we have [36]:

Theorem 16. *For each prime power $n = p^e$ and each $f \leq e$, the $\phi(p^{e-f})$ curves $\mathcal{X}_{f,u}$ form a single orbit under* $\mathrm{Gal}\,\mathbf{Q}(\eta)/\mathbf{Q}$ *(and hence under $\mathbf{\Gamma}$).* □

Here $\mathrm{Gal}\,\mathbf{Q}(\eta)/\mathbf{Q} \cong \mathbf{Z}^*_{p^{e-f}}$, the group of units mod (p^{e-f}); each unit $j \in \mathbf{Z}^*_{p^{e-f}}$ acts on $\mathbf{Q}(\eta)$ by $\eta \mapsto \eta^j$, and on the maps and curves by $u \mapsto ju$ mod (p^{e-f}).

20 EDGE-TRANSITIVE EMBEDDINGS

It is useful to extend the classification of orientable embeddings of $K_{n,n}$ to include all the cases where the group $G = \mathrm{Aut}_0^+\mathcal{M}$ acts transitively on edges, without also assuming (as before) that some element of $\mathrm{Aut}^+\mathcal{M}$ reverses an edge. This is of interest from the point of view of the theory of dessins d'enfants, since it corresponds to the cases where the associated Belyĭ function β is a regular covering, i.e. of the form $\mathcal{X} \to \mathcal{X}/G \cong \hat{\mathbf{C}}$. In terms of groups, this generalisation corresponds to omitting condition (iii) in Lemma 2.

The methods developed in [13, 17] and described in §8 provide such a classification in the cases where n is an odd prime power, and also where $n = 2^e$ with G metacyclic. Results analogous to Theorems 14, 15 and 16 have also been obtained for this wider class of embeddings in [38]. The techniques used to prove Theorem 10 allow this classification to be extended to the cases where the Sylow 2-subgroup of G is metacyclic, in particular including those cases where n is odd.

21 WORK IN PROGRESS OR REMAINING TO BE DONE

There are still many open problems in this area. Work is in progress on some of them, whereas others have yet to be considered seriously. Here are some of the open problems:

- Understand the connections between the group-theoretic approach to embeddings of $K_{n,n}$ and the more combinatorial approach used by Kwak and Kwon [1, 2, 12], described in §14. For instance, can the former method be applied to non-orientable embeddings, perhaps by considering products of dihedral groups?
- Understand the role of skew-morphisms in these two approaches. For instance, which orientably regular embeddings of $K_{n,n}$ are Cayley maps (see §15)? They all are when n is an odd prime power [17], but what happens in general?
- Extend Theorem 15 to deal with all the prime power embeddings, not just those with $f \geq e/2$. The Galois theory involved here seems to be very difficult, since the groups involved are rather far from abelian.
- Extend the results in §18 and §19 to deal with all n, not just the prime powers. It should be possible to use Theorem 10, together with Theorems 14 and 16, to find fields of definition and Galois orbits for more general values of n, though finding explicit equations for the curves appears to be impossibly difficult.

- Extend the classification of edge-transitive orientable embeddings of $K_{n,n}$, mentioned in §20, to all n. The obstacle to progress on even n is the fact that the case where $n = 2^e$ and G is not metacyclic remains open.
- Extend the latter classification to $K_{m,n}$ for all m and n. Again, this is a natural generalisation for the theory of dessins d'enfants. There is some hope that current methods can achieve this, at least when m and n are powers of the same odd prime.
- The automorphisms $\eta \mapsto \eta^j$ of cyclotomic fields $\mathbf{Q}(\eta)$ appearing in Theorem 16 act on the maps $\mathcal{M}_{f,u}$ in the same way as certain map operations H_j defined by Wilson [39]. Work in progress with Streit and Wolfart shows that this phenomenon occurs for certain other classes of orientably regular maps, such as embeddings of complete graphs, but not for all of them. One would like a better understanding of this connection, and of the more general relationship between Galois conjugacy and map operations.

REFERENCES

[1] J. H. Kwak and Y. S. Kwon, Classification of reflexive regular embeddings and self-Petrie dual regular embeddings of complete bipartite graphs, Discrete Math. 308(2008) 2156–2166.

[2] J. H. Kwak and Y. S. Kwon, Classification of nonorientable regular embeddings of complete bipartite graphs, submitted.

[3] L. D. James and G. A. Jones, Regular orientable imbeddings of complete graphs, *J. Combinatorial Theory Ser. B* 39 (1985), 353–367.

[4] S-F. Du, J. H. Kwak and R. Nedela, Classification of regular embeddings of hypercubes of odd dimension, *Discrete Math.* 307 (2007), 119–124.

[5] G. A. Jones, Automorphisms and regular embeddings of merged Johnson graphs, *European J. Combin.* 26 (2005), 417–435.

[6] Y. S. Kwon, New regular embeddings of n-cube, Q_n, *J. Graph Theory* 46 (2004), 297–312.

[7] N. L. Biggs, Automorphisms of imbedded graphs, *J. Combinatorial Theory Ser. B* 11 (1971), 132–138.

[8] N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures*, London Math. Soc. Lecture Note Series 33, Cambridge University Press, Cambridge, 1979.

[9] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 3rd ed., Springer-Verlag, Berlin—Heidelberg—New York, 1972.

[10] A. Grothendieck, Esquisse d'un programme, in *Geometric Galois Actions* 1, London Math. Soc. Lecture Note Ser. 242, Cambridge University Press, Cambridge, 1997, pp. 5–48. [English translation, pp. 243–283.]

[11] R. Nedela, M. Škoviera and A. Zlatoš, Regular embeddings of complete bipartite graphs, *Discrete Math.* 258 (2002), 379–381.

[12] J. H. Kwak and Y. S. Kwon, Regular orientable embeddings of complete bipartite graphs, *J. Graph Theory* 50 (2005), 105–122.

[13] G. A. Jones, R. Nedela and M. Škoviera, Complete bipartite graphs with a unique regular embedding, *J. Combinatorial Theory Ser. B*, to appear.

[14] J. S. Rose, *A Course in Group Theory*, Cambridge University Press, 1978.

[15] P. Erdős, Some asymptotic formulas in number theory, *J. Indian Math. Soc.* 12 (1948), 75–78.

[16] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Z.* 58 (1953), 243–264.

[17] G. A. Jones, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is an odd prime power, *European J. Combinatorics* 28 (2007), 1863–1875.

[18] S-F. Du, G. A. Jones, J. H. Kwak, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is a power of 2. I: Metacyclic case, *European J. Combinatorics*, 28 (2007), no. 6, 1595–1609.

[19] S-F. Du, G. A. Jones, J. H. Kwak, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is a power of 2. II: Non-metacyclic case, in preparation.

[20] H. Wielandt, Über das Produkt von paarweise vertauschbaren nilpotenten Gruppen, *Math. Z.* 55 (1951), 1–7.

[21] N. Itô, Über das produkt von zwei abelschen Gruppen, *Math. Z.* 62 (1955), 400–401.

[22] P. Hall, A note on soluble groups, *J. London Math. Soc.* 3 (1928), 98–105.

[23] G. A. Jones, Regular embeddings of complete bipartite graphs: classification and enumeration, preprint.

[24] P. Erdős and A. Rényi, Asymmetric graphs, *Acta Math. Acad. Sci. Hungary* 14 (1963), 295–315.

[25] R. Rado, Universal graphs and universal functions, *Acta Arith.* 9 (1964), 331–340.

[26] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts Series 45, Cambridge University Press, Cambridge, 1999.

[27] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics 163, Springer, New York, 1996.

[28] R. Nedela, private communication, April 2006.

[29] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* 244 (2002), 167–179.

[30] G. A. Jones, Maps on surfaces and Galois groups, *Math. Slovaca* 47 (1997), 1–33.

[31] G. A. Jones and D. Singerman, Belyĭ functions, hypermaps and Galois groups, *Bull. London Math. Soc.* 28 (1996), 561–590.

[32] S. K. Lando and A. K. Zvonkin, *Graphs on Surfaces and their Applications, Encyclopaedia of Mathematical Sciences*, 141, Springer-Verlag, Berlin, 2004.

[33] G. V. Belyĭ, Galois extensions of a maximal cyclotomic field (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* 43 (1979), 267–276, 479.

[34] B. Koeck, Belyi's theorem revisited, *Beiträge Algebra Geom.* 45 (2004), 253–265.

[35] J. Wolfart, *ABC* for polynomials, dessins d'enfants and uniformization—a survey, in *Elementare und analytische Zahlentheorie*, Schr. Wiss. Ges. Johann Wolfgang Goethe Univ. Frankfurt am Main, 20, Franz Steiner Verlag Stuttgart, Stuttgart, 2006, pp. 313–345.

[36] G. A. Jones, M. Streit and J. Wolfart, Galois action on families of generalised Fermat curves, *J. Algebra* 307 (2007), 829–840.

[37] G. A. Jones and M. Streit, Galois groups, monodromy groups and cartographic groups, in *Geometric Galois Actions* 2, London Math. Soc. Lecture Note Ser. 243, Cambridge University Press, Cambridge, 1997, pp. 25–65.

[38] A. Coste, G. A. Jones, M. Streit and J. Wolfart, Generalised Fermat hypermaps and Galois orbits, submitted, ArXiv math.AG/0606712.

[39] S. E. Wilson, Operators over regular maps, *Pacific J. Math.* 81 (1979), 559–568.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Separability properties of groups

Goansu Kim[1]
Yeungnam University, Kyongsan, Korea

C.Y. Tang[2]
University of Waterloo, Waterloo, Ontario, Canada

1 INTRODUCTION

Separability properties came from residual properties which, according to Gruenberg [23], were first suggested by P. Hall. In the wider applications of these concepts D. Solitar preferred using the term *separable*. Therefore, we define S-separability of a group as follows:

(1) If S is a subset of a group G, then we say G is S-*separable* if for each $g \in G\backslash S$ and $g \neq 1$, there exists a normal subgroup N_g, depending on g, of finite index in G such that in $\overline{G} = G/N_g$, $\overline{g} \notin \overline{S}$. That is S is closed under the profinite topology of G.

(2) If S is a group property, then we say G is S-*separable* if for each $g \in G$ and $g \neq 1$, there exists a normal subgroup N_g, depending on g, in G such that $\overline{G} = G/N_g$ has property S and $\overline{g} \neq 1$. This is also known as *residually* S.

The first result on S-separability is due to Magnus [37].

Theorem 1.1. *Free groups are nilpotently separable* (*or residually nilpotent*).

Theorem 1.2 (Hirsch [25]). *Polycyclic groups are* $\{1\}$-*separable.*

We note that $\{1\}$-separable groups are precisely the same class of groups as residually finite groups ($\mathcal{RF}$). It follows that:

Theorem 1.3. *Free groups are* $\{1\}$-*separable or residually finite.*

Residual finiteness is the most widely studied S-separable properties. Probably it is because we know more about finite groups than infinite groups. So by reducing infinite groups to their various finite images, we can use the properties of their finite images to derive the properties of the infinite groups involved. I believe this techniques could be used in other mathematical systems such as number theory, lattice theory, graph theory or ring theory etc. Nice applications have been found in group theory and topology. A good example of its application is in certain decision problems for finitely presented groups (*i.e.*, groups with finite number of generators and defining relations).

Dehn (1911 [18]) from topological consideration raised the following decision problems for finitely presented groups G:

(1) *Word Problem* (W.P.) Given a word w in G, is there an algorithm to decide whether $w = 1$?

[1] The first author was supported by KOSEF F01-2007-000-10151-0.

[2] The second author gratefully acknowledges the partial support by the Natural Science and Engineering Research Council of Canada, Grant No. A-4064.

AMS Subject Classification: Primary 20E26, 20E06; Secondary 20F34, 57M05.

(2) *Conjugacy Problem* (C.P.) Given two words w_1, w_2 in G, is there an algorithm to decide whether w_1 and w_2 are conjugate in G?

(3) *Isomorphism Problem* (I.P.) Given two groups G_1 and G_2, is there an algorithm to decide whether G_1 and G_2 are isomorphic?

W.P. and C.P. are obvious for abelian groups and free groups. However even for nilpotent groups and 1-relator groups, it is a different story. Magnus (1932 [36]) proved that W.P. is solvable for 1-relator groups. He then raised another problem:

(4) *Generalized Word Problem* (G.W.P.) He asked: Is there an algorithm to decide whether a word w in G is in a given subgroup of G?

To relate separability properties with some of the decision problems, we emphasize some special S-separabilities:

I. G is $\{1\}$*-separable*, *i.e.,* residually finite ($\mathcal{RF}$).

II. G is *subgroup separable* (s.s.), that is, G is S-separable for all subgroups S of G. In other words, S is closed in the profinite topology in G.

III. G is *conjugacy separable* (c.s.), that is, G is $\{x\}^G$-separable for each $x \in G$, where $\{x\}^G$ is the conjugacy class of x in G.

The following diagram illustrates their relationship. They are proved independently at different times by Malcev [38], McKinsey [39] and Mostowski [40].

$$\begin{tikzcd}
\text{c.s.} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{C.P.} \arrow[d, Rightarrow] \\
\mathcal{RF} \arrow[r, Rightarrow] & \text{W.P.} \\
\text{s.s.} \arrow[r, Rightarrow] \arrow[u, Rightarrow] & \text{G.W.P.} \arrow[u, Rightarrow]
\end{tikzcd}$$

Note: None of the implications can be reversed.

Other interesting separability properties are:

HxK-separability, where $x \in G$ and H, K are subgroups of G (double coset separability).
C-separability (or π_c), where C is a cyclic subgroup of G.
$H_1 H_2 \cdots H_n$*-separability*, where H_i are subgroups of G (product separability).

2 {1}-SEPARABLE OR RESIDUALLY FINITE GROUPS ($\mathcal{RF}$)

This is the most widely studied S-separable groups. They include finitely generated abelian groups, nilpotent groups, polycyclic groups, free groups, direct and free products of $\mathcal{RF}$ groups. However, solvable groups and generalized free products (g.f.p.) of $\mathcal{RF}$ groups need not be $\mathcal{RF}$. Gruenberg [23] constructed a wreath product of S_3 with an infinite cyclic group which is not $\mathcal{RF}$. Ruth Camm [17] constructed an infinite simple group using g.f.p. of two free groups. However, with suitable restriction on the amalgamated subgroup we can get $\mathcal{RF}$ from g.f.p.

Note: In general, even infinitely generated abelian groups need not be $\mathcal{RF}$. Examples are: (1) Z_{p^∞}, (2) the additive group of rationals modulo 1. Thus throughout the following discussion we assume our groups are finitely generated.

One of the basic result in the study of residually finite generalized free products is due to G. Baumslag [12].

Theorem 2.1. *Generalized free products of two finite groups are* $\mathcal{RF}$.

This is because free-by-finite groups are $\mathcal{RF}$, since $\mathcal{RF}$-by-finite groups are $\mathcal{RF}$. Using this result Baumslag proved:

Theorem 2.2 ([12]). *Generalized free products of two nilpotent groups or free groups amalgamating a cyclic subgroup are $\mathcal{RF}$.*

The proofs are quite long. Later Allenby and Tang [7] introduced the concept of potency making the proof of Theorem 2.2 quite simple.

Definition 2.3. Let $1 \neq x \in G$. If for each integer $n > 0$, there exists $N_n \lhd_f G$ such that, in $\overline{G} = G/N_n$, $\|\overline{x}\| = n$, then G is said to be $\langle x \rangle$*-potent* (briefly $\langle x \rangle$-pot). If G is $\langle x \rangle$-pot for all $x \in G$, then G is said to be *potent*.

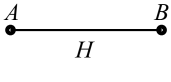
Theorem 2.4 (Allenby and Tang [7]). *Generalized free products of potent and cyclic subgroup separable (π_c) groups amalgamating a cyclic subgroup are $\mathcal{RF}$.*

Proof. (Sketch) Let $G = A *_H B$ where A, B are potent, π_c and $H = \langle h \rangle$. In general, elements of G are of the form $a_1 b_1 \cdots a_n b_n$ where $a_i \in A \backslash H$, $b_i \in B \backslash H$ with a_1 or b_n possibly equal to 1. To apply Theorem 2.1, we need to map G to $\overline{G} = \overline{A} *_{\overline{H}} \overline{B}$ where $\overline{A}, \overline{B}$ are finite. We illustrate with a simple case $x = ab$ where $a \in A \backslash H$ and $b \in B \backslash H$. Since A, B are π_c, there exist normal subgroups $L_a \lhd_f A$ and $M_b \lhd_f B$ such that $a \notin L_a H$ and $b \notin M_b H$. Let $L_a \cap H = \langle h^\alpha \rangle$ and $M_b \cap H = \langle h^\beta \rangle$. Let $n = \alpha\beta$. Since A, B are potent, there exist $X_A \lhd_f A$ and $Y_B \lhd_f B$ such that $X_A \cap H = \langle h^n \rangle$ and $Y_B \cap H = \langle h^n \rangle$. Let $N_a = L_a \cap X_A$ and $N_b = M_b \cap Y_B$. Then $N_a \cap H = N_b \cap H = \langle h^n \rangle$ with $a \notin N_a H$ and $b \notin N_b H$. Let $\overline{A} = A/N_a$ and $\overline{B} = B/N_b$. Then we can form $\overline{G} = \overline{A} *_{\overline{H}} \overline{B}$ since $|\overline{H}| = n$ in both $\overline{A}$ and $\overline{B}$. Moreover $\overline{a}, \overline{b} \notin \overline{H}$, whence $\overline{x} = \overline{a}\overline{b} \neq 1$. Since $\overline{A}, \overline{B}$ are finite, by Theorem 2.1, $\overline{G}$ is $\mathcal{RF}$. Hence G is $\mathcal{RF}$. □

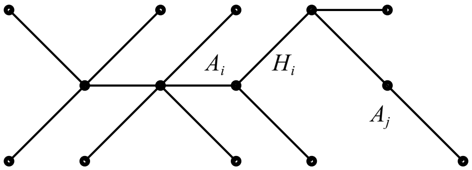
Since finitely generated nilpotent groups and free groups are both potent and π_c, we have:

Corollary 2.5. *Generalized free products of two finitely generated nilpotent groups or free groups or combination of these groups amalgamating a cyclic subgroup are $\mathcal{RF}$. In particular, surface groups are $\mathcal{RF}$.*

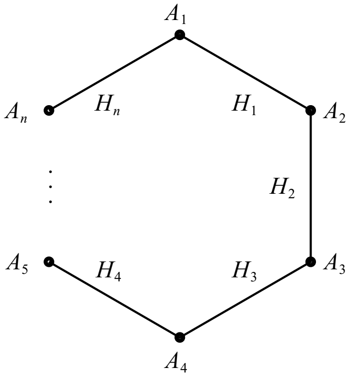
Following Serre [45], we represent generalized free products of groups by graphs. Thus $G = A *_H B$ is represented by the graph:



where A, B are represented by the vertices A, B called the *vertex groups*. The amalgamated subgroup H is represented by the edge H called the *edge group*. We can extend this to arbitrary graphs.



If the graph is a tree then we can call it a *tree product*. If the graph is a polygon then we call it a *polygonal product* such as:



Problem 1. *Are tree products or polygonal products of $\mathcal{RF}$ groups $\mathcal{RF}$? In particular, are polygonal products of p-groups amalgamating cyclic subgroups $\mathcal{RF}$?*

In general the answer is *no*, unless we put suitable restrictions on the amalgamated subgroups, such as: (1) the edge subgroups of a vertex group intersect trivially; (2) edge groups are restricted to cyclic subgroups; (3) in the case of polygonal products, the number of vertex groups are ≥ 4.

Applying Theorem 2.4 and using induction, we can prove:

Theorem 2.6. *Tree products of finitely generated abelian groups amalgamating cyclic subgroups are $\mathcal{RF}$.*

This result was later generalized by Kim and Tang to other separability properties.

This is also true for tree products of free groups with cyclic amalgamations.

Theorem 2.7 (Allenby and Tang [9]). *Polygonal products of finitely generated abelian groups amalgamating cyclic trivial intersecting subgroups are $\mathcal{RF}$.*

Allenby and Tang [9] gave an example of polygonal product of 4 nilpotent groups amalgamating cyclic subgroups which is not $\mathcal{RF}$.

Example 1. Let $A_i = \langle a_i, b_i; [a_i, b_i, a_i] = [a_i, b_i, b_i] = 1\rangle$, $i = 1, \ldots, 4$. Clearly A_i is nilpotent of class 2. Form the polygonal product P with $a_{i+1}^2 = b_i^{-1}a_i^3 b_i$, where $a_5 = a_1$. Then P is not $\mathcal{RF}$.

Note: The amalgamated subgroups are not maximal cyclic.

Theorem 2.8 (Kim and Tang [28]). *Polygonal products of nilpotent groups amalgamating trivial intersecting maximal cyclic subgroups are $\mathcal{RF}$.*

Problem 2. *Is this true for polygonal products of free groups?*

Definition 2.9. Let A be a group. Let $G = \langle A, t; t^{-1}Ht = K\rangle$, where $\phi : H \to K$ is an isomorphism and $t^{-1}ht = \phi(h)$, $h \in H$. Then G is called an *HNN-extension* of A by t with *associated subgroups* and H and K.

In general, HNN-extensions of $\mathcal{RF}$ groups need not be $\mathcal{RF}$.

Example 2. $\langle a, t; t^{-1}a^2t = a^3\rangle$, the Baumslag-Solitar groups [14], is not $\mathcal{RF}$.

Kim and Tang [33] characterized $\mathcal{RF}$ HNN extensions of nilpotent groups with cyclic associated subgroups.

Theorem 2.10. *Let A be a finitely generated nilpotent group. Let $h, k \in A$ be of infinite order such that $\langle h\rangle \cap \langle k\rangle \neq 1$. Then $G = \langle A, t; t^{-1}ht = k\rangle$ is $\mathcal{RF}$ if and only if one of the following holds:*

(1) *If $A = \langle b\rangle$, $h = b^\alpha$ and $k = b^\beta$ then $|\alpha| = 1$ or $|\beta| = 1$ or $\alpha \pm \beta = 0$.*
(2) *If A is not cyclic then $h^\delta = h^{\pm\delta}$ for some $\delta > 0$.*

In the case of 1-relator groups, Baumslag showed that $G = \langle a, b; (a^{-1}b^l ab^m)^k = 1\rangle$, where l, k, m are coprime, is $\mathcal{RF}$.

Baumslag's Conjecture [13]: $G = \langle a_1, \ldots, a_n; r^k = 1\rangle$ is $\mathcal{RF}$, where $k > 1$ and r is a word on the a_i's.

This conjecture is still open.

The best results so far are:

(1) $G = \langle a, b; (a^\alpha b^\beta a^\delta b^\delta)^k = 1\rangle$ is $\mathcal{RF}$ for $k > 1$. (Allenby and Tang [8])
(2) $G = \langle a_1, \ldots, a_n; r^k = 1\rangle$ is $\mathcal{RF}$ if $k > 8\|r\|$. (D. Wise [50])

For a long time it was an open question whether knot groups are $\mathcal{RF}$. Thurston [48] proved it to be $\mathcal{RF}$. He asked what kind of separability properties *Kleinian groups* have. Not much is known although *Fuchsian groups* have nice separability properties. In fact they are conjugacy separable whence $\mathcal{RF}$. They are given by:

$$G = \langle a_1, b_1, \ldots, a_n, b_n, c_1, \ldots, c_r, d_1, \ldots, d_s;\ d_i^{\alpha_i} = 1, c_1 \cdots c_r d_1 \cdots d_s \textstyle\prod_{i=1}^n [a_i, b_i] = 1\rangle.$$

In particular, G is $\mathcal{RF}$. If $n = r = 0$ and $s = 3$, G reduces to a triangle group:

$$G = \langle d_1, d_2;\ d_1^{\alpha_1} = d_2^{\alpha_2} = (d_1d_2)^{\alpha_3} = 1\rangle.$$

Hence triangle groups are $\mathcal{RF}$. This can also be seen in another way: Triangle groups are either finite or finite extensions of surface groups. Since surface groups are $\mathcal{RF}$ and finite extensions of $\mathcal{RF}$ groups are $\mathcal{RF}$, triangle groups are $\mathcal{RF}$. Since $\mathcal{RF}$ of triangle groups is of interest to Combinatorics, maybe other separability properties, such as, subgroup separability could be of interest to Combinatorics too.

3 SUBGROUP SEPARABILITY (S.S.)

It is easy to see finitely generated abelian groups are subgroup separable. The first nontrivial result on subgroup separability is due to M. Hall.

Theorem 3.1 (M. Hall [24]). *Free groups are subgroup separable.*

Theorem 3.2 (Malcev [38]). *Polycyclic groups are subgroup separable.*

Topologists are interested in subgroup separability because it is related to questions of embeddability of equivariant subspaces in their regular covering spaces. Many of subgroup separable groups studied are related to 3-manifold groups.

Theorem 3.3 (P. Scott [44]). *Surface groups are subgroup separable.*

Now finite extension of subgroup separable groups are again subgroup separable. Since Fuchsian groups contain surface groups as subgroups of finite indices, it follows that Fuchsian groups are subgroup separable.

Since surface groups can be considered as generalized free products amalgamating a cyclic subgroup, Brunner, Burns and Solitar [16] generalized Scott's result by proving:

Theorem 3.4. *Generalized free products of two free groups amalgamating a cyclic subgroup are subgroup separable.*

Niblo [41] generalized this result to:

Theorem 3.5. *Generalized free products of two Fuchsian groups amalgamating a cyclic subgroup are subgroup separable.*

Niblo also showed that Seifert 3-manifold groups [42] are subgroup separable.

Another generalization of Theorem 3.4 is:

Theorem 3.6 (Allenby and Tang [10]). *Generalized free products of two free-by-finite groups amalgamating a cyclic subgroup are subgroup separable.*

This answers a question raised by G. Rosenberger whether groups of F-type are subgroup separable, where *groups of F-type* are defined by:

$$G = \langle a_1, \ldots, a_m, b_1, \ldots, b_n;\ a_i^{\alpha_i} = 1, b_j^{\beta_j} = 1, uv = 1\rangle,$$

where u, v are words on a_i's and b_j's respectively and orders of u, v are infinite.

Note: A group of F-type is a 1-relator product of cyclics. They are generalizations of Fuchsian groups. We observe that $G = A \underset{u=v^{-1}}{*} B$, where

$$A = \langle a_1, \ldots, a_m;\ a_i^{\alpha_i} = 1\rangle = \langle a_1;\ a_1^{\alpha_i} = 1\rangle * \cdots * \langle a_m;\ a_m^{\alpha_m} = 1\rangle,$$

$$B = \langle b_1, \ldots, b_n;\ b_i^{\beta_i} = 1\rangle = \langle b_1;\ b_1^{\beta_i} = 1\rangle * \cdots * \langle b_n;\ b_n^{\beta_n} = 1\rangle.$$

Since A and B are free products of cyclic groups, A and B are free-by-finite groups. Thus, by Theorem 3.6, groups of F-type are subgroup separable. In fact with more work we can prove:

Theorem 3.7 (Allenby and Tang [10]).

$$G = \langle a_1, \ldots, a_m, b_1, \ldots, b_n;\ a_i^{\alpha_i} = 1, b_j^{\beta_j} = 1, (uv)^t = 1\rangle, \quad t \geq 1$$

where u, v are words on a_i's and b_j's respectively, are subgroup separable.

Not much is known about subgroup separability of HNN-extensions of subgroup separable groups. Stebe proved the following result about π_c groups:

Theorem 3.8 (Stebe [46]). *$\langle a, t;\ t^{-1}a^{\gamma}t = a^{\delta}\rangle$ is π_c iff $\gamma = \pm\delta$.*

Theorem 3.9 (Kim and Tang [33]). *Let A be π_c and $h, k \in A$ be of infinite order. Then $G = \langle A, t;\ t^{-1}ht = k\rangle$ is π_c iff A is quasi-regular at $\{h, k\}$.*

Definition 3.10. Let A be a group and $h, k \in A$ be of infinite order. Then A is said to be quasi-regular at $\{h, k\}$ if for each $n > 0$, there exists an integer $\lambda_n > 0$ and $N_n \lhd_f A$ such that $N_n \cap \langle h \rangle = \langle h^{n\lambda_n} \rangle$ and $N_n \cap \langle k \rangle = \langle k^{n\lambda_n} \rangle$.

As a result, we have:

Theorem 3.11 (Kim and Tang [33]). *Let A be a finitely generated nilpotent group and $h, k \in Z(A)$ be of infinite order. Then $G = \langle A, t; t^{-1}ht = k \rangle$ is π_c iff $\langle h \rangle \cap \langle k \rangle = 1$ or $h^\delta = k^{\pm\delta}$ for some $\delta > 0$.*

The need of quasi-regularity is crucial as seen by the following example. Without quasi-regularity HNN-extensions can be not $\mathcal{RF}$.

Example 3 (Kim and Tang [33]). Let $A = \langle a, b; [a, b, a] = [a, b, b] = 1 \rangle$. Then A is a free nilpotent group of class 2 with $[a, b] \in Z(A)$. This makes calculation easy. Write $[a, b] = z$. Let $h = a^2z^2$ and $k = a^3z^2$. Then $\langle h \rangle \cap \langle k \rangle = 1$. Let $g = [t^{-1}azt, az]$. Then $g \neq 1$. Suppose G is $\mathcal{RF}$. Then there exists $N \lhd_f G$ such that $g \notin N$. Let $N \cap \langle h \rangle = \langle h^n \rangle$. Then, $h^n = (a^2z^2)^n = a^{2n}z^{2n} \in N$ and $k^n = (a^3z^2)^n = a^{3n}z^{2n} \in N$. Hence $a^n \in N$. If n is even, say, $n = 2m$, then $h^m = (a^2z^2)^m = a^{2m}z^{2m} = a^n[a, b]^n = a^n[a^n, b] \in N$. Contradicting $N \cap \langle h \rangle = \langle h^n \rangle$. Hence n is odd. This implies that there exist integers r, s such that $rn + 2s = 1$. Let $\overline{G} = G/N$. Then in $\overline{G}$, $\overline{a}^n = \overline{z}^n = 1$. Thus $\overline{t^{-1}azt} = \overline{t}^{-1}(\overline{az})^{rn+2s}\overline{t} = \overline{t}^{-1}\overline{h}^s\overline{t} = \overline{k}^s$. This implies that $\overline{g} = [\overline{t^{-1}azt}, \overline{az}] = [\overline{k}^s, \overline{az}] = 1$. But this contradicts the choice of N that $g \notin N$. Hence G is not residually finite. The reason for G to be not $\mathcal{RF}$ is that A is not quasi-regular at $\{h, k\}$.

In this case for integer 2, there does not exist any integer λ and $N \lhd_f A$ such that $N \cap \langle h \rangle = \langle h^{2\lambda} \rangle$ and $N \cap \langle k \rangle = \langle k^{2\lambda} \rangle$.

Suppose there exist an integer λ and $N \lhd_f A$ such that $N \cap \langle h \rangle = \langle h^{2\lambda} \rangle$ and $N \cap \langle k \rangle = \langle k^{2\lambda} \rangle$. Then $h^{2\lambda} = (a^2z^2)^{2\lambda} = a^{4\lambda}z^{4\lambda}$ and $k^{2\lambda} = (a^3z^2)^{2\lambda} = a^{6\lambda}z^{4\lambda}$. This implies $a^{2\lambda} \in N$. Thus, $z^{2\lambda} = [a, b]^{2\lambda} = [a^{2\lambda}, b] = a^{-2\lambda}b^{-1}a^{2\lambda}b \in N$. It follows that $h^\lambda = (a^2z^2)^\lambda = a^{2\lambda}z^{2\lambda} \in N$, contradicting $N \cap \langle h \rangle = \langle h^{2\lambda} \rangle$. Hence A is not quasi-regular at $\{h, k\}$.

Problem 3. *Characterize pairs of quasi-regular elements in free groups or nilpotent groups.*

4 CONJUGACY SEPARABILITY (C.S.)

Proving conjugacy separability is much more difficult than proving residual finiteness or subgroup separability. This is similar to the fact that solving the conjugacy problem is much more difficult than solving the word problem. Magnus solved the word problem for 1-relator groups in 1932 [36]. So far the conjugacy problem for 1-relator groups is not yet solved. Finitely generated nilpotent groups have been known to have solvable word problem since 1946 (Hirsch [25] and McKinsey [39]). But the conjugacy problem for the nilpotent groups was not solved until 1965, when Blackburn [15] proved that these groups are conjugacy separable.

A basic result for conjugacy separability of generalized free products of groups was proved by Dyer [19].

Theorem 4.1. *Let $G = A *_H B$, where A, B are conjugacy separable and H is finite. Then G is conjugacy separable.*

Applying this result Dyer [19] proved:

Theorem 4.2. *Generalized free products of two nilpotent groups or free groups amalgamating a cyclic subgroup are conjugacy separable.*

Kim and Tang [31] generalized this result to:

Theorem 4.3. *Let $G = A *_H B$, where A and B are conjugacy separable finite extensions of nilpotent separable groups A_1 and B_1. If A_1 and B_1 are conjugacy separable then G is conjugacy separable.*

Theorem 4.4 (Fine and Rosenberger [20]). *Fuchsian groups are conjugacy separable.*

They also proved that groups of F-type are conjugacy separable [21]. Since groups of F-type are generalized free products of two free products of cyclic groups, which are free-by-finite, amalgamating a cyclic subgroup, by Theorem 4.3, we have:

Theorem 4.5 ([21, 31]). *Groups of F-type are conjugacy separable.*

In 1982, Tang asked in the Kourovka Note Book whether generalized free products of polycyclic groups amalgamating a cyclic subgroup are conjugacy separable? This was answered positively by Ribes, Segal and Zalesskii [43].

Theorem 4.6. *Generalized free products of polycyclic-by-finite groups amalgamating a cyclic subgroup are conjugacy separable.*

Problem 4. *Are generalized free products of two groups of F-type amalgamating a cyclic subgroup conjugacy separable?*

For linear groups, Stebe [47] showed $GL_2(Z), SL_2(Z), GL_n(Z_p), SL_n(Z_p)$ are conjugacy separable. Wilson and Zalesskii [49] showed that $PSL_2(Q(\sqrt{-d}))$ are conjugacy separable for $d = 1, 2, 7, 11$.

For tree products, Kim and Tang [35] proved the following:

Theorem 4.7. *Let G be a tree product of central subgroup separable and conjugacy separable groups amalgamating central edge groups. Then G is conjugacy separable. In particular if G is a tree product of polycyclic groups amalgamating central edge groups then G is conjugacy separable.*

The group for the linkage of a torus knot with a cycle is presented as

$$\langle x, y : [x, y] \rangle \underset{x^n y^m = z^m}{*} \langle z \rangle.$$

And the group for the linkage of a torus knot with cycles within and outside the torus is presented as

$$\langle x, y : [x, y] \rangle \underset{x^n y^m = a^m b^n}{*} \langle a, b : [a, b] \rangle.$$

The groups of linkages of torus knots are presented as

$$\langle a \rangle \underset{a^{n_1} = x_1^{\delta_1}}{*} \langle x_1, y_1 : [x_1, y_1] \rangle \underset{x_1^{\alpha_1} y_1^{\beta_1} = x_2^{\delta_2}}{*} \langle x_2, y_2 : [x_2, y_2] \rangle \underset{x_2^{\alpha_2} y_2^{\beta_2} = x_3^{\delta_3}}{*} \cdots$$
$$\cdots \underset{x_{n-1}^{\alpha_{n-1}} y_{n-1}^{\beta_{n-1}} = x_n^{\delta_n}}{*} \langle x_n, y_n : [x_n, y_n] \rangle \underset{x_n^{\alpha_n} y_n^{\beta_n} = x_{n+1}^{\delta_{n+1}}}{*} \langle x_{n+1} \rangle .$$

It follows that the groups of linkages of torus knots are conjugacy separable.

Theorem 4.7 also holds for polygonal products of central subgroup separable and conjugacy separable groups amalgamating trivially intersecting central edge groups [34].

In the case of HNN-extensions, we have:

Theorem 4.8 (Kim and Tang [29]). *Let A be a finitely generated abelian group. Let $h, k \in A$ be of infinite order. Then the HNN-extension $G = \langle A, t : t^{-1}ht = k \rangle$ is conjugacy separable iff one of the followings holds:*

(1) *If $A = \langle a \rangle$, $h = a^{\alpha}$ and $k = a^{\beta}$, then $|\alpha| = 1$ or $|\beta| = 1$ or $\alpha \pm \beta = 0$.*
(2) *If A is not cyclic, then $\langle h \rangle \cap \langle k \rangle = 1$ or $h^n = k^{\pm n}$ for some $n > 0$.*

For a more general base group A, we have:

Theorem 4.9 (Kim and Tang [32]). *Let A be π_c, conjugacy separable, c-quasi-regular and double coset separable at $\{h, k\}$. If A is cyclic conjugacy separable for $\langle h \rangle$ and $\langle k \rangle$, then $G = \langle A, t : t^{-1}ht = k \rangle$ is conjugacy separable.*

Here c-quasi-regular is defined by:

Definition 4.10. Let A be a group and let $h, k \in A$ be of infinite order. Then A is said to be *c-quasi-regular at* $\{h, k\}$ if $\langle h \rangle \cap \langle k \rangle = 1$ and there exists an integer α such that, for a fixed integer $m > 0$ and for each integer $\epsilon > 0$, there exist an integer $\lambda_\epsilon > 0$ and $N_\epsilon \lhd_f A$ such that: (1) $N_\epsilon \cap \langle h \rangle = \langle h^{\epsilon\lambda_\epsilon} \rangle$ and $N_\epsilon \cap \langle k \rangle = \langle k^{\epsilon\lambda_\epsilon} \rangle$, (2) in $\overline{A} = A/N_\epsilon$, $\langle \overline{h} \rangle \cap \langle \overline{k} \rangle = 1$, (3) if $\overline{h}^{\alpha m} \sim_{\overline{A}} \overline{h}^{j}$ then $\overline{h}^{j} = \overline{h}^{\pm\alpha m}$, (4) if $\overline{k}^{\alpha m} \sim_{\overline{A}} \overline{k}^{j}$ then $\overline{k}^{j} = \overline{k}^{\pm\alpha m}$, (5) if $\overline{h}^{i} \sim_{\overline{A}} \overline{k}^{j}$ then $\overline{h}^{i} = \overline{k}^{j} = 1$.

In the case of 1-relator groups, the best known result is:

Theorem 4.11 (Kim, McCarron and Tang [26]). *$G = \langle a, b; (a^{-\alpha} b^{\beta} a^{\alpha} b^{\gamma})^k = 1 \rangle$, $k > 1$, is conjugacy separable. For $k = 1$, G is conjugacy separable iff $|\beta| = 1$ or $|\gamma| = 1$ or $\beta \pm \gamma = 0$.*

Problem 5. *Are 1-relator groups with torsion conjugacy separable?*

In [4], Allenby, Kim and Tang proved that most of the Seifert 3-manifold groups are conjugacy separable.

5 OUTER AUTOMORPHISM GROUPS

Baumslag [11] proved that automorphism groups of finitely generated $\mathcal{RF}$ groups are $\mathcal{RF}$. Thus it is natural to ask whether outer automorphism groups of finitely generated $\mathcal{RF}$ groups are $\mathcal{RF}$. D. Wise [51] gave an example of a finitely generated $\mathcal{RF}$ group G such that $Out(G)$ is not $\mathcal{RF}$. Both group theorists and topologists are interested in the outer automorphism groups of the fundamental groups of surfaces and 3-manifolds because of their relation to mapping class groups (MCG).

Theorem 5.1 (Grossman [22]). *Let S_k be the fundamental group of an orientable surface group of genus k. Then $Out(S_k)$ is $\mathcal{RF}$.*

Since MCG of surfaces are isomorphic to Out(surface groups), it follows that MCG of orientable surface groups are $\mathcal{RF}$. This prompt A. Gaglione to ask whether MCG of non-orientable surfaces are $\mathcal{RF}$? Allenby, Kim and Tang [2] gave a positive answer to this question. We need the following results:

Theorem 5.2 (Grossman [22]). *Let G be a finitely generated, conjugacy separable group. If G has Property E. Then $Out(G)$ is $\mathcal{RF}$.*

By *Property E*, we mean every *conjugating endomorphism*, *i.e.,* the endomorphism $\alpha : G \to G$ satisfying $\alpha(g) = k_g^{-1} g k_g$ for $g \in G$, where k_g depends on g, is an *inner automorphism* of G.

Theorem 5.3 (Allenby, Kim and Tang [5]). *Let $G = A *_H B$, where $A \neq H \neq B$. Suppose the following conditions hold:*

(1) *H is malnormal in A and B.*
(2) *There exists $a \in A$ such that (i) $\{a\}^A \cap H = \emptyset$ and (ii) if $u^{-1}au = h'ah$, where $u \in A$ and $h', h \in H$, then $h' = h^{-1}$.*
Then G has Property E.

A subgroup H of a group G is said to be *malnormal* in G if, for all $g \in G \backslash H, g^{-1}Hg \cap H = 1$. An interesting corollary of Theorem 5.3 is:

Corollary 5.4. *Any nontrivial free products of groups have Property E.*

Now the fundamental groups of orientable and non-orientable surfaces are respectively given by:

$$S_k = \langle a_1, \dots, a_k, b_1, \dots, b_k;\ \prod_{i=1}^{k} [a_i, b_i] = 1 \rangle, \tag{5.1}$$

$$N_k = \langle a_1, \dots, a_k;\ a_1^2 \cdots a_k^2 = 1 \rangle. \tag{5.2}$$

It is easy to see that both (5.1) and (5.2), except for a few cases which can be taken care of individually, are generalized free products of two free groups amalgamating a maximal cyclic subgroup. This means the amalgamated subgroup is malnormal in both of the free factors. Hence by Theorem 4.2, 5.2, 5.3 we have:

Theorem 5.5 (Allenby, Kim and Tang [2]). *Outer automorphism groups of surface groups are $\mathcal{RF}$.*

Corollary 5.6. *Mapping class groups of orientable and non-orientable surfaces are $\mathcal{RF}$.*

In fact with more work we can show:

Theorem 5.7 (Allenby, Kim and Tang [1,6]). *Almost all Seifert 3-manifold groups have $\mathcal{RF}$ outer automorphism groups.*

Recall groups of F-type are of the form:

$$G = \langle a_1, \dots, a_m, b_1, \dots, b_n;\ a_i^{\alpha_i} = 1, b_j^{\beta_j} = 1, uv = 1 \rangle,$$

where u, v are words on a_i's and b_j's respectively. They can be considered as 1-relator products of cycles with the relation $uv = 1$. Let a group G of F-type. We call G to be a F_1-type, if $\langle u \rangle$, $\langle v \rangle$ are maximal cycles on $\langle a_1, \dots, a_m \rangle$, $\langle b_1, \dots, n_n \rangle$, respectively. Thus groups of F_1-type can be considered as generalized free products of two free products of cycles amalgamating the maximal cyclic subgroups $\langle u \rangle$ and $\langle v \rangle$ which are malnormal in their respective free factors. Hence, by Theorem 5.3, groups of F_1-type have Property E. As we have seen earlier groups of F-types are conjugacy separable, we have:

Theorem 5.8. *Let G be a group of F_1-type. Then Out(G) is $\mathcal{RF}$.*

Recent results showed that outer automorphism groups of tree products and polygonal products of finitely generated abelian groups are $\mathcal{RF}$.

Applying Theorem 4.11, Kim and Tang [27] recently proved the following result for 1-relator groups:

Theorem 5.9. *Let $G = \langle a, b; (a^{-\alpha} b^{\beta} a^{\alpha} b^{\gamma})^k = 1 \rangle, \quad k > 1$. Then Out$(G)$ is $\mathcal{RF}$.*

This raises the following problems:

Problem 6. *Are the outer automorphism groups of conjugacy separable* 1*-relator groups $\mathcal{RF}$? More generally, are the outer automorphism groups of conjugacy separable groups $\mathcal{RF}$?*

The answer to the latter question is probably negative. But we need a definite example.

REFERENCES

[1] R.B.J.T. Allenby, G. Kim, and C.Y. Tang. Outer automorphism groups of non-orientable seifert 3-manifold groups. Preprint.

[2] R.B.J.T. Allenby, G. Kim, and C.Y. Tang. Residual finiteness of outer automorphism groups of certain pinched 1-relator groups. *J. Algebra*, 246(2):849–858, 2001.

[3] R.B.J.T. Allenby, G. Kim, and C.Y. Tang. On the residual finiteness of Out$(\pi_1(M))$ of certain Seifert manifolds. *Algebra Colloq.*, 10(2):121–126, 2003.

[4] R.B.J.T. Allenby, G. Kim, and C.Y. Tang. Conjugacy separability of certain seifert 3-manifold groups. *J. Algebra*, 285(2):481–507, 2005.

[5] R.B.J.T. Allenby, G. Kim, and C.Y. Tang. Residual finiteness of outer automorphism groups of finitely generated non-triangle fuchsian groups. *Internat. J. Algebra Comput.*, 15(1):59–72, 2005.

[6] R.B.J.T. Allenby, G. Kim, and C.Y. Tang. Outer automorphism groups of certain orientable seifert 3-manifold groups. In *Contemp. Math., Amer. Math. Soc.*, 421:15–22, 2006.

[7] R.B.J.T. Allenby and C.Y. Tang. The residual finiteness of some one-relator groups with torsion. *J. Algebra*, 71(1):132–140, 1981.

[8] R.B.J.T. Allenby and C.Y. Tang. Residually finite one-relator groups with torsion. *Arch. Math.*, 37:97–105, 1981.

[9] R.B.J.T. Allenby and C.Y. Tang. On the residual finiteness of certain polygonal products. *Canad. Math. Bull.*, 32(1):11–17, 1989.

[10] R.B.J.T. Allenby and C.Y. Tang. Subgroup separability of generalized free products of free-by-finite groups. *Canad. Math. Bull.*, 36(4):385–389, 1993.

[11] G. Baumslag. Automorphism groups of residually finite groups. *J. London Math. Soc.*, 38:117–118, 1963.

[12] G. Baumslag. On the residual finiteness of generalized free products of nilpotent groups. *Trans. Amer. Math. Soc.*, 106:193–209, 1963.

[13] G. Baumslag. Residually finite one-relator groups. *Bull. Amer. Math. Soc.*, 73:618–620, 1967.

[14] G. Baumslag and D. Solitar. Some two-generator one-relator non-Hopfian groups. *Bull. Amer. Math. Soc.*, 38:199–201, 1962.

[15] N. Blackburn. Conjugacy in nilpotent groups. *Proc. Amer. Math. Soc.*, 16:143–148, 1965.

[16] A.M. Brunner, R.G. Burns, and D. Solitar. The subgroup separability of free products of two free groups with cyclic amalgamation. *Contemp. Math., Amer. Math. Soc.*, 33:90–115, 1984.

[17] R. Camm. Simple free products. *J. London Math. Soc.*, 28:66–76, 1953.

[18] M. Dehn. Uber unendliche diskontinuerliche gruppen. *Math. Ann.*, 71:116–144, 1912.

[19] J.L. Dyer. Separating conjugates in amalgamated free products and HNN extensions. *J. Austral. Math. Soc. Ser. A*, 29(1):35–51, 1980.

[20] B. Fine and G. Rosenberger. Conjugacy separability of Fuchsian groups and related questions. *Contemp. Math., Amer. Math. Soc.*, 109:11–18, 1990.

[21] B. Fine and G. Rosenberger. *Groups of* F*-type: Reflections and Extensions*. In *Group Theory Proc. of the Biennial Ohio State-Dennison Conference*, pages 92–127. World Sci. Pub. Co., Singapore, 1993.

[22] E.K. Grossman. On the residual finiteness of certain mapping class groups. *J. London Math. Soc. (2)*, 9:160–164, 1974.

[23] K.W. Gruenberg. Residual properties of infinite soluble groups. *Proc. London Math. Soc. (3)*, 7:29–62, 1957.

[24] M. Hall, Jr. Coset representations in free groups. *Trans. Amer. Math. Soc.*, 67:421–432, 1949.

[25] K.A. Hirsch. On infinite soluble groups III. *Proc. London Math. Soc. (2)*, 44:184–194, 1946.

[26] G. Kim, J. McCarron, and C.Y. Tang. Adjoining roots to conjugacy separable groups. *J. Algebra*, 176(2):327–345, 1995.

[27] G. Kim and C.Y. Tang. Outer automorphism groups of certain 1-relator groups. Preprint.

[28] G. Kim and C.Y. Tang. On the residual finiteness of polygonal products of nilpotent groups. *Canad. Math. Bull.*, 35(3):390–399, 1992.

[29] G. Kim and C.Y. Tang. Conjugacy separability of HNN-extensions of abelian groups. *Arch. Math.*, 67:353–359, 1996.

[30] G. Kim and C.Y. Tang. A criterion for the conjugacy separability of amalgamated free products of conjugacy separable groups. *J. Algebra*, 184:1052–1072, 1996.

[31] G. Kim and C.Y. Tang. Conjugacy separability of generalized free products of finite extensions of residually nilpotent groups. In *Group Theory (Proc. of the '96 Beijing Int'l Symposium)*, pages 10–24. Springer-Verlag, 1998.

[32] G. Kim and C.Y. Tang. A criterion for the conjugacy separability of certain HNN-extensions of groups. *J. Algebra*, 222:574–594, 1999.

[33] G. Kim and C.Y. Tang. Cyclic subgroup separability of HNN-extensions with cyclic associated subgroups. *Canad. Math. Bull.*, 42(3):335–343, 1999.

[34] G. Kim and C.Y. Tang. Separability properties of certain polygonal products of groups. *J. Korean Math. Soc.*, 39(3):461–494, 2002.

[35] G. Kim and C.Y. Tang. Separability properties of certain tree products of groups. *J. Algebra*, 251:323–349, 2002.

[36] W. Magnus. Das Identitäts problem für Gruppen mit einer definierenden Relation. *Math. Ann.*, 106:295–307, 1932.

[37] W. Magnus. Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. *Math. Ann.*, 111:259–280, 1935.

[38] A.I. Mal'cev. Homomorphisms of finite groups. *Ivanov Gos. Ped. Inst. Učen. Zap. Uchen. Zap. Karel. Ped. Inst. Ser. Fiz.-Mat. Nauk*, 18:49–60, 1958.

[39] J.C.C. MeKinsey. The decision problem for some classes of sentences without quantifiers. *J. Symb. Logic*, 8:61–76, 1943.

[40] A.W. Mostowski. On the decidability of some problems in special classes of groups. *Fund. Math.*, 59:123–135, 1966.

[41] G.A. Niblo. H.N.N. extensions of a free group by Z which are subgroup separable. *Proc. London Math. Soc.*, 61:18–32, 1990.

[42] G.A. Niblo. Separability properties of free groups and surface groups. *J. Pure and Appl. Algebra*, 78:77–84, 1992.

[43] L. Ribes, D. Segal, and P.A. Zalesskii. Conjugacy separability and free products of groups with cyclic amalgamation. *J. London Math. Soc.*, 57(3):609–628, 1998.

[44] P. Scott. Subgroups of surface groups are almost geometric. *J. London Math. Soc.*, 17:555–565, 1978.

[45] J.P. Serre. *Trees*. Springer-Verlag, Berlin–Heidelberg–New York, 1980.

[46] P.F. Stebe. Residual finiteness of a class of knot groups. *Comm. Pure. Appl. Math.*, 21:563–583, 1968.

[47] P.F. Stebe. Conjugacy separability of groups of integer matrices. *Proc. Amer. Math. Soc.*, 32:1–7, 1972.

[48] W.F. Thurston. Three dimensional manifolds, Kleinian groups and hyperbolic geometry. *Bull. Amer. Math. Soc.*, 6:357–381, 1982.

[49] J.S. Wilson and P.A. Zalesskii. Conjugacy separability of certain Bianchi groups and HNN extensions. *Math. Proc. Camb. Phil. Soc.*, 123:227–242, 1998.

[50] Daniel Wise. Residual finiteness of quasi-positive 1-relator groups. *J. London Math. Soc. (2)*, 66(2):334–350, 2002.

[51] Daniel Wise. A residually finite version of Rips's constructions. *Bull. London Math. Soc.*, 35:23–29, 2003.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Coverings, enumeration and Hurwitz problems

Jin Ho Kwak
Mathematics, Pohang University of Science and Technology, Pohang, Korea

Jaeun Lee
Mathematics, Yeungnam University, Kyongsan, Korea

Alexander Mednykh
Sobolev Institute of Mathematics, Novosibirsk State University, Novosibirsk, Russia

ABSTRACT: In the nineteen century, a branched covering of the Riemann sphere was considered as a natural set of definition of multi-valued analytic function. Later, this became a basis for creating the concept of Riemann surface or, more generally of Riemannian manifold. The first background for the Riemann surface theory was done by A. Hurwitz in his classical papers in 1891 and 1903. In particular, these papers became a source of so-called Hurwitz Enumeration Problem: Determine the number of branched coverings of a given Riemann surface with prescribed ramification type. In twenty century a lot of papers devoted to this problem have been appeared. In the end of century it became clear that the Hurwitz Enumeration Problem is closely related with description of strata in the moduli spaces and is a key for understanding of important invariants in the string theory, for example such as Witten-Gromov invariant. In the recent papers by A. Okounkov a deep relationship was discovered between Hurwitz numbers, representation theory of finite group, probability theory and partial differential equations. It was also shown that the generating function for Hurwitz numbers satisfies the KdV equation. This gives a positive solution of celebrated Witten conjecture.

This paper is devoted to solutions of the enumeration problem for (branched) coverings of Riemann surfaces and, more generally graphs, manifolds and orbifolds with finitely generated fundamental group. We represent here some well-known results in this field, recent developments of the problem and indicate a general approach to solve the problem in high-dimensional case. In this survey we cover group theoretical, combinatorial and topological points of view on the problem and do not concern with its application to theoretical physics.

1 INTRODUCTION

Let $\mathcal{M}$ be a connected manifold. A *covering* $p : \mathcal{U} \to \mathcal{M}$ is a surjective continuous map with every $x \in \mathcal{M}$ having open neighborhood O such that any connected component of $p^{-1}(O)$ is mapped homeomorphically onto O by p. Note that cardinality of fiber $p^{-1}(x)$ does not depends on the choice of x. A covering $p : \mathcal{U} \to \mathcal{M}$ (connected or not) is said to be *n-fold* if fiber $p^{-1}(x)$ consists of n elements. Two coverings $p : \mathcal{U} \to \mathcal{M}$ and $p' : \mathcal{U}' \to \mathcal{M}$ are *equivalent* (or *isomorphic*) if there exists a homomorphism $h : \mathcal{U} \to \mathcal{U}'$ such that $\pi = \pi' \circ h$.

In the case of connected coverings it is convenient to deal with *rooted* (or *pointed*) coverings. Two rooted coverings $p : (\mathcal{U}, \widetilde{x}_0) \to (\mathcal{M}, x_0)$ and $p' : (\mathcal{U}', \widetilde{x}_0^{'}) \to (\mathcal{M}, x_0)$ are equivalent if exists a homomorphism $h : (\mathcal{U},\widetilde{x}_0) \to (\mathcal{U}',\widetilde{x}_0^{'})$ such that $\pi = \pi' \circ h$. The following facts are well known in algebraic topology. See for example [1] and [2].

Let $p : \mathcal{U} \to \mathcal{M}$ be a connected n-fold covering of $\mathcal{M}$. Then the fundamental group $K = \pi_1(\mathcal{U})$ is contained as a subgroup of index n in the group $\Gamma = \pi_1(\mathcal{M})$. Conversely, each subgroup K of index n in Γ is the fundamental group of an appropriated n-fold covering.

Two (unrooted) coverings $p : \mathcal{U} \to \mathcal{M}$ and $p' : \mathcal{U}' \to \mathcal{M}$ are equivalent if and only if the corresponding subgroups $\pi_1(\mathcal{U})$ and $\pi_1(\mathcal{U})$ are conjugate in Γ. Hence, the number of non-equivalent n-fold coverings of $\mathcal{M}$ coincides with the number $c_\Gamma(n)$ of conjugacy classes of subgroups of index n in the group Γ.

Respectively, two rooted coverings are equivalent if and only if the corresponding subgroups are the same. So the number of non-equivalent n-fold rooted coverings of $\mathcal{M}$ coincides with the number $s_\Gamma(n)$ of subgroups of index n in the group Γ.

Situation with disconnected coverings is slightly more complicated. In this case, non-equivalent n-sheeted coverings of $\mathcal{M}$ are classified by equivalence classes of homomorphisms $\rho : \pi_1(\mathcal{M}) \to \mathbf{S}_n$, where is $\mathbf{S}_n$ is the symmetric group on n symbols and the equivalence relation identifies a homeomorphism ρ with each of its conjugates $h^{-1}\rho\, h$ by elements $h \in \mathbf{S}_n$. We note that this action is transitive if and only if the covering manifold $\mathcal{U}$ is connected. Moreover, the number of orbits of the action coincides with the number of connected components of the covering. See Sections 3 and 5 for more detailed description of disconnected and branched coverings.

All the above mentioned results remain to be true for any path-connected, locally path-connected and semilocally simply connected topological space $\mathcal{M}$. See, for example ([2], Ch. 1.3). In particular, they are true for any *finite graph*.

There are few natural numerical invariants related with coverings. The first two are so called *Hurwitz numbers* $H_\Gamma(n)$ and $h_\Gamma(n)$. By definition, $H_\Gamma(n) = |\mathrm{Hom}\,(\Gamma,\, \mathbf{S}_n)|$ is the number of homomorphisms from Γ to the symmetric group $\mathbf{S}_n$ and $h_\Gamma(n) = \frac{1}{n!} H_\Gamma(n)$. We note that $h_\Gamma(n)$ is not necessary integer, while $nh_\Gamma(n)$ does. Both $H_\Gamma(n)$ and $h_\Gamma(n)$ are very important in theoretical physics, especially in string theory and Gromov-Witten theory. These numbers are also responsible for the structure of singular loci in the moduli space of Riemann surfaces. Recently it was discovered by A. Okounkov that there is a deep relationship between Hurwitz numbers, representation theory of finite groups, probability theory and partial differential equations. Hurwitz numbers are closely related with the number $s_\Gamma(n)$ of subgroups of index n in the group Γ. Indeed, by the well-known exponential law (see, for example [3], p. 111) we have

$$\sum_{n\geq 0} h_\Gamma(n)\, x^n = \exp\left(\sum_{n\geq 1} \frac{s_\Gamma(n)\, x^n}{n}\right).$$

So, the sequence of Hurwitz numbers $h_\Gamma(n)$ and the sequence $s_\Gamma(n)$ produce essentially the same invariants for the group Γ. However, it was shown in [4] that the fundamental groups of closed surfaces of the same Euler characteristic (orientable and not) share the same number $s_\Gamma(n)$, while the numbers of conjugacy classes of subgroups $c_\Gamma(n)$ for them are different. In particular, this is true for the torus and Klein bottle [5]. That is, the number of conjugacy classes $c_\Gamma(n)$ is more powerful characteristic as the number of subgroups, or Hurwitz numbers. It will be discovered later that the numbers $c_\Gamma(n)$ are responsible also for the number of chiral and self-dual objects such as coverings of non-orientable manifolds, maps on surfaces and polyhedra. We introduce also the number $b_\Gamma(n) = |\mathrm{Hom}\,(\Gamma,\, \mathbf{S}_n)/\mathbf{S}_n|$ of all (connected or disconnected) n-fold coverings which coincides with the number of orbits of $\mathbf{S}_n$ acting on the set of homomorphisms by conjugation. Despite of similar notation $b_\Gamma(n) = |\mathrm{Hom}\,(\Gamma,\, \mathbf{S}_n)/\mathbf{S}_n|$ and $h_\Gamma(n) = |\mathrm{Hom}\,(\Gamma,\, \mathbf{S}_n)|/|\mathbf{S}_n|$ the properties of numbers $b_\Gamma(n)$ and $h_\Gamma(n)$ are different. In the same time $b_\Gamma(n)$ and $c_\Gamma(n)$ are related by the following Euler transform [6]

$$\sum_{n\geq 0} b_\Gamma(n)\, x^n = \prod_{n\geq 1} (1 - x^n)^{-c_\Gamma(n)}.$$

In this sense, the sequences $b_\Gamma(n)$ and $c_\Gamma(n)$ represent the same invariant of the group Γ.

The aim of this survey paper is to collect old and recent results on enumeration of coverings. For remarkable properties of Hurwitz numbers we refer reader to the papers [7], [8] and [9].

Let G be a finite connected graph with Betti number β. The fundamental group $\pi_1(G) = F_\beta$ is a free group of rank β. Since the number of coverings of G depends only on its fundamental group we can assume that $G = B_\beta$ is a bouquet of β circles. In this section we describe different types of n-fold coverings of B_β and count their numbers. Recall that the number $\mathrm{Iso}(G; n)$ of non-equivalent n-fold coverings of B_β is counted by orbits of symmetric group $\mathbf{S}_n$ acting by conjugation on the set of homomorphisms $\mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n)$. We consider $\mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n)$ as the set of ordered β-tuples of elements of $\mathbf{S}_n$

$$\mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n) = \{(\sigma_1, \ldots, \sigma_\beta) : \sigma_i \in \mathbf{S}_n,\ i = 1, \ldots, \beta\}.$$

Let B_β be a bouquet of β circles, say $\ell_1, \ell_2, \ldots, \ell_\beta$. For each loop, we fix an orientation on it, called a positively directed loop. Let $\mathbf{S}_n$ denote the symmetric group on n elements $\{1, 2, \ldots, n\}$. Then every n-fold covering graph of B_β can be derived from an element in $\mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n)$ as follows: Each $\phi = (\sigma_1, \ldots, \sigma_\beta) \in \mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n)$ derives a covering graph having n vertices $1, 2, \ldots, n$ and the vertices i and $\sigma_j(i)$ are adjacent for all i and σ_j. The covering projection is defined to map the arc $(i, \sigma_j(i))$ to the positively directed loop ℓ_j for $i = 1, 2, \ldots, d$. We define an $\mathbf{S}_n$-action on the set $\mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n)$ by simultaneous coordinatewise conjugacy: For any $g \in \mathbf{S}_n$ and any $(\sigma_1, \ldots, \sigma_\beta) \in \mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n)$,

$$g(\sigma_1, \sigma_2, \ldots, \sigma_\beta) = (g\sigma_1 g^{-1}, g\sigma_2 g^{-1}, \ldots, g\sigma_\beta g^{-1}).$$

The following lemma was shown in [10].

Lemma 2.1.

(1) *Two tuples $\phi = (\sigma_1, \ldots, \sigma_\beta)$ and $\psi = (\sigma_1', \ldots, \sigma_\beta')$ yield isomorphic unrooted coverings of B_β if and only if they belong to the same orbit under the $\mathbf{S}_n$-action. (In this case we say that ϕ and ψ are similar.)*

(2) *Two tuples $\phi = (\sigma_1, \ldots, \sigma_\beta)$ and $\psi = (\sigma_1', \ldots, \sigma_\beta')$ yield isomorphic rooted coverings of B_β if and only if they belong to the same orbit under the $\mathbf{S}_{n-1}$ action, as the subgroup of $\mathbf{S}_n$ consisting of permutations σ fixing* 1*, i.e., $\sigma(1) = 1$. (In this case we say that ϕ and ψ are root-similar.)*

Now, one can get the following theorem from the orbit-counting theorem commonly known as Burnside's Lemma.

$$\mathrm{Iso}(G; n) = |\mathrm{Hom}\,(F_\beta,\, \mathbf{S}_n)/\mathbf{S}_n| = \frac{1}{n!} \sum_{g \in \mathbf{S}_n} |\mathrm{Fix}(g)|,$$

where $\mathrm{Fix}(g) = \{(\sigma_1, \ldots, \sigma_\beta) \in S_n^\beta : g\,\sigma_i\, g^{-1} = \sigma_i,\ i = 1, \ldots, \beta\}$.
Since the number of elements of $\mathrm{Fix}(g)$ depends only on the cycle type of g and $\mathrm{Fix}(g)$ is the centralizer $Z(g)$ of g, we have

$$\begin{aligned}\mathrm{Iso}(G;\, n) &= \frac{1}{n!} \sum_{g \in \mathbf{S}_n} |\mathrm{Fix}(g)| \\ &= \sum_{k_1 + 2k_2 + \cdots + nk_n = n} (\ell_1!\, 2^{\ell_2} \ell_2! \cdots n^{\ell_n} \ell_n!)^{\beta(G)-1}.\end{aligned}$$

Theorem 2.2 [10]. *Let G be a connected graph with Betti number β. Then the number of non-equivalent m-fold (connected or disconnected) coverings of G is*

$$\mathrm{Iso}(G;\, n) = \sum_{\ell_1+2\ell_2+\cdots+r\ell_n=n} (\ell_1!\, 2^{\ell_2}\ell_2! \cdots r^{\ell_r}\ell_r!)^{\beta-1}.$$

The fundamental group of a graph B_β is a free group of rank β, and there exists a one-to-one correspondence between the rooted *connected* non-equivalent n-fold coverings of B_β and the index n subgroups in the fundamental group of B_β. Then, $s_{F_\beta}(n)$ equals to the number of *connected* rooted non-equivalent n-fold coverings of B_β. By Lemma 2.1 this coincides with the root-similar classes of transitive permutation representations of the free group F_β. The number $s_{F_\beta}(n)$ was determined by Hall [11] and his proof can be rephrased by covering terminologies.

Theorem 2.3 [11]. *The number of rooted connected non-equivalent r-fold coverings of B_β is*

$$s_{F_\beta}(n) = n(n!)^{\beta-1} - \sum_{t=1}^{n-1} ((n-t)!)^{\beta-1}\, s_{F_\beta}(t) \quad \textit{with}\; s_{F_\beta}(1) = 1.$$

We present here a sketch of a combinatorial proof. First, recall that $F_\beta = \pi_1(B_\beta)$ is a free group generated by β elements and all n-fold (connected or disconnected) coverings of a bouquet B_β of β cycles (a one vertex graph with β loops and no semiedges) are determined by β-tuples $(\sigma_1, \ldots, \sigma_\beta) \in \mathbf{S}_n^\beta$.

(i) Given any β-tuple $\sigma = (\sigma_1, \ldots, \sigma_\beta)$, let the orbit of 1 under the action of $G_\sigma = \langle \sigma_1, \ldots, \sigma_\beta \rangle$ on $F = \{1, 2, \ldots, n\}$ be

$$O = \{1, b_2, \ldots, b_t\},$$

and let V_O be the corresponding orbit in the covering $B_\beta^\sigma \longrightarrow B_\beta$. Let V be the n-element set of vertices and α be a labelling $\alpha : F \to V$ taking $1 \mapsto v_1$, where $v_1 \in V_O$ is fixed. Each σ and each α gives a subgroup $\pi_1(B_\beta^\sigma, v_1)$ of $\mathcal{F}_\beta$ of index t.

(ii) How many 1-similarity classes of σ are there? In other words, how many labellings $\alpha : F \to V$ taking $1 \to v_1$ and preserving O set-wise does exist? There are $(n-1)\cdots(n-t+1)$ choices of labels in O and there are $(n-t)!$ choices of labels for vertices in $V \setminus V_O$. Note that all $\sigma_1, \ldots, \sigma_\beta$ in σ should have the same letters for the orbit of 1, but free for the letters which do not in the orbit of 1. Hence, in total, there are

$$(n-1)\cdots(n-t+1)[(n-t)!]^\beta = (n-1)![(n-t)!]^{\beta-1}$$

permutations in the 1-similar class of σ.

(iii) Let $s_{F_\beta}(t)$ denote the number of subgroups of F_β of index t. Since each subgroup of index t is induced by the same number of β-tuples of permutations (in its 1-similar class) among $(n!)^\beta$ permutations in $(\mathbf{S}_n)^\beta$, we have,

$$(n!)^\beta = \sum_{t=1}^{n} (n-1)![(n-t)!]^{\beta-1} S_{F_\beta}(t).$$

Divide by $(n-1)!$ to get

$$n(n!)^{\beta-1} = \sum_{t=1}^{n-1} [(n-t)!]^{\beta-1} s_{F_\beta}(t) + s_{F_\beta}(n). \qquad \square$$

Next, we compute the number Isoc $(B_\beta;\, n)$ of unrooted *connected* non-equivalent n-fold coverings of B_β.

Let $\mathcal{T}(n;\beta)$ denote the set of all transitive β-tuples of permutations in $\mathbf{S}_n$. The symmetric group $\mathbf{S}_n$ acts naturally on the set $\{1, 2, \ldots, n\}$, and also acts on the set $\mathcal{T}(n;\beta)$ by the simultaneous coordinatewise conjugacy. Then, Lemma 2.1(2) and Burnside's Lemma gives

$$s_{F_\beta}(n) = |\mathcal{T}(r;\beta)/\mathbf{S}_{n-1}| = \frac{1}{(n-1)!}\sum_{g\in\mathbf{S}_{n-1}} |\mathrm{Fix}(g)|,$$

where the group $\mathbf{S}_{n-1}$, as the subgroup of $\mathbf{S}_n$, consists of permutations σ fixing 1, *i.e.,* $\sigma(1) = 1$. Since any β-tuple in the set $\mathcal{T}(\beta;n)$ is transitive, the group $\mathbf{S}_{n-1}$ acts freely on the set $\mathcal{T}(\beta;n)$, which gives

$$|\mathcal{T}(\beta;n)| = (n-1)!\, s_{F_\beta}(n).$$

Now, we follow the Liskovets' method for computing the number Isoc $(B_\beta;\, n)$. By Lemma 2.1(1) and Burnside's Lemma, we have

$$\mathrm{Isoc}\,(B_\beta;\, n) = |\mathcal{T}(\beta;n)/\mathbf{S}_n| = \frac{1}{n!}\sum_{g\in\mathbf{S}_n} |\mathrm{Fix}\,(g)|,$$

and Fix $(g) = \mathcal{T}(\beta;n) \cap (Z(g)\times\cdots\times Z(g))$. If Fix $(g) \neq \emptyset$ and $\phi = (\sigma_1, \ldots, \sigma_\beta)$ belongs to Fix (g), then g commutes with the group $\langle\sigma_1, \ldots, \sigma_\beta\rangle$, which is transitive on the set $\{1, 2, \ldots, n\}$. Hence, g must be a *regular* permutation, *i.e.,* it consists of independent cycles of the same length ℓ. For each $\ell\, m = n$, there exist $n!/(m!\,\ell^m)$ regular permutations g in $\mathbf{S}_n$ consisting of m cycles of length ℓ, and $|\mathrm{Fix}\,(g)|$ are equal for all such regular g. We denote this value by $|\mathrm{Fix}\,((\ell^m))|$, and call such g a permutation of type (ℓ^m). Hence, we get

$$\mathrm{Isoc}\,(B_\beta;\, n) = \frac{1}{n!}\sum_{g\in\mathbf{S}_n} |\mathrm{Fix}\,(g)| = \sum_{\ell|n,\ell\, m=n} \frac{|\mathrm{Fix}\,((\ell^m))|}{m!\,\ell^m}.$$

Liskovets computed $|\mathrm{Fix}\,((\ell^m))|$ in terms of the numbers $s_{F_\beta}(m)$ for $m|n$ and the Möbius function to get the following theorem.

Theorem 2.4 [12]. *Let G be a connected graph with Betti number β. Then the number of (unrooted) non-equivalent connected n-fold coverings of G is given by the formula*

$$\mathrm{Isoc}\,(G;\, n) = \frac{1}{n}\sum_{m|n} s_{F_\beta}(m) \sum_{d|\frac{n}{m}} \mu\left(\frac{n}{md}\right) d^{(\beta-1)m+1},$$

where $\mu(n)$ is the number-theoretic Möbius function.

Later, Hofmeister [13] and Kwak and Lee [14] independently found another combinatorial enumeration formulae for the number of unrooted non-equivalent connected n-fold coverings of a graph. Since this number coincides with the number of conjugacy classes of subgroups of index n in F_β it counts also the number of non-equivalent connected n-fold coverings of bordered surface $\mathcal{B}_\beta$ with Euler characteristic $\chi = 1 - \beta$ and fundamental group F_β.

A graph covering is regular if the covering projection is equivalent to the quotient map induced by a free action of a finite group on the covering graph. When the acting group is $\mathcal{A}$, we call it an $\mathcal{A}$-covering. Let Iso $(G;\mathcal{A})$ be the number of regular $\mathcal{A}$-coverings, and Isoc $(G;\mathcal{A})$ the number that are connected. Similarly, we let $\text{Iso}^R(G;r)$ be the number of regular r-fold coverings regardless of the group $\mathcal{A}$ involved, and of course $\text{Isoc}^R(G;r)$ denote the number that are connected.

It is not difficult to show that the components of any regular covering of a graph G are isomorphic as coverings of G, and any two isomorphic connected regular coverings of G must have isomorphic covering transformation groups. Moreover, any two regular coverings of G of the same fold number are isomorphic if and only if their components are isomorphic as coverings. Notice that each component of an $\mathcal{A}$-covering of G is an $\mathcal{S}$-covering of G for some subgroup $\mathcal{S}$ of $\mathcal{A}$. The following theorem of Kwak, Chun and Lee [15] lists some basic counting properties about regular coverings.

Theorem 2.5.

(1) *For any* $r \in \mathbb{N}$, $\text{Iso}^R(G;r) = \sum_{d|r} \text{Isoc}^R(G;d)$.

(2) *For any* $r \in \mathbb{N}$, $\text{Isoc}^R(G;r) = \sum_{\mathcal{A}} \text{Isoc}\,(G;\mathcal{A})$, *where the sum is over all nonisomorphic groups of order r.*

(3) *For any finite group* $\mathcal{A}$, $\text{Iso}\,(G;\mathcal{A}) = \sum_{\mathcal{S}} \text{Isoc}\,(G;\mathcal{S})$, *where the sum is over all nonisomorphic subgroups of* $\mathcal{A}$.

(4) *For any finite groups* $\mathcal{A}$ *and* $\mathcal{B}$ *with* $(|\mathcal{A}|, |\mathcal{B}|) = 1$,

$$\text{Iso}\,(G;\mathcal{A}\oplus\mathcal{B}) = \text{Iso}\,(G;\mathcal{A})\ \text{Iso}\,(G;\mathcal{B}) \quad \textit{and}$$
$$\text{Isoc}\,(G;\mathcal{A}\oplus\mathcal{B}) = \text{Isoc}\,(G;\mathcal{A})\ \text{Isoc}\,(G;\mathcal{B}),$$

where $\mathcal{A}\oplus\mathcal{B}$ *is the direct sum of two groups* $\mathcal{A}$ *and* $\mathcal{B}$.

(5)

$$\text{Isoc}\,(G;\mathcal{A}) = \frac{|\mathcal{T}(\beta;\,\mathcal{A})|}{|\text{Aut}\,(\mathcal{A})|},$$

where $\text{Aut}\,(\mathcal{A})$ *is the automorphism group of* $\mathcal{A}$ *and* $\mathcal{T}(r;\mathcal{A}) = \{(g_1,\, g_2,\, \dots, g_r) \in\ \mathcal{A}^r \mid \{g_1,\, g_2, \dots, g_r\}$ generates $\mathcal{A}\}$.

To complete the enumeration of $\text{Iso}^R(G;r)$ and $\text{Isoc}^R(G;r)$, we need to determine $|\text{Aut}\,(\mathcal{A})|$ and $|\mathcal{T}(\beta;\mathcal{A})|$. For any finite abelian group $\mathcal{A}$, Kwak et al. [15] computed explicitly $|\text{Aut}\,(\mathcal{A})|$ and $|\mathcal{T}(\beta;\mathcal{A})|$.

Now, we introduce a formula to compute the number $|\mathcal{T}(\beta;\mathcal{A})|$ for any finite group $\mathcal{A}$ in terms of the Möbius function defined on the subgroup lattice of $\mathcal{A}$. The Möbius function assigns an integer $\mu(K)$ to each subgroup K of $\mathcal{A}$ by the recursive formula

$$\sum_{H\geq K} \mu(H) = \delta_{K,\mathcal{A}} = \begin{cases} 1 & \text{if } K = \mathcal{A}, \\ 0 & \text{if } K < \mathcal{A}. \end{cases}$$

Jones [16, 17] used such function to count the normal subgroups of a surface group or a crystallographic group, and applied it to count certain covering surfaces. We see that

$$|\mathcal{A}|^\beta = \sum_{K\leq\mathcal{A}} |\mathcal{T}(\beta;K)|.$$

Now, it comes from the Möbius inversion that

$$|\mathcal{T}(\beta;\mathcal{A})| = \sum_{K\leq\mathcal{A}} \mu(K)|K|^\beta.$$

Now, the following theorem follows from Theorem 2.5(5).

Theorem 2.6. *For any finite group $\mathcal{A}$,*

$$\operatorname{Isoc}(G;\mathcal{A}) = \frac{1}{|\operatorname{Aut}(\mathcal{A})|}\sum_{K\le\mathcal{A}} \mu(K)|K|^{\beta}.$$

We illustrate Theorem 2.6 by applying it to a graph G with Betti number β.

Example 2.7.

(1) The cyclic group $\mathcal{A} = \mathbb{Z}_n$ has a unique subgroup $\mathbb{Z}_m$ for each m dividing n, and has no other subgroups. The Möbius function on the subgroup is $\mu(\mathbb{Z}_m) = \mu(n/m)$ (the Möbius function of the elementary number theory) and $|\operatorname{Aut}(\mathbb{Z}_n)| = \varphi(n)$ (Euler φ-function).

For a subgroup $\mathbb{Z}_m \le \mathbb{Z}_n$ with $m|n$, we get $\mu(\mathbb{Z}_m) = \mu\left(\frac{n}{m}\right)$. Hence,

$$\operatorname{Isoc}(G;\mathbb{Z}_n) = \frac{1}{\varphi(n)}\sum_{m|n}\mu\left(\frac{n}{m}\right)m^{\beta}.$$

This coincides with the formula which can be derived from the results in [15].

(2) Let $\mathcal{A} = \mathbb{D}_n = \langle a, b : a^2 = 1 = b^n, aba = b^{-1}\rangle$ be the dihedral group of order $2n$. For convenience, let $\mathbb{Z}_m = \langle b^{\frac{n}{m}}\rangle$ and let $\mathbb{D}_m^{(i)} = \mathbb{Z}_m \cup \mathbb{Z}_m ab^i$ for $i = 0, \dots, \frac{n}{m} - 1$. Then each subgroup of $\mathbb{D}_n$ is one of $\mathbb{Z}_m$ or $\mathbb{D}_m^{(i)}$ for each m dividing n. Now, consider the lattice induced by the subgroups of $\mathbb{D}_n$. Then, for each subgroup K of $\mathbb{D}_n$, we have

$$\mu(K) = \begin{cases} \mu\left(\dfrac{n}{m}\right) & \text{if } K = \mathbb{D}_m^{(i)} \quad \text{for } i = 0, \dots, \dfrac{n}{m} - 1, \\ -\dfrac{n}{m}\mu\left(\dfrac{n}{m}\right) & \text{if } K = \mathbb{Z}_m. \end{cases}$$

Since $|\operatorname{Aut}(\mathbb{D}_n)| = n\cdot\varphi(n)$ for $n \ge 3$ and $|\mathbb{D}_m|^{\beta} = (2m)^{\beta}$ we have

$$\begin{aligned} \operatorname{Isoc}(G;\mathbb{D}_n) &= \frac{1}{n\cdot\varphi(n)}\left(\sum_{m|n}\frac{n}{m}\mu\left(\frac{n}{m}\right)(2m)^{\beta} - \sum_{m|n}\frac{n}{m}\mu\left(\frac{n}{m}\right)m^{\beta}\right) \\ &= \frac{2^{\beta}-1}{\varphi(n)}\sum_{m|n}\mu\left(\frac{n}{m}\right)m^{\beta-1} \end{aligned}$$

for $n \ge 3$. The group $\mathbb{D}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$ contains three proper subgroups isomorphic to $\mathbb{Z}_2$. From the definition of Möbius function we have $\mu(\mathbb{D}_2) = 1, \mu(\mathbb{Z}_2) = -1$, and $\mu(\mathbb{Z}_1) = 2$. Hence, taking into account $|\operatorname{Aut}(\mathbb{D}_2)| = 6$ we also obtain

$$\operatorname{Isoc}(G;\mathbb{D}_2) = \frac{1}{6}\left(4^{\beta} - 3\cdot 2^{\beta} + 2\right).$$

This coincides with the formulas given in Theorem 4.2 of [15].

A *surface* S is a compact connected 2-manifold without boundary. It is known that a surface S is homeomorphic to the orientable surface S_h with h handles or the non-orientable surface N_k with k crosscaps.

Mednykh [18, 4] enumerated the number of conjugacy classes of index n subgroups in the fundamental group of any surface S, which is equal to number of connected n-fold coverings of S. To state this, we need some further notations. Let $s_k(m)$ denote the number of index m subgroups in the fundamental group $\pi_1(S)$, where k is the number of handles or crosscaps of the surface S depending on the orientability. Denote by ν the Euler characteristic of S. That is $\nu = 2k - 2$ if S is an orientable surface of genus k, and $\nu = k - 2$ if S is a non-orientable surface of genus k. It was shown in [4, 18] that $s_k(m) = r_\nu(m)$, and the function $r_\nu(m)$ can be defined by the following recursive relation

$$r_\nu(m) = m\,\beta_m - \sum_{j=1}^{m-1} \beta_{m-j} r_\nu(j), \quad r_\nu(1) = 1,$$

where $\beta_h = \sum_{\chi \in \mathrm{Irr}_h} \left(\frac{h!}{f^{(\chi)}}\right)^\nu$, Irr_h is the set of all irreducible representations of the symmetric group $\mathbf{S}_h$, and $f^{(\chi)}$ is the degree of the representation.

In fact, the number $r_\nu(m)$ is given as follows:

$$r_\nu(m) = m \sum_{s=1}^{m} \frac{(-1)^{s+1}}{s} \sum_{\substack{i_1+i_2+\cdots+i_s=m\\ i_1, i_2, \ldots, i_s \geq 1}} \beta_{i_1}\beta_{i_2}\cdots\beta_{i_s}.$$

A non-orientable surface admits two kinds of coverings—orientable and non-orientable ones. The fundamental groups of these coverings are called *orientable* and *non-orientable*, respectively.

Denote by $s_k^+(m)$ and $s_k^-(m)$ the respective numbers of orientable and non-orientable subgroups of index m in the fundamental group of non-orientable surface of genus k. Then $s_k^+(m) = 0$ if m is odd, $s_k^+(m) = r_{2\nu}(\frac{m}{2})$ if m is even, and $s_k^-(m) = r_\nu(m) - s_k^+(m)$.

We have the following result [4, 18].

Theorem 2.8. *The number of connected n-fold coverings of a surface is given by*

$$\mathrm{Isoc}\,(S_k; n) = \frac{1}{n} \sum_{m|n} s_k(m) \sum_{d|\frac{n}{m}} \mu\left(\frac{n}{md}\right) d^{(2k-2)m+2} \quad \textit{and}$$

$$\mathrm{Isoc}\,(N_k; r) = \frac{1}{r} \sum_{m|n} \sum_{d|\frac{n}{m}} \mu\left(\frac{n}{md}\right) d^{(k-2)m+1}[(2,d)s_k^-(m) + d\,s_k^+(m)],$$

where μ is the Möbius function and $(2, d)$ is the greatest common divisor of 2 and d.

We illustrate the above theorem by the following examples.

Example 2.9. Let S_k be an orientable surface of genus g *and* $\nu = 2k - 2$. Then

$$\mathrm{Isoc}\,(S_k; 2) = -1 + 4 \cdot 2^\nu$$
$$\mathrm{Isoc}\,(S_k; 3) = 2 \cdot (-2^\nu + 2 \cdot 3^\nu + 6^\nu)$$
$$\mathrm{Isoc}\,(S_k; 4) = -3^\nu + 4^\nu - 2 \cdot 6^\nu + 6 \cdot 8^\nu + 12^\nu + 2 \cdot 24^\nu.$$

Example 2.10. Let N_k be a non-orientable surface of genus k *and* $\nu = k - 2$. Then

$$\mathrm{Isoc}\,(N_k; 2) = -1 + 4 \cdot 2^\nu$$
$$\mathrm{Isoc}\,(N_k; 3) = 2 \cdot (-2^\nu + 3^\nu + 6^\nu)$$
$$\mathrm{Isoc}\,(N_k; 4) = -3^\nu - 4^\nu - 2 \cdot 6^\nu + 6 \cdot 8^\nu + 12^\nu + 2 \cdot 24^\nu.$$

A covering over a nonorientable surface can be orientable. Kwak et al. [19] enumerate the isomorphism classes of orientable coverings of a nonorientable surface, as an answer of the question raised by Liskovets in [20].

Theorem 2.11. *Let N_k be a nonorientable surface of genus k. Then, every connected orientable covering of N_k must be even-fold, and for any r, the number of isomorphism classes of connected $2r$-fold orientable coverings of N_k is*

$$\begin{aligned}\mathrm{Isoc}^O(N_k; 2r) = \frac{1}{2r}\sum_{\ell \mid r}\Bigg(&\sum_{d \mid \frac{r}{\ell}} \mu\left(\frac{r}{d\ell}\right) d^{2\ell(k-2)+2} s_k(\ell) \\ &+ \sum_{d \mid \frac{r}{\ell}, \frac{r}{d\ell}:\text{odd}} \mu\left(\frac{r}{d\ell}\right) d^{\ell(k-2)+1}\, \frac{1+(-1)^{k\ell(d-1)}}{2} (2, d)\, s_k^-(\ell)\Bigg),\end{aligned}$$

where $s_k(\ell)$ and $s_k^-(\ell)$ are the numbers mentioned in Theorem 2.8.

The proof of the two above theorems will be given later in a general setting.

Example 2.12. Let N_k be a non-orientable surface of genus k *and* $\nu = k - 2$. Then

$$\begin{aligned}\mathrm{Isoc}^O(N_k; 2) &= 1 \\ \mathrm{Isoc}^O(N_k; 4) &= -1 + (2, \nu) \cdot 2^\nu + 4 \cdot 4^\nu - 2 \cdot 8^\nu \\ \mathrm{Isoc}^O(N_k; 6) &= -2^\nu + 3^\nu - 4^\nu + 6^\nu + 2 \cdot 9^\nu + 36^\nu.\end{aligned}$$

3 COVERINGS OF MANIFOLDS

3.1 *Coverings of manifolds*

Let $\mathcal{M}$ be a connected manifold, possibly with non-empty boundary. Denote by $\Gamma = \pi_1(\mathcal{M})$ the fundamental group of $\mathcal{M}$.

In [21], the following formula for the number of conjugacy classes of subgroups of given index in a finitely generated group is obtained. This also gives the number of non-equivalent n-fold coverings of $\mathcal{M}$.

Theorem 3.1. *Let Γ be a finitely generated group. Then the number of conjugacy classes of subgroups of index n in the group Γ is given by the formula*

$$c_\Gamma(n) = \frac{1}{n}\sum_{\substack{\ell \mid n \\ \ell\, m = n}} \sum_{K <_m \Gamma} |\mathrm{Epi}\,(K, \mathbb{Z}_\ell)|,$$

where the sum $\sum_{K <_m \Gamma}$ is taken over all subgroups K of index m in the group Γ and $\mathrm{Epi}\,(K, \mathbb{Z}_\ell)$ *is the set of epimorphisms of the group K onto a cyclic group $\mathbb{Z}_\ell$ of order ℓ.*

The proof of Theorem 3.1 is essentially based on the following observations.

(1) First of all, by a version of Burnside lemma given in ([3], p. 111) we have $c_\Gamma(n) = \frac{1}{n}\sum_{P \underset{n}{<} \Gamma} |N_\Gamma(P)/P|$, where the sum is taken over all subgroups of index n in Γ and $N_\Gamma(P)$ is the normalizer of the group P in Γ.

(2) The next observation is that

$$|N_\Gamma(P)/P| = \sum_{\substack{\ell|n \\ \ell\, m=n}} \sum_{P \underset{\mathbb{Z}_\ell}{\lhd} K \underset{m}{<} \Gamma} \phi(\ell).$$

Indeed, there is a natural bijection between cyclic subgroups of order ℓ in $N_\Gamma(P)/P$ and subgroups K satisfying $P \underset{\mathbb{Z}_\ell}{\lhd} K \underset{m}{<} \Gamma$. Each element of finite group $G = N_\Gamma(P)/P$ generates a cyclic subgroup $\mathbb{Z}_\ell$ of order ℓ for some $\ell|n$. For each subgroup $\mathbb{Z}_\ell < G$ there are $\phi(\ell)$ elements of group G generating $\mathbb{Z}_\ell$. Hence,

$$|G| = \sum_{\ell|n} \sum_{\mathbb{Z}_\ell < G} \phi(\ell) = \sum_{\substack{\ell|n \\ \ell\, m=n}} \sum_{P \underset{\mathbb{Z}_\ell}{\lhd} K \underset{m}{<} \Gamma} \phi(\ell).$$

(3) Let $P \underset{\mathbb{Z}_\ell}{\lhd} K$. Then there are exactly $\phi(\ell)$ epimorphisms K onto $\mathbb{Z}_\ell$ with kernel P. That is, $\sum_{P \underset{\mathbb{Z}_\ell}{\lhd} K} \phi(\ell) = |\mathrm{Epi}\,(K, \mathbb{Z}_\ell)|$.

Combining these results we have the theorem.

There is a simple way to calculate the number of epimorphisms $\mathrm{Epi}\,(K,\ \mathbb{Z}_\ell)$ for any finitely generated group K if the first homology group $H_1(K) = K/[K, K]$ is known. More precisely, we have the following result ([21], Lemma 4).

Lemma 3.2. *Let K be a finitely generated group and $H_1(K) = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_s}$. Then*

$$|\mathrm{Epi}\,(K,\ \mathbb{Z}_\ell)| = \sum_{d\,|\,\ell} \mu\left(\frac{\ell}{d}\right) (k_1,\ d)(k_2,\ d) \cdots (k_s,\ d),$$

where $\mu(\ell)$ is the Möbius function and $(k,\ d)$ is the greatest common divisor of k and d.

We illustrate Lemma 3.2. by the following examples.

Example 3.3.

(i) Let F_r be a free group of rank r. Then $H_1(F_r) = \mathbb{Z}^r$ and $|\mathrm{Epi}\,(F_r,\ \mathbb{Z}_\ell)| = \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) d^r$.

(ii) Let $\Phi_g = \langle a_1, b_1, \ldots, a_g, b_g \mid \prod_{i=1}^g [a_i\, b_i] = 1\rangle$ be the fundamental group of a closed orientable surface of genus g. Then $H_1(\Phi_g) = \mathbb{Z}^{2g}$ and $|\mathrm{Epi}(\Phi_g,\ \mathbb{Z}_\ell)| = \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) d^{2g}$.

(iii) Let $\Lambda_p = \langle a_1, a_2, \ldots, a_p \mid \prod_{i=1}^p a_i^2 = 1\rangle$ be the fundamental group of a closed non-orientable surface of genus p. Then $H_1(\Lambda_p) = \mathbb{Z}_2 \oplus \mathbb{Z}^{p-1}$ and $|\mathrm{Epi}(\Lambda_p,\ \mathbb{Z}_\ell)| = \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) (2, d)\, d^{p-1}$.

Now, as applications of Theorem 3.1. we obtain the proof of Theorems 2.4 and 2.8.

First, we prove Liskovets Theorem 2.4. Let G be a graph with fundamental group F_β. By the Schreier theorem all subgroups of index m in F_β are isomorphic to $F_{(\beta-1)m+1}$. Since $\mathrm{Isoc}\,(G; n) = c_{F_\beta}(n)$ by the main counting principle (Theorem 3.1), we have

$$\mathrm{Isoc}\,(G; n) = \frac{1}{n} \sum_{\substack{\ell\,|\,n \\ \ell\, m=n}} |\mathrm{Epi}(\Gamma_m,\ \mathbb{Z}_\ell)| \cdot s_{F_\beta}(m),$$

By Example 3.3 (i) we get

$$|\mathrm{Epi}(\Gamma_m,\,\mathbb{Z}_\ell)| = \sum_{d\,|\,\ell} \mu\left(\frac{\ell}{d}\right) d^{(\beta-1)m+1}$$

and the result follows.

Now, we show how to prove the first statement in the Theorem 2.8. By the Riemann-Hurwitz formula all subgroups of index m in the fundamental group $\pi_1(S_k)$ of orientable surface S_k are isomorphic to the group $\pi_1(S_{(k-1)m+1})$,

Applying Theorem 3.1 we have

$$\mathrm{Isoc}\,(S_k;n) = \frac{1}{n} \sum_{\substack{\ell\,|\,n \\ \ell\, m=n}} |\mathrm{Epi}(K_m,\,\mathbb{Z}_\ell)| \cdot s_k(m),$$

where

$$|\mathrm{Epi}(K_m,\,\mathbb{Z}_\ell)| = \sum_{d\,|\,\ell} \mu\left(\frac{\ell}{d}\right) d^{2(k-1)m+2}$$

is given by Example 3.3 (ii).

To finish the proof of Theorem 2.8 we note that by Riemann-Hurwitz formula, any subgroup of index m in $\pi_1(N_k)$ is isomorphic either to group $\Gamma_m^+ = \pi_1(S_{m(k-2)/2+1})$ or to $\Gamma_m^- = \pi_1(N_{m(k-2)+2})$. By Theorem 3.1. the number of non-equivalent n-fold coverings of N_k is given by the formula

$$\frac{1}{n} \sum_{\substack{\ell\,|\,n \\ \ell\, m=n}} (|\mathrm{Epi}(\Gamma_m^+,\,\mathbb{Z}_\ell)| \cdot s_k^+(m) + |\mathrm{Epi}(\Gamma_m^-,\,\mathbb{Z}_\ell)| \cdot s_k^-(m)).$$

Hence, by using of Examples 3.3 (ii) and (iii) we have the second formula of Theorem 2.8 which was obtained in [4] in a rather complicated way. See also [22] and [23] for alternative proof.

3.2 *Orientable coverings of non-orientable manifolds*

Let $\mathcal{M}$ be a connected non-orientable manifold. Denote by $\Gamma = \pi_1(\mathcal{M})$ the fundamental group and by $\tilde{\mathcal{M}}$ the universal covering of $\mathcal{M}$. Identify Γ with the group of covering transformations of $\tilde{\mathcal{M}} \to \mathcal{M}$. We note that $\tilde{\mathcal{M}}$ is always orientable and Γ acts on $\tilde{\mathcal{M}}$ as a group of homeomorphisms.

Denote by Γ^+ a subgroup of index two in Γ consisting of all orientation preserving homeomorphisms. Then $\mathcal{M}^+ = \tilde{\mathcal{M}}\,/\,\Gamma^+$ is an *orientable double* of $\mathcal{M}$ with fundamental group $\Gamma^+ = \pi_1(\mathcal{M}^+)$. The following facts from algebraic topology are well known.

Let $\pi\,:\,\mathcal{U} \to \mathcal{M}$ be an n-fold covering of $\mathcal{M}$. Then the fundamental group $K = \pi_1(\mathcal{U})$ is contained as a subgroup of index n in the group $\Gamma = \pi_1(\mathcal{M})$. Conversely, any subgroup on index n in Γ is the fundamental group of an n-fold covering of $\mathcal{M}$. Moreover, if $\mathcal{U}$ is orientable then the number $n = 2m$ is even and the group K is contained as a subgroup of index m in the group Γ^+. In this case, $\mathcal{U}$ is an m-fold covering of the manifold $\mathcal{M}^+$.

Two coverings $\pi\,:\,\mathcal{U} \to \mathcal{M}$ and $\pi'\,:\,\mathcal{U}' \to \mathcal{M}$ are *equivalent* (or *isomorphic*) if there exists a homeomorphism $h : \mathcal{U} \to \mathcal{U}'$ such that $\pi = \pi' \circ h$. An orientable covering $\pi\,:\mathcal{U}^+ \to \mathcal{M}$ is called *reflexible* if there exists an orientation reversing homeomorphism $h : \mathcal{U}^+ \to \mathcal{U}^+$ such that $\pi \circ h = \pi$ and *irreflexible* (or *chiral*) otherwise. Irreflexible coverings are divided into chiral pairs of twins. Two twins are non-equivalent as coverings of $\mathcal{M}^+$, but have to be equivalent as coverings of $\mathcal{M}$.

During the discussion at Dresden University between V.A. Liskovets and one of the authors in 1988 the following problem was stated:

Liskovets problem. *Find the number of non-equivalent n-fold orientable coverings of a given non-orientable manifold with a finitely generated fundamental group.*

We recall that Theorem 2.11 is a solution of this problem for the surface case. The importance of the Liskovets problem is motivated by the following reasons. First, it gives a possibility to derive the numbers of reflexible coverings and of chiral pairs of coverings. In turns, these results are used for counting chiral pairs of maps (in particular, chiral polyhedra) on closed orientable surface [24]. In the second, a general formula for the number of reflexible coverings (Theorem 3.13) allows also to count self-dual and Petri-dual combinatorial objects.

Now we give a solution of the Liskovets problem. To do this we need a slight modification of the Theorem 3.1 which can be found, for example in [25]. Let $\mathcal{P}$ be a property of subgroups of Γ invariant under conjugation (for instance: to be normal, to be torsion free, to be orientable and so on). Then we have

Theorem 3.4. *Let Γ be a finitely generated group. Then the number of conjugacy classes of subgroups of index n in the group Γ having property $\mathcal{P}$ is given by the formula*

$$c_\Gamma^{\mathcal{P}}(n) = \frac{1}{n} \sum_{\substack{\ell | n \\ \ell\, m = n}} \sum_{K <_m \Gamma} |\mathrm{Epi}^{\mathcal{P}}(K, \mathbb{Z}_\ell)|,$$

where the sum $\sum_{K <_m \Gamma}$ is taken over all subgroups K of index m in Γ and $\mathrm{Epi}^{\mathcal{P}}(K, \mathbb{Z}_\ell)$ is the set of epimorphisms of the group K onto the cyclic group $\mathbb{Z}_\ell$ whose kernel has property $\mathcal{P}$.

Let $\Gamma = \pi_1(\mathcal{M})$ be the fundamental group of non-orientable manifold $\mathcal{M}$. A subgroup K of Γ is called *orientable* if $K < \Gamma^+$ and *non-orientable* otherwise. Define properties $\mathcal{P} = \mathcal{P}^+$ or $\mathcal{P} = \mathcal{P}^-$ for the subgroups of Γ as "to be oriented" or "to be non-oriented", respectively. For the sake of simplicity, we use notations

$$c_\Gamma^{+}(n) = c_\Gamma^{\mathcal{P}}(n), \;\; \mathrm{Epi}^{+}(K, \mathbb{Z}_\ell) = \mathrm{Epi}^{\mathcal{P}}(K, \mathbb{Z}_\ell)$$

for $\mathcal{P} = \mathcal{P}^+$ and

$$c_\Gamma^{-}(n) = c_\Gamma^{\mathcal{P}}(n), \;\; \mathrm{Epi}^{-}(K, \mathbb{Z}_\ell) = \mathrm{Epi}^{\mathcal{P}}(K, \mathbb{Z}_\ell)$$

for $\mathcal{P} = \mathcal{P}^-$. By definition, we have the following identities

$$c_\Gamma(n) = c_\Gamma^{+}(n) + c_\Gamma^{-}(n), \;\; |\mathrm{Epi}\,(K, \mathbb{Z}_\ell)| = |\mathrm{Epi}^{+}(K, \mathbb{Z}_\ell)| + |\mathrm{Epi}^{-}(K, \mathbb{Z}_\ell)|.$$

By applying Theorem 3.4 for $\mathcal{P} = \mathcal{P}^-$ we immediately have the following result.

Theorem 3.5. *Let $\mathcal{M}$ be a connected non-orientable manifold with a finitely generated fundamental group $\Gamma = \pi_1(\mathcal{M})$. Then the number of non-equivalent n-fold non-orientable coverings of $\mathcal{M}$ is given by the formula*

$$c_\Gamma^{-}(n) = \frac{1}{n} \sum_{\substack{\ell | n \\ \ell\, m = n}} \sum_{K^- <_m \Gamma} |\mathrm{Epi}^{-}(K^-, \mathbb{Z}_\ell)|,$$

where the sum $\sum_{K^- <_m \Gamma}$ is taken over all non-orientable subgroups of index m in the group Γ and $\mathrm{Epi}^{-}(K, \mathbb{Z}_\ell)$ is the set of epimorphisms of the group K onto a cyclic group $\mathbb{Z}_\ell$ of order ℓ with non-orientable kernel.

The next theorem can be obtained by essentially the same arguments. It gives a complete solution of V.A. Liskovets problem.

Theorem 3.6. *Let $\mathcal{M}$ be a connected non-orientable manifold with a finitely generated fundamental group $\Gamma = \pi_1(\mathcal{M})$. Then the number of non-equivalent orientable $2n$-fold coverings of $\mathcal{M}$ is equal to*

$$c_{\Gamma}^{+}(2n) = \frac{1}{2n} \sum_{\substack{\ell | n \\ \ell\, m = n}} \left(\sum_{K^{+} <_{m} \Gamma^{+}} |\mathrm{Epi}\,(K^{+},\, \mathbb{Z}_{\ell})| + \sum_{K^{-} <_{m} \Gamma} |\mathrm{Epi}^{\,+}(K^{-},\, \mathbb{Z}_{2\ell})| \right),$$

where the sum $\sum_{K^{-} <_{m} \Gamma}$ is taken over all non-orientable subgroups of index m in the group Γ, and $\mathrm{Epi}^{\,+}(K^{-}, \mathbb{Z}_{2\ell})$ *is the set of epimorphisms of the group K^{-} onto a cyclic group $\mathbb{Z}_{2\ell}$ with orientable kernel.*

Proof. Apply Theorem 3.4. for $\mathcal{P} = \mathcal{P}^{+}$. Then $c_{\Gamma}^{+}(2n)$ is given by the formula

$$\frac{1}{2n} \sum_{\substack{\ell \,|\, 2n \\ \ell\, m = 2n}} \left(\sum_{K^{+} <_{m} \Gamma} |\mathrm{Epi}\,(K^{+},\, \mathbb{Z}_{\ell})| + \sum_{K^{-} <_{m} \Gamma} |\mathrm{Epi}^{\,+}(K^{-},\, \mathbb{Z}_{\ell})| \right),$$

where the sums $\sum_{K^{+} <_{m} \Gamma}$ and $\sum_{K^{-} <_{m} \Gamma}$ are taken over all orientable and non-orientable subgroups of index m in the group Γ, respectively and $\mathrm{Epi}^{\,+}(K^{-}, \mathbb{Z}_{\ell})$ is the set of epimorphisms of the group K^{-} onto a cyclic group $\mathbb{Z}_{\ell}$ of order ℓ with orientable kernel. We note that all orientable subgroups in Γ are of even index. Hence, the condition $\sum_{K^{+} <_{m} \Gamma}$ can be rewritten in the form $\sum_{K^{+} <_{\bar{m}} \Gamma^{+}}$, where $m = 2\,\bar{m}$ and $\ell\,\bar{m} = n$. By the same reason any orientable kernel of the epimorphism of K^{-} onto $\mathbb{Z}_{\ell}$ has an even index in K^{-}. Hence, ℓ is even and $\mathrm{Epi}^{\,+}(K^{-}, \mathbb{Z}_{\ell})$ can be represented in the form $\mathrm{Epi}^{\,+}(K^{-}, \mathbb{Z}_{2\,\bar{\ell}})$, where $\bar{\ell}\, m = n$. After these remarks, by replacing $\bar{\ell}$ to ℓ an $\bar{m}$ to m we get the theorem. □

The following results are helpful to find $|\mathrm{Epi}^{\,+}(K, \mathbb{Z}_{\ell})|$ and $|\mathrm{Epi}^{\,-}(K, \mathbb{Z}_{\ell})|$.

Let K be a finite index subgroup in the group Γ and $K^{+} = K \cap \Gamma^{+}$ is the maximal orientable subgroup of K. Denote by $\omega : K \to K/K^{+}$ the canonical epimorphism. We identify K/K^{+} with $\mathbb{Z}_1 = \{+1\}$ if K is orientable subgroup of Γ and with $\mathbb{Z}_2 = \{\pm 1\}$ otherwise. Then ω can be projected to the homomorphism $\overline{\omega} : H_1(K) \to \mathbb{Z}_2 = \{\pm 1\}$.

We represent the oriented homology group of K in the form

$$H_1(K) = \mathbb{Z}_{k_1}^{\epsilon_1} \oplus \mathbb{Z}_{k_2}^{\epsilon_2} \oplus \cdots \oplus \mathbb{Z}_{k_n}^{\epsilon_n},$$

where $k_j \in \{2, 3, \ldots, \infty\}$, $j = 1, 2, \ldots, n$ and $\mathbb{Z}_{k}^{\epsilon}$ means that the corresponding cyclic group $\mathbb{Z}_k$ is generated by an element x with $\overline{\omega}(x) = \epsilon$ for $\epsilon \in \{-1, +1\}$.

We accept the following conventions $\mathbb{Z}_{k}^{-1} = \mathbb{Z}_{k}^{-}$, $\mathbb{Z}_{k}^{+1} = \mathbb{Z}_{k}^{+}$, $\mathbb{Z}_{\infty} = \mathbb{Z}$, $(-1)^{\infty} = 1$, and $(\infty, \ell) = \ell$ for any positive integer ℓ.

Example 3.7. *Let F_r be the fundamental group of a bordered non-orientable surface of Euler characteristic $1 - r$. Then $H_1(F_r) = (\mathbb{Z}^{-})^{r}$.*

Example 3.8. *Let $\Lambda_p = \langle x_1, x_2, \ldots, x_p : x_1^2 x_2^2 \cdots x_p^2 = 1\rangle$ be the fundamental group of a closed non-orientable surface of genus p. Then $H_1(\Lambda_p) = (\mathbb{Z}^{-})^{(p-1)} \oplus \mathbb{Z}_2^{(-1)^p}$.*

The next theorem was obtained in [26]

Theorem 3.9. *Let K be a finitely generated orientable group and let*

$$H_1(K) = \mathbb{Z}_{k_1}^{\epsilon_1} \oplus \mathbb{Z}_{k_2}^{\epsilon_2} \oplus \cdots \oplus \mathbb{Z}_{k_n}^{\epsilon_n}$$

be the oriented homology group of K. Then $|\mathrm{Epi}^+(K,\mathbb{Z}_\ell)| = 0$ if ℓ is odd and

$$|\mathrm{Epi}^+(K,\mathbb{Z}_{2\ell})| = \prod_{j=1}^{n} \frac{1+\epsilon_j^{\frac{k_j}{(k_j,\ell)}}}{2} \sum_{\substack{m \\ \frac{\ell}{m}:\mathrm{odd}}} \mu\left(\frac{\ell}{m}\right)(k_1,\, m)(k_2,\, m)\cdots(k_n,\, m).$$

We note that $|\mathrm{Epi}^-(K,\mathbb{Z}_\ell)| = |\mathrm{Epi}\,(K,\mathbb{Z}_\ell)| - |\mathrm{Epi}^+(K,\mathbb{Z}_\ell)|$, where $\mathrm{Epi}\,(K,\mathbb{Z}_\ell)$ is defined by Lemma 3.2.

Now we apply the obtained result to the fundamental groups F_r and Λ_p of bordered and closed non-orientable surfaces.

Let $\varphi_p(\ell) = \sum_{d\,|\,n} \mu\left(\frac{\ell}{d}\right) d^p$ be the Jordan function. It follows from Example 3.3 that $|\mathrm{Epi}\;(F_r,\,\mathbb{Z}_\ell)| = \varphi_r(\ell)$ and $|\mathrm{Epi}\,(\Lambda_p,\,\mathbb{Z}_p)| = \sum_{d\,|\,n} \mu\left(\frac{\ell}{d}\right)(2,d)d^{p-1}$, where $(2,d) = \mathrm{GCD}(2,d)$ and GCD means the greatest common divisor.

Let we introduce the *odd* Jordan function in the following way:

$$\varphi_p^{\mathrm{odd}}(\ell) = \sum_{d\,|\,n,\, \frac{\ell}{d}:\mathrm{odd}} \mu\left(\frac{\ell}{d}\right) d^p.$$

Consider the groups F_r and Λ_p as oriented groups with natural orientation. By Examples 3.7 and 3.8 we have $H_1(F_r) = (\mathbb{Z}^-)^r$ and $H_1(\Lambda_p) = (\mathbb{Z}^-)^{(p-1)} \oplus \mathbb{Z}_2^{(-1)^p}$. Hence, as a consequence of the above theorem we obtain the following proposition

Proposition 3.10. *Let Γ be the group F_r or Λ_p with natural orientation. Then the number of epimorphisms of Γ onto the cyclic group $\mathbb{Z}_\ell$ having orientable kernel is given by the following formulas*

(1) $|\mathrm{Epi}^+(\Gamma,\,\mathbb{Z}_\ell)| = 0$ *for ℓ odd*;

(2) $|\mathrm{Epi}^+(F_r,\,\mathbb{Z}_{2\ell})| = \varphi_r^{\mathrm{odd}}(\ell)$ *for $\ell \geq 1$*;

(3) $|\mathrm{Epi}^+(\Lambda_p,\,\mathbb{Z}_{2\ell})| = (2,\ell)\frac{1+(-1)^{p(\ell-1)}}{2}\,\varphi_{p-1}^{\mathrm{odd}}(\ell)$ *for $\ell \geq 1$.*

Now we are ready to count the number of orientable coverings over a bordered non-orientable surface. Recall that the fundamental group $\pi_1(\mathcal{B})$ of a bordered surface $\mathcal{B}$ of Euler characteristic $\chi = 1 - r$, $r > 0$, is a free group F_r of rank r. An example of such a surface is the Möbius strip with $r - 1$ holes. An equivalent statement of the following theorem for the number of balanced $2n$-fold coverings of a unbalanced graph B_r was obtained in [19].

Theorem 3.11. *Let $\mathcal{B}$ be a bordered non-orientable surface with the fundamental group $\pi_1(\mathcal{B}) = F_r$. Then the number of orientable $2n$-fold coverings of $\mathcal{B}$ is given by the formula*

$$\mathrm{Isoc}^O(\mathcal{B};2n) = \frac{1}{2n} \sum_{\substack{\ell|n \\ \ell\, m=n}} (\varphi_{2m(r-1)+1}(\ell)\, s_{F_{2r-1}}(m) + \varphi_{m(r-1)+1}^{odd}(\ell)\, s_{F_r}^-(m)),$$

where $\varphi_r(\ell)$ and $\varphi_r^{odd}(\ell)$ are the Jordan functions, $s_{F_r}(m)$ is the numbers of subgroups of index m, and $s_{F_r}^-(m)$ is the numbers of non-orientable subgroups of index m in the group F_r.

The proof is based on the following arguments. By Theorem 3.6. for $\Gamma = F_r$ we have

$$c_{\Gamma}^{+}(2n) = \frac{1}{2n} \sum_{\substack{\ell | n \\ \ell\, m=n}} \left(\sum_{K^{+} <_m \Gamma^{+}} \operatorname{Epi}(K^{+}, \mathbb{Z}_{\ell}) + \sum_{K^{-} <_m \Gamma} \operatorname{Epi}^{+}(K^{-}, \mathbb{Z}_{2\ell}) \right),$$

where the sum $\sum_{K^{-} <_m \Gamma}$ is taken over all non-orientable subgroups of index m in the group Γ, and $\operatorname{Epi}^{+}(K^{-}, \mathbb{Z}_{2\ell})$ is the set of epimorphisms of the group K^{-} onto a cyclic group $\mathbb{Z}_{2\ell}$ with orientable kernel.

By the Schreier theorem, the subgroup Γ^{+} of index two in the free group $\Gamma = F_r$ is isomorphic to a free group F_{2r-1}. Consider the first term of the above formula. Again, by the Schreier theorem any subgroup of index m in the group F_{2r-1} is isomorphic to $F_{m(r-1)+1}$ and the number of such subgroups is equal to $s_{F_{2r-1}}(m)$. Moreover, by Example 3.3.(i) we have $|\operatorname{Epi}(K^{+}, \mathbb{Z}_{\ell})| = \varphi_{m(r-1)+1}(\ell)$. Hence, one can write

$$\sum_{\substack{\ell | n \\ \ell\, m=n}} \sum_{K^{+} <_m \Gamma} |\operatorname{Epi}(K^{+}, \mathbb{Z}_{\ell})| = \sum_{\substack{\ell | n \\ \ell\, m=n}} \varphi_{2m(r-1)+1}(\ell)\, s_{F_{2r-1}}(m).$$

By similar arguments, any non-orientable subgroup $K^{-} <_m \Gamma$ is isomorphic to $F_{m(r-1)+1}$. We note that the number of such subgroups is equal to $s_{F_r}^{-}(m)$. By Proposition 3.10. we have $|\operatorname{Epi}^{+}(K^{-}, \mathbb{Z}_{2\,\ell})| = \varphi_{m(r-1)+1}^{odd}(\ell)$. Hence, the second summand of the formula for $c_{\Gamma}^{+}(2n)$ can be equivalently rewritten as $\sum_{\substack{\ell | n \\ \ell\, m=n}} \varphi_{m(r-1)+1}^{odd}(\ell)\, s_{F_r}^{-}(m)$. □

Remark. By applying the same argument to the fundamental group of a closed non-orientable surface we obtain an alternating proof of the Theorem 2.11.

Let $\mathcal{K}$ be a Klein bottle, that is a closed non-oriented surface of genus 2. It was shown in [5] and [16, 28] that the number $N_{\mathcal{K}}(n)$ of n-fold coverings of $\mathcal{K}$ can be expressed in terms of classical number-theoretical functions.

Recall that any positive integer n can be uniquely represented in the form $n = 2^s \cdot n^{-}$, where $s \geq 0$ and n^{-} is an *odd* part of n.

Now, as a corollary of Theorem 3.11 we give a simple formula for $N_{\mathcal{K}}^{-}(n)$ obtained earlier in [28].

Theorem 3.12. *Let $\mathcal{K}$ be a Klein bottle. Then the number of non-orientable n-fold coverings of $\mathcal{K}$ is given by the formula*

$$N_{\mathcal{K}}^{-}(n) = (2, n)\, d(n^{-}),$$

where n^{-} is the odd part of n and $d(n)$ is the number of positive divisors of n.

3.3 *Reflexible coverings and chiral pairs*

Let $\mathcal{M}$ be a connected non-orientable manifold with fundamental group $\Gamma = \pi_1(\mathcal{M})$. Suppose that Γ acts by homeomorphisms on the universal covering $\tilde{\mathcal{M}}$ of the manifold $\mathcal{M}$. Note that the universal covering $\tilde{\mathcal{M}}$ is always orientable. Consider a subgroup Γ^{+} of index two in Γ consisting of all orientation preserving homeomorphisms of $\tilde{\mathcal{M}}$. Denote by $\mathcal{M}^{+}$ the orientable double of $\mathcal{M}$, then $\Gamma^{+} = \pi_1(\mathcal{M}^{+})$. The following facts from algebraic topology are well known.

Let $\pi : \mathcal{U} \to \mathcal{M}$ be an n-fold covering of $\mathcal{M}$. Then the fundamental group $K = \pi_1(\mathcal{U})$ is contained as a subgroup of index n in the group $\Gamma = \pi_1(\mathcal{M})$. Conversely, any subgroup on index n

in Γ is the fundamental group of an n-fold covering of $\mathcal{M}$. Moreover, if $\mathcal{U}$ is orientable then the number $n = 2m$ is even and the group K is contained as a subgroup of index m in the group Γ^+.

Two twins are non-equivalent as coverings of $\mathcal{M}^+$, but have to be equivalent as coverings of $\mathcal{M}$. Note that every regular covering is reflexible. The folding number of any reflexible covering should be even.

Recall that two coverings $\pi : \mathcal{U} \to \mathcal{M}^+$ and $\pi' : \mathcal{U}' \to \mathcal{M}^+$ are equivalent if and only if the corresponding subgroups $\pi_1(\mathcal{U})$ and $\pi_1(\mathcal{U}')$ are conjugate in Γ^+.

The following theorem is a consequence of Theorems 3.1 and 3.5.

Theorem 3.13. *Let $\mathcal{M}$ be a connected non-orientable manifold with finitely generated fundamental group Γ. Then the number of $2n$-fold reflexible coverings of $\mathcal{M}$ is given by the formula*

$$a_\Gamma(n) = \frac{1}{n} \sum_{\substack{\ell \mid n \\ \ell\, m = n}} \sum_{K^- <_m \Gamma} |\mathrm{Epi}^+(K^-, \mathbb{Z}_{2\ell})|,$$

where the sum $\sum_{K^- <_m \Gamma}$ is taken over all non-orientable subgroups of index m in the group Γ and $\mathrm{Epi}^+(K, \mathbb{Z}_\ell)$ is the set of epimorphisms of the group K onto a cyclic group $\mathbb{Z}_\ell$ of order ℓ with orientable kernel.

To prove the theorem we set

$$I(n) = \frac{1}{n} \sum_{\substack{\ell \mid n \\ \ell\, m = n}} \sum_{K^- <_m \Gamma} |\mathrm{Epi}^+(K^-, \mathbb{Z}_{2\ell})|.$$

Let Γ^+ be the positive subgroup of Γ and $\Gamma = \Gamma^+ + \sigma\,\Gamma^+$ is a coset decomposition. Let K be a subgroup of Γ^+. Denote by $[K]_{\Gamma^+}$ and $[K]_\Gamma$ the conjugacy class of K in Γ^+ and Γ, respectively.

There are two kinds of subgroups K in Γ^+. Either *reflexible* with the property $[K]_{\Gamma^+} = [K^\sigma]_{\Gamma^+} = [K]_\Gamma$ or *twin* with $[K]_{\Gamma^+} \neq [K^\sigma]_{\Gamma^+}$ and $[K]_\Gamma = [K]_{\Gamma^+} \cup [K^\sigma]_{\Gamma^+}$. By definition, the set of all orientable subgroups is disjoint union of reflexible and twin subgroups. Denote by $a_\Gamma(n)$ and $t_\Gamma(n)$ the numbers of conjugacy classes of reflexible and twin subgroups of index $2n$ in the group Γ, respectively. Now we calculate the numbers of orientable subgroups of index $2n$ up to conjugacy in Γ and Γ^+. We get

$$\begin{aligned} c_\Gamma^+(2n) &= a_\Gamma(n) + t_\Gamma(n) \\ c_{\Gamma^+}(n) &= a_\Gamma(n) + 2\,t_\Gamma(n). \end{aligned}$$

From Theorem 3.6 we have

$$c_\Gamma^+(2n) = \frac{1}{2}(\,c_{\Gamma^+}(n) + I(n)).$$

Hence,

$$a_\Gamma(n) = 2c_\Gamma^+(2n) - c_{\Gamma^+}(n) = (c_{\Gamma^+}(n) + I(n)) - c_{\Gamma^+}(n) = I(n). \qquad \square$$

Also, since $t_\Gamma(n) = \frac{1}{2}(c_{\Gamma^+}(n) - a_\Gamma(n))$ we obtain

Proposition 3.14. *Let $\mathcal{M}^+$ be the orientable double of a non-orientable manifold $\mathcal{M}$. Then the number of chiral pairs of n-fold coverings of $\mathcal{M}^+$ is given by the formula*

$$t_\Gamma(n) = \frac{c_{\Gamma^+}(n) - a_\Gamma(n)}{2},$$

where Γ^+ is the fundamental group of $\mathcal{M}^+$, and $c_{\Gamma^+}(n)$ and $a_\Gamma(n)$ are determined by Theorems 3.1 *and* 3.13*, respectively.*

We illustrate results of the last section by the following example.

Let $\mathcal{M} = \mathcal{K}$ be the Klein bottle with fundamental group

$$\Gamma = \pi_1(\mathcal{K}) = \langle x, y \mid xyxy^{-1} = 1\rangle.$$

The orientable double of $\mathcal{K}$ is a torus $\mathcal{T}$ with fundamental group

$$\Gamma^+ = \pi_1(\mathcal{T}) = \langle a, b \mid [a, b] = 1\rangle,$$

where $a = x$ and $b = y^2$. We note that $\Gamma = \Gamma^+ + \Gamma^+ y,\ yay^{-1} = a^{-1}$, and $yby^{-1} = b$.

Set $n = 5$. Then, by direct calculation from Theorems 3.12. and 3.13. we obtain

$$c_\Gamma^+(10) = a_\Gamma(5) + t_\Gamma(5) = 4$$
$$c_{\Gamma^+}(5) = a_\Gamma(5) + 2\,t_\Gamma(5) = 6.$$

Hence, $a_\Gamma(5) = t_\Gamma(5) = 2$. That is the group Γ^+ has six (conjugacy classes of) subgroups producing coverings. Two of them, $\langle a^5, b\rangle$ and $\langle a, b^5\rangle$ are reflexible and other four are divided into chiral pairs. They are $\langle a^2 b, a^{-1}b^2\rangle$, $\langle a^{-2}b, ab^2\rangle$ and $\langle ab, a^{-2}b^3\rangle$, $\langle a^{-1}b, a^2b^3\rangle$, respectively. The twin subgroups in chiral pairs are not conjugate in Γ^+ but do conjugate by element y in group Γ.

The above results form a background for counting chiral pairs of maps (in particular, chiral polyhedra) [24]. The general formula for the number of reflexible coverings (Theorem 3.13) allows also to count self-dual and Petri-dual combinatorial objects.

3.4 *All connected or disconnected coverings of manifold*

In this section we calculate the number of non-equivalent coverings (connected or not) over a connected manifold with an arbitrary finitely generated fundamental group.

Let $p : \mathcal{U} \to \mathcal{M}$ be (possibly disconnected) covering over connected manifold $\mathcal{M}$. Then every path $\gamma \in \mathcal{M}$ has a unique lift $\widetilde{\gamma}$ starting at a given point of $p^{-1}(\gamma(0))$, so we obtain a well-defined map $L_\gamma : p^{-1}(\gamma(0)) \to p^{-1}(\gamma(1))$ by sending the starting point $\widetilde{\gamma}(0)$ of each lift $\widetilde{\gamma}$ to its ending point $\widetilde{\gamma}(1)$. By the monodromy theorem, L_γ depends only on homotopy class of γ. This means that the association $\gamma \mapsto L_\gamma$ gives a homomorphisms from $\pi_1(\mathcal{M}, x_0)$ to the group of permutations of $p^{-1}(x_0)$. It gives an action of $\pi_1(\mathcal{M}, x_0)$ on the fiber $p^{-1}(x_0)$. We note that this action is transitive if and only if the covering manifold $\mathcal{U}$ is connected. Moreover, the number of orbits of the action coincides with the number of connected components of the covering.

Two coverings $p_1 : \mathcal{U}_1 \to \mathcal{M}$ and $p_2 : \mathcal{U}_2 \to \mathcal{M}$ are equivalent if and only if the corresponding actions of $\pi_1(\mathcal{M}, x_0)$ on the fibers F_1 and F_2 over x_0 are isomorphic. This shows that n-sheeted coverings spaces of $\mathcal{M}$ are classified by equivalence classes of homomorphisms $\rho : \pi_1(\mathcal{M}, x_0) \to \mathbf{S}_n$, where is $\mathbf{S}_n$ is the symmetric group on n symbols and the equivalence relation identifies a homomorphisms ρ with each of its conjugates $h^{-1}\rho\, h$ by elements $h \in \mathbf{S}_n$.

All the above mentioned results remains to be true for any path-connected, locally path-connected and semilocally simply connected topological space $\mathcal{M}$. See, for example ([2], Ch. 1.3). In particular, they are true for finite graphs.

This approach allows to prove the following result obtained in [6].

Theorem 3.15. *Let $\mathcal{M}$ be a connected manifold with finitely generated fundamental group Γ. Denote by b_n the number of non-equivalent (connected or disconnected) n-fold coverings of $\mathcal{M}$ and set $b(x) = 1 + b_1 x + b_2 x^2 + \cdots$. Then*

$$b(x) = \exp\left(\sum_{n=1}^{\infty} \frac{1}{n} \sum_{\ell m = n} \sum_{K <_m \Gamma} |\mathrm{Hom}(K, \mathbb{Z}_\ell)|\, x^n\right),$$

where the sum $\sum_{K\ <_m \Gamma}$ is taken over all subgroups K of index m in the group Γ and Hom $(K,\ \mathbb{Z}_\ell)$ *is the set of homomorphisms of the group K into a cyclic group $\mathbb{Z}_\ell$ of order ℓ.*

We note that relevant results were obtained by Hirotaka Tamanoi in [22] and [23]. Let

$$c_n = \frac{1}{n} \sum_{\substack{\ell | n \\ \ell\, m = n}} \sum_{K <_m \Gamma} |\mathrm{Epi}\,(K,\ \mathbb{Z}_\ell)|$$

be the number of connected n-fold coverings given by Theorem 3.1. The following lemma gives a relation between the numbers of connected coverings and all coverings. For similar results see ([3], p. 113) and [29].

Lemma 3.16. *The number c_n of connected and the number b_n of all non-equivalent n-fold coverings are related by the Euler transformation*

$$b(x) = 1 + b_1 x + b_2 x^2 + \cdots = \prod_{i=1}^{\infty} \frac{1}{(1 - x^i)^{c_i}}.$$

The proof of Lemma 3.16 is based on the following arguments. Denote by $\mathfrak{S}$ the set of equivalency classes of all connected coverings of finite multiplicity of a manifold $\mathcal{M}$. Let $\mathfrak{D} = \mathbb{N}\mathfrak{S}$ be the set of all finite linear combinations of the type $m_1 C_1 + m_2 C_2 + \cdots + m_k C_k$, where $m_1, m_2, \ldots, m_k \in \mathbb{N}$ and $C_1, C_2, \ldots, C_k \in \mathfrak{S}$. We identify $\mathfrak{D}$ with the set of equivalence classes of all coverings of finite multiplicity of a manifold $\mathcal{M}$.

Define $\mu : \mathfrak{S} \to \mathbb{N}$ to be the multiplicity of a covering. For any $d = m_1 C_1 + m_2 C_2 + \cdots + m_k C_k \in \mathfrak{D}$ we set $\mu(d) = m_1 \cdot \mu(C_1) + m_2 \cdot \mu(C_2) + \cdots + m_k \cdot \mu(C_k)$. Then $c_n = |(a \in \mathfrak{S} : \mu(a) = n)|$ and $b_n = |(d \in \mathfrak{D} : \mu(d) = n)|$ are the numbers of equivalency classes of connected and all n-fold coverings, respectively.

Let $C_1^i, C_2^i, \ldots, C_{a_i}^i \in \mathfrak{S}$ be the list of equivalence classes of all i-fold connected coverings for any $i = 1, 2, \ldots$. Then any n-fold covering, up to equivalency, can be uniquely represented as $C = \sum_{i=1}^n \sum_{j=1}^{a_i} m_j^i C_j^i$ for some non-negative integers m_j^i satisfying $\mu(C) = n$. Since $\mu(C_j^i) = i$, the last condition is equivalent to $\sum_{i=1}^n \sum_{j=1}^{a_i} i \cdot m_j^i = n$. Hence, b_n coincides with the number of non-negative solutions of above equation. We set also $b_0 = 1$. Then we have

$$b_n x^n = \sum_{\sum_{i=1}^n \sum_{j=1}^{a_i} i \cdot m_j^i = n} \ \prod_{i=1}^{n} \prod_{j=1}^{a_i} x^{i \cdot m_j^i}$$

and, consequently,

$$b_0 + b_1 x + b_2 x^2 + \cdots = \prod_{i=1}^{\infty} (1 + x^i + x^{2i} + \cdots)^{c_i} = \prod_{i=1}^{\infty} \frac{1}{(1 - x^i)^{c_i}}.$$

1. The number of coverings of a circle

In this case $\Gamma = \pi_1(S^1) = \mathbb{Z}$. The number of n-fold coverings of S^1 is given by the Hardy-Ramanujan partition function $p(n)$, where

$$p(0) + p(1)\,x + p(2)\,x^2 + \cdots = \prod_{i=1}^{\infty}(1 - x^i)^{-1}.$$

In particular,

$$p(0) = 1, p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5, p(5) = 7, p(6) = 11.$$

2. The number of coverings of a graph

Let G be a finite connected graph with Betti number $r = \beta(G)$. Then $\Gamma = \pi_1(G) = F_r$ is a free group of rank r. By Theorem 2.2 we have

$$b_n = \sum_{c_1+2c_2+\cdots+nc_n=n} \prod_{i=1}^{n}(i^{c_i}\,c_i!)^{r-1}.$$

This result was obtained in [10] and used in [14] to calculate the number of connected coverings of the graph G. This number coincides with the number of conjugacy classes of subgroups of index n in free group F_r obtained earlier in [12]. Lemma 3.16 gives a positive answer of J.H. Kwak's question how relate the results of papers [14] and [12].

3. The number of coverings of a closed orientable surface

Let S_k be a closed orientable surface of genus k and $\Gamma = \pi_1(S_k)$. By the Riemann-Hurwitz formula, any subgroup K of index m in Γ is isomorphic to $\pi_1(S_{k'})$, where $2k' = (2k-2) + 2m$. Since $H_1(K) = \mathbb{Z}^{2k'}$ we have $|\mathrm{Hom}\,(K, \mathbb{Z}_\ell)| = |\mathrm{Hom}(H_1(K), \mathbb{Z}_\ell)| = \ell^{(2k-2)m+2}$. Hence, $\sum_{K<_m\Gamma} |\mathrm{Hom}(K, \mathbb{Z}_\ell)| = \ell^{(2k-2)m+2}\,s_k(m)$, where $s_k(m)$ is the number of subgroups of index m in $\pi_1(S_k)$, given by Theorem 2.8.

Putting this into the statement of Theorem 3.15 we get

$$b(x) = \exp\left(\sum_{n=1}^{\infty}\sum_{\ell m=n} \ell^{(2g-2)m+2}\,s_k(m)\,\frac{x^n}{n}\right).$$

Example 3.17. Let $b_n = \mathrm{Iso}\,(S_k; n)$ be the number of connected or disconnected n-fold coverings of a closed orientable surface S_k of genus k, and $\nu = 2k - 2$. Then

$$\mathrm{Iso}\,(S_k; 2) = 4 \cdot 2^\nu$$

$$\mathrm{Iso}\,(S_k; 3) = 2 \cdot (2^\nu + 2 \cdot 3^\nu + 6^\nu)$$

$$\mathrm{Iso}\,(S_k; 4) = 3 \cdot 3^\nu + 9 \cdot 4^\nu + 6 \cdot 8^\nu + 12^\nu + 2 \cdot 24^\nu.$$

4. The number of coverings of a torus

The fundamental group $\Gamma = \pi_1(S_1)$ of torus S_1 is isomorphic to a free abelian group $\mathbb{Z}^2$. By [5] we have $s_\Gamma(n) = \sigma(n)$, where $\sigma(n) = \sum_{d|n} d$ is the sum of positive divisors of n. By Theorem 3.15 we obtain

$$b(x) = \exp\left(\sum_{n=1}^{\infty}\sum_{\ell\, m=n} \ell^2\,\sigma(m)\,\frac{x^n}{n}\right).$$

In particular, the sequence b_n is given by

$$1, 4, 8, 21, 39, 92, 170, 360, 667, 1316, 2393, 4541, 8100, 14824, 26071$$

for $n = 1, 2, \ldots, 15$. This is sequence A061256 from the On-Line Encyclopedia of Integer Sequences [30].

4 REGULAR COVERINGS OF MANIFOLDS

4.1 *Regular $\mathcal{A}$-coverings*

In this section we enumerate the regular coverings of a manifold $\mathcal{M}$ with prescribed finite covering transformation group $\mathcal{A}$. It will be done in terms of the Möbius function defined on the lattice of subgroup of $\mathcal{A}$ by P. Hall [31]. G. Jones ([16], [17]) used such Möbius function to find a method for counting normal subgroups of a surface group and a crystallographic group, and applied it to count some covering surfaces. The same approach has been used in [32] to calculate regular branched coverings of a bordered surface. A covering $p : \tilde{\mathcal{M}} \to \mathcal{M}$ (connected of disconnected) is *regular* if the covering transformation group

$$\mathrm{Cov}(\tilde{\mathcal{M}}, \mathcal{M}) = \{h \in \mathrm{Home}(\tilde{\mathcal{M}}) : p = p \circ h\}$$

has a subgroup $\mathcal{A}$ which acts transitively on each fibre of p and has no fixed points. If $\tilde{\mathcal{M}}$ is connected then $\mathcal{A} = \mathrm{Cov}(\tilde{\mathcal{M}}, \mathcal{M})$ and the later condition can be omitted. We call p simply an $\mathcal{A}$-covering. Two $\mathcal{A}$-coverings $p : \tilde{\mathcal{M}} \to \mathcal{M}$ and $q : \mathcal{M}' \to \mathcal{M}$ are equivalent (or isomorphic) if there exists a homeomorphism $h : \tilde{\mathcal{M}} \to \tilde{\mathcal{M}}'$ such that $p = q \circ h$. For a connected $\mathcal{A}$-covering p, the fibre F can be identified with the set of elements of the group $\mathcal{A}$. Then the action of $\pi_1(\mathcal{M}, x_0)$ on the fiber $p^{-1}(x_0)$ coincides with action of the group $\mathcal{A}$ on itself by the right multiplication. That is, an epimorphism $\varphi : \pi_1(\mathcal{M}, x_0) \to \mathcal{A}$ is well defined. Moreover, for any $\tilde{x}_0 \in p^{-1}(x_0)$ the image $p^*\pi_1(\tilde{\mathcal{M}}, \tilde{x}_0)$ of the fundamental group $\pi_1(\tilde{\mathcal{M}}, x_0)$ under the canonical projection $p^* : \pi_1(\tilde{\mathcal{M}}, \tilde{x}_0) \to \pi_1(\mathcal{M}, x_0)$ coincides with kernel of epimorphism $\phi : \pi_1(\mathcal{M}, x_0) \to \mathcal{A}$. Two epimorphisms $\varphi : \pi_1(\mathcal{M}, x_0) \to \mathcal{A}$ and $\psi : \pi_1(\mathcal{M}, x_0) \to \mathcal{A}$ share the same kernel if and only if there is an automorphism $\alpha \in \mathrm{Aut}(\mathcal{A})$ such that $\psi = \alpha \circ \varphi$. This shows that $\mathcal{A}$-coverings of $\mathcal{M}$ are classified by equivalence classes of epimorphisms $\varphi : \pi_1(\mathcal{M}, x_0) \to \mathcal{A}$, and the equivalence relation identifies an epimorphism ϕ with each of epimorphism $\alpha \circ \varphi$, where $\alpha \in \mathrm{Aut}(\mathcal{A})$. As a result, we have that the number of non-equivalent $\mathcal{A}$-coverings of a connected manifold $\mathcal{M}$ with the fundamental group $\Gamma = \pi_1(\mathcal{M}, x_0)$ and the number $|\mathrm{Epi}(\Gamma, \mathcal{A})|$ of epimorphisms of Γ onto the group $\mathcal{A}$ are related by

$$\mathrm{Isoc}\,(\mathcal{M}, \mathcal{A}) = \frac{|\mathrm{Epi}(\Gamma, \mathcal{A})|}{|\mathrm{Aut}(\mathcal{A})|}.$$

By using a similar argument in Section 2, we can have the following result obtained by G. Jones [16].

Theorem 4.1. *The number of connected $\mathcal{A}$-coverings of a manifold $\mathcal{M}$ with finitely generated fundamental group Γ is given by the formula*

$$\mathrm{Isoc}\,(\mathcal{M}; \mathcal{A}) = \frac{1}{|\mathrm{Aut}\,(\mathcal{A})|} \sum_{K \le \mathcal{A}} \mu(K) |\mathrm{Hom}(\Gamma, K)|.$$

In particular, for the cyclic group $\mathcal{A} = \mathbb{Z}_\ell$ from the above theorem and Lemma 3.2 we have

Theorem 4.2. *Let $\mathcal{M}$ be a connected manifold with finitely generated fundamental group $\Gamma = \pi_1(\mathcal{M})$ and $H_1(\Gamma) = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_s}$. Then*

$$\operatorname{Isoc}(\mathcal{M}, \mathbb{Z}_\ell) = \frac{1}{\varphi(\ell)} \sum_{d\,|\,\ell} \mu\left(\frac{\ell}{d}\right)(k_1, d)(k_2, d)\cdots(k_s, d),$$

where $\mu(\ell)$ is the Möbius function and (k, d) is the greatest common divisor of k and d.

By applying Theorem 4.1 to a bordered surface $\mathcal{D}_r$ of Euler characteristic $\chi = 1 - r$, we have the following theorem obtained in [32]. (The definition of a branched covering will be given in the next section.)

Theorem 4.3. *For any finite group $\mathcal{A}$, the number of connected branched $\mathcal{A}$-coverings of $\mathcal{D}_r$ with branched set B, $|B| = b \geq 0$, is given by formula*

$$\operatorname{Isoc}(\mathcal{D}_r, B; \mathcal{A}) = \frac{1}{|\operatorname{Aut}(\mathcal{A})|} \sum_{H \leq \mathcal{A}} \mu(H)(|H| - 1)^b |H|^r,$$

where the sum is taken over all subgroups H of the group $\mathcal{A}$ and $0^b = 1$ if $b = 0$.

In particulary, we have

$$\operatorname{Isoc}(\mathcal{D}_r, B; \mathbb{Z}_n) = \frac{1}{\varphi(n)} \sum_{m|n} \mu\left(\frac{n}{m}\right)(m-1)^b m^r,$$

$$\operatorname{Isoc}(\mathcal{D}_r, B; \mathbb{D}_n) = \frac{1}{\varphi(n)} \sum_{m|n} \mu\left(\frac{n}{m}\right)[(2m-1)^b 2^r - (m-1)^b] m^{r-1}$$

for $n \geq 3$ and

$$\operatorname{Isoc}(\mathcal{D}_r, B; \mathbb{D}_2) = \frac{1}{6}(3^b \cdot 4^r - 3 \cdot 2^r + 2 \cdot 0^b).$$

4.2 *Cyclic coverings of non-orientable manifolds*

In this section we calculate orientable and non-orientable cyclic coverings of a non-orientable manifold. Let $\mathcal{M}$ be a non-orientable manifold with a finitely generated fundamental group $\Gamma = \pi_1(\mathcal{M})$. Suppose that the groups $\Gamma = (\Gamma, \omega)$ and $\mathcal{A} = (\mathcal{A}, \eta)$ are endowed by orientations ω and η, respectively. Especially, we are interested in the case when $\Gamma^+ = \operatorname{Ker}(\omega)$ and $\mathcal{A}^+ = \operatorname{Ker}(\eta)$ are the subgroups of orientation preserving homeomorphisms in Γ and $\mathcal{A}$. Denote by $\operatorname{Epi}^+(\Gamma, \mathcal{A})$ and $\operatorname{Epi}^-(\Gamma, \mathcal{A})$ the sets of epimorphisms of the group Γ onto the group $\mathcal{A}$ with orientable and non-orientable kernel, respectively.

Let $\mathcal{A} = \mathbb{Z}_{2\ell}$ be a cyclic group and $\mathcal{A}^+ = \mathbb{Z}_\ell$. By a slight modification of arguments in [16] we have the following proposition.

Proposition 4.4. *Let $\mathcal{M}$ be a connected non-orientable manifold with the fundamental group Γ and $\mathcal{A} = \mathbb{Z}_{2\ell}$. Then the numbers of orientable and non-orientable $\mathcal{A}$-coverings of $\mathcal{M}$ are given by the formulas*

(1) $\operatorname{Isoc}^+(\mathcal{M}, G) = |\operatorname{Epi}^+(\Gamma, G)|/|\operatorname{Aut}(G)|$,
(2) $\operatorname{Isoc}^-(\mathcal{M}, G) = |\operatorname{Epi}^-(\Gamma, G)|/|\operatorname{Aut}(G)|$.

Combining the above result with Theorems 4.2 and 3.9 we obtain the following

Theorem 4.5. *Let $\mathcal{M}$ be a non-orientable manifold with the fundamental group Γ and*

$$H_1(\Gamma) = \mathbb{Z}_{k_1}^{\varepsilon_1} \oplus \mathbb{Z}_{k_2}^{\varepsilon_2} \oplus \cdots \oplus \mathbb{Z}_{k_n}^{\varepsilon_n}$$

is the oriented homology group. Then the number $\operatorname{Isoc}^+(\mathcal{M}, \mathbb{Z}_{2\ell})$ *of cyclic orientable $2n$-fold coverings of $\mathcal{M}$ are given by the formula*

$$\frac{1}{\varphi(2\ell)} \prod_{j=1}^{n} \frac{1+\varepsilon_j^{\frac{k_j}{(k_j,\ell)}}}{2} \sum_{\substack{m \\ \frac{\ell}{m}:\text{odd}}} \mu\left(\frac{\ell}{m}\right)(k_1,\, m)(k_2,\, m)\cdots(k_n,\, m).$$

Moreover, we have $\operatorname{Isoc}^-(\mathcal{M}, \mathbb{Z}_{2\ell}) = \operatorname{Isoc}(\mathcal{M}, \mathbb{Z}_{2\ell}) - \operatorname{Isoc}^+(\mathcal{M}, \mathbb{Z}_{2\ell})$, *where* $\operatorname{Isoc}(\mathcal{M}, \mathbb{Z}_{2\ell})$ *is given by Theorem 4.2.*

As a consequence, taking into account Proposition 3.10 we obtain the following two theorems

Theorem 4.6. *Let $\mathcal{S}$ be a bordered non-orientable surface with the fundamental group F_r. The number of orientable and non-orientable cyclic coverings of $\mathcal{S}$ with the covering group $\mathbb{Z}_\ell$ is given by the formulas*

(1) $\operatorname{Isoc}^+(\mathcal{S}, \mathbb{Z}_\ell) = \dfrac{2^r - (2,\ell)}{2^r - 1}\dfrac{\varphi_r(\ell)}{\varphi(\ell)}$,

(2) $\operatorname{Isoc}^-(\mathcal{S}, \mathbb{Z}_\ell) = \dfrac{(2,\ell) - 1}{2^r - 1}\dfrac{\varphi_r(\ell)}{\varphi(\ell)}$.

Theorem 4.7. *Let S be a closed non-orientable surface of genus p. Then the number of orientable and non-orientable cyclic coverings of $\mathcal{S}$ is given by the formulas*

(1) $\operatorname{Isoc}^-(\mathcal{S}, \mathbb{Z}_\ell) = 0$ *for* ℓ odd,

(2) $\operatorname{Isoc}^+(\mathcal{S}, \mathbb{Z}_{2\ell}) = (2,\ell)\dfrac{1+(-1)^{p(\ell-1)}}{2}\dfrac{\varphi_{p-1}^{\text{odd}}(\ell)}{\varphi(\ell)}$ *for* $\ell \geq 1$,

(3) $\operatorname{Isoc}^-(\mathcal{S}, \mathbb{Z}_{2\ell}) = 2(2^{p-1} - (2,\ell,p))\,\dfrac{\varphi_{p-1}^{\text{odd}}(\ell)}{\varphi(\ell)}$ *for* $\ell \geq 1$, *where* $(2,\ell,p) = \operatorname{GCD}(2,\ell,p)$.

Let $\mathcal{A}$ is an arbitrary finite group. Then there are, in general a few different subgroups $\mathcal{A}^+$ of index two in $\mathcal{A}$. Denote by $\operatorname{Epi}((\Gamma,\Gamma^+),(\mathcal{A},\mathcal{A}^+))$ the set of epimorphisms Γ to $\mathcal{A}$ sending Γ^+ to $\mathcal{A}^+$ and by $\operatorname{Aut}(\mathcal{A},\mathcal{A}^+)$ the set of automorphisms of $\mathcal{A}$ keeping $\mathcal{A}^+$ invariant.

We have to pass through all equivalence classes of subgroups of index two in $\mathcal{A}$ up to $\operatorname{Aut}(\mathcal{A})$ action to get the following result [33].

Theorem 4.8. *Let $\mathcal{M}$ be a connected non-orientable manifold with the fundamental group Γ and $\mathcal{A}$ is a finite group. Then the number of orientable $\mathcal{A}$-coverings of $\mathcal{M}$ is given by the formula*

$$\operatorname{Isoc}^+(\mathcal{M}, \mathcal{A}) = \sum_{\mathcal{A}^+} \frac{|\operatorname{Epi}((\Gamma,\Gamma^+),(\mathcal{A},\mathcal{A}^+))|}{|\operatorname{Aut}(\mathcal{A},\mathcal{A}^+)|},$$

where $\mathcal{A}^+$ runs over all representatives of equivalence classes of subgroups of index two in $\mathcal{A}$ up to $\operatorname{Aut}(\mathcal{A})$ *action.*

5 BRANCHED SURFACE COVERINGS

5.1 *Branched coverings with prescribed branch sets*

Let $\tilde{X}$ and X be compact surfaces, and let $p : \tilde{X} \to X$ be a continuous surjection. We call $p : \tilde{X} \to X$ a *branched covering* if there is a finite subset B of points in X such that the restriction $p|_{\tilde{X}-p^{-1}(B)} : \tilde{X} - p^{-1}(B) \to X - B$ is a covering. The smallest subset B of X with the above property is called the *branch set* of p. We refer to $p|_{\tilde{X}-p^{-1}(B)}$ as a *covering associated with* the branched covering p. Notice that if B is empty, then $p : \tilde{X} \to X$ is a covering. A branched covering $p : \tilde{X} \to X$ is *regular* if the associated covering is regular, that is, it means by definition, there exists a (finite) group $\mathcal{A}$ which acts pseudofreely on $\tilde{X}$ so that the space X is homeomorphic to the quotient space $\tilde{X}/\mathcal{A}$, say by h, and the quotient map $\tilde{X} \to \tilde{X}/\mathcal{A}$ is the composition $h \circ p$ of p and h. In this case, the group $\mathcal{A}$ is the group of covering transformations of the branched covering $p : \tilde{X} \to X$. If the branched covering $p : \tilde{X} \to X$ is regular with the group $\mathcal{A}$ of covering transformations, then we call it simply a *branched $\mathcal{A}$-covering*.

Two branched coverings $p_i : \tilde{X}_i \to X$ $(i = 1, 2)$ are *equivalent* if there exists a homeomorphism $\tilde{h} : \tilde{X}_1 \to \tilde{X}_2$ such that $p_2 \circ \tilde{h} = \circ p_1$.

For a combinatorial description of the branched surface coverings, Hurwitz [34] introduced a system, now called *Hurwitz system*, and Gross and Tucker [35] introduced embedded voltage graphs. In fact, the Hurwitz system is a kind of voltage assignment on a bouquet of circles (see [36]). Let B_ℓ be the bouquet of ℓ circles and let $|B| = b$. Let $\mathbf{S}_r$ be the symmetric group on r letters and let $\mathcal{A}$ be a finite group. Let $C^1(B_{2h+b} \hookrightarrow S_h - B; r)$ (resp. $C^1(B_{2h+b} \hookrightarrow S_h - B; \mathcal{A})$) denote the subset of $\mathbf{S}_r^{2h+b}$ (resp. of $\mathcal{A}^{2h+b}$) consisting of all $(2h + b)$-tuples $(\sigma_1, \ldots, \sigma_{2h+b})$ (i.e., voltage assignments) that satisfy the following three conditions:

(C1) The subgroup $\langle \sigma_1, \ldots, \sigma_{2h+b} \rangle$ generated by $\{\sigma_1, \ldots, \sigma_{2h+b}\}$ is transitive on $\{1, 2, \ldots, r\}$ (resp. is the full group $\mathcal{A}$),

(C2) $\prod_{i=1}^{h} \sigma_i \sigma_{h+i} \sigma_i^{-1} \sigma_{h+i}^{-1} \prod_{i=1}^{b} \sigma_{2h+i} = 1,$

(C3) $\sigma_i \neq 1$ for each $i = 2h + 1, \ldots, 2h + b$.

Kwak et al. [36] suggested the following version of Hurwitz existence and classification theorem on branched surface coverings.

Theorem 5.1. (Existence and classification of branched coverings) *Let S be an orientable surface S_h of genus h, and let B be a set of b points in S. Every element ϕ in $C^1(B_{2h+b} \hookrightarrow S - B; r)$ induces a connected branched r-fold covering $\tilde{p}_\phi : S^\phi \to S$ of S with branch set B. Conversely, every connected branched r-fold covering of S with branch set B can be derived from an element in $C^1(B_{2h+b} \hookrightarrow S - B; r)$. Furthermore, for two such elements $\phi_1 = (\sigma_1, \ldots, \sigma_{2h+b})$ and $\phi_2 = (\sigma'_1, \ldots, \sigma'_{2h+b})$, the derived branched coverings $\tilde{p}_{\phi_1} : S^{\phi_1} \to S$ and $\tilde{p}_{\phi_2} : S^{\phi_2} \to S$ are isomorphic if and only if there exists a permutation $\alpha \in \mathbf{S}_r$ such that*

$$\sigma'_i = \alpha \sigma_i \alpha^{-1}$$

for each $i = 1, 2, \ldots, 2h + b$.

Theorem 5.2. (Existence and classification of branched $\mathcal{A}$-coverings) *Let S be an orientable surface S_h of genus h, and let B be a set of b points in S. Every element ϕ in $C^1(B_{2h+b} \hookrightarrow S - B; \mathcal{A})$ induces a connected branched $\mathcal{A}$-covering $\tilde{p}_\phi : S^\phi \to S$ of S with branch set B. Conversely, every connected branched $\mathcal{A}$-covering of S with branch set B can be derived from an element in $C^1(B_{2h+b} \hookrightarrow S - B; \mathcal{A})$. Furthermore, for two such elements $\phi_1 = (\sigma_1, \ldots, \sigma_{2h+b})$ and*

$\phi_2 = (\sigma'_1, \ldots, \sigma'_{2h+b})$, the derived branched coverings $\tilde{p}_{\phi_1} : S^{\phi_1} \to S$ and $\tilde{p}_{\phi_2} : S^{\phi_2} \to S$ are isomorphic if and only there exists a group automorphism $\alpha \colon \mathcal{A} \to \mathcal{A}$ such that

$$\sigma'_i = \alpha(\sigma_i)$$

for each $i = 1, 2, \ldots, 2h + b$.

A corresponding result for a non-orientable surface N_k of genus k with the only difference being that B_{k+b} replaces B_{2h+b} and (C2)$'$ does (C2), where

$$\text{(C2)}' \prod_{i=1}^{k} \sigma_i \sigma_i \prod_{i=1}^{b} \sigma_{k+i} = 1.$$

In fact, the condition (C1) guarantees that the surface S^{ϕ} is connected, and the conditions (C2)(or (C2)$'$) and (C3) provide that the set B is the branch set of the branched covering $\tilde{p}_{\phi} : S^{\phi} \to S$.

We observe that every branched covering surface of an orientable surface is orientable, but that of a nonorientable surface can be orientable or nonorientable. The orientability of the derived branched covering surface can be determined as follows. It follows from Theorems 5.1 and 5.2 that branched coverings of the base surface are completely determined by the coverings of the punched surface which is the surface obtained by deleting the branch points from the base surface. For the nonorientable surface N_k, the punched surface $N_k - B$ is also nonorientable. The fundamental group of $N_k - B$ can be presented as follows;

$$\langle c_1, \ldots, c_k, d_1, \ldots, d_b : a_1^2 \cdots a_k^2 d_1 \cdots d_b = 1 \rangle.$$

The generators $c_1, \ldots, c_k$ are the curves whose tubular neighborhoods are Möbius bands and those of the generators $d_1, \ldots, d_b$ are annuli. Now, we consider an orientable covering of $N_k - B$. The Hurwitz system of this covering is the $(k + b)$-tuples of permutations in $\mathbf{S}_r$ which are determined by the liftings of the generators. Since every orientable surface contains no Möbius bands, the preimage of c_1 is consists of cycles of which each contains even number of points in the preimage of the bass point. Let's identify the preimage of the base point with the set $\{1, 2, \ldots, 2r\}$ so that the permutation determined by the liftings of c_1 reverses the parity. We denote it by σ_1. Let $\sigma_2, \ldots, \sigma_k$ be the permutations determined by the liftings of c_i for $i = 2, \ldots, k$ and $\sigma_{k+1}, \ldots, \sigma_{k+b}$ the permutations determined by those of d_i for $i = 1, \ldots, b$. Then the permutations $\sigma_2, \ldots, \sigma_k$ reverse the parity and $\sigma_{k+1}, \ldots, \sigma_{k+b}$ preserves the parity because the covering surface is orientable. The converse is also true. We summarize our discussion as follows.

Lemma 5.3. (Orientability criterion)

(1) *Let $\phi \in C^1(B_{k+b} \hookrightarrow N_k - B; r)$. Then the covering surface S^{ϕ} induced by ϕ is orientable if and only if r is even, $\sigma_1, \ldots, \sigma_k$ reverse the parity, and $\sigma_{k+1}, \ldots, \sigma_{k+b}$ preserve the parity.*

(2) *Let $\phi \in C^1(B_{k+b} \hookrightarrow N_k - B; \mathcal{A})$. Then the covering surface S^{ϕ} induced by ϕ is orientable if and only if there exists a subgroup $\mathcal{B}$ of index 2 in $\mathcal{A}$ such that $\sigma_1, \ldots, \sigma_k$ are elements of $\mathcal{A} - \mathcal{B}$ and $\sigma_{k+1}, \ldots, \sigma_{k+b}$ are elements of $\mathcal{B}$.*

We define an equivalence relation $\sim$ on the set of all transitive β-tuples $(\sigma_1, \ldots, \sigma_\beta)$ in $\mathbf{S}_r^{\beta}$ by $(\sigma_1, \ldots, \sigma_\beta) \sim (\sigma'_1, \ldots, \sigma'_\beta)$ if and only if there exists a permutation σ such that $\sigma\sigma_i\sigma = \sigma'_i$ for each $i = 1, 2, \ldots, \beta$. Then Isoc $(B_\beta; r)$ is equal to the number equivalence classes under this relation. Since $\sim$ is induced by a $\mathbf{S}_r$ action, Isoc $(B_\beta; r)$ is equal to the number orbits under the corresponding $\mathbf{S}_r$ action.

Example 5.4. We consider the set $C^1(B_{2h+3} \hookrightarrow S_h - \{x_1, x_2, x_3\}; r)$. For each $i = 1, 2, 3$, let $\mathcal{P}_i$ be the property that the $(2h+i)$-th coordinate of an element of $\mathbf{S}_r^{2h+3}$ is the identity. For each subset S of $\{1, 2, 3\}$, let $A(\mathcal{P}_S)$ be the set of elements in the product $\mathbf{S}_r^{2h+3}$ which satisfy conditions (C1), (C2) and the properties $\mathcal{P}_i$ for all $i \in S$. Notice that $A(\mathcal{P}_\emptyset)$ is the set of all elements in the product $\mathbf{S}_r^{2h+3}$ which satisfy conditions (C1) and (C2). Also, the set $C^1(\mathfrak{B}_{2h+3} \hookrightarrow \mathbb{S}_k - \{x_1, x_2, x_3\}; r)$ is equal to the set of elements of $\mathbf{S}_r^{2h+3}$ which satisfy conditions (C1) and (C2), but not any other property $\mathcal{P}_i$ for $i = 1, 2, 3$. Moreover, $|A(\mathcal{P}_S)| = |A(\mathcal{P}_{S'})|$ for any two subsets S, S' of $\{1, 2, 3\}$ with the same cardinality. It comes from the principle of inclusion and exclusion that

$$\begin{aligned}\left|C^1(\mathfrak{B}_{2h+3} \hookrightarrow \mathbb{S}_k - \{x_1, x_2, x_3\}; r)\right| &= (-1)^0 \binom{3}{0} |A(\mathcal{P}_\emptyset)| + (-1)^1 \binom{3}{1} |A(\mathcal{P}_{\{1\}})| \\ &\quad + (-1)^2 \binom{3}{2} |A(\mathcal{P}_{\{1,2\}})| + (-1)^3 \binom{3}{3} |A(\mathcal{P}_{\{1,2,3\}})|.\end{aligned}$$

Since the set $A(\mathcal{P}_S)$ is invariant under the $\mathbf{S}_r$ action for each subset S of $\{1, 2, 3\}$, by taking the $\mathbf{S}_n$-action on the underlying sets of the both sides of this equation, we have

$$\begin{aligned}\left|C^1(\mathfrak{B}_{2h+3} \hookrightarrow S_h - \{x_1, x_2, x_3\}; r)/\mathbf{S}_r\right| &= (-1)^0 \binom{3}{0} |A(\mathcal{P}_\emptyset)/\mathbf{S}_r| + (-1)^1 \binom{3}{1} |A(\mathcal{P}_{\{1\}})/\mathbf{S}_r| \\ &\quad + (-1)^2 \binom{3}{2} |A(\mathcal{P}_{\{1,2\}})/\mathbf{S}_r| + (-1)^3 \binom{3}{3} |A(\mathcal{P}_{\{1,2,3\}})/\mathbf{S}_r|.\end{aligned}$$

Since $A(\mathcal{P}_S)$ $(S \neq \{1, 2, 3\})$ can be regarded as the set of all transitive $(2h + 3 - |S| - 1)$-tuples, we can see that

$$\begin{aligned}|A(\mathcal{P}_\emptyset)/\mathbf{S}_r| &= \text{Isoc}\,(B_{2h+3-0-1}; r), \\ |A(\mathcal{P}_{\{1\}})/\mathbf{S}_r| &= \text{Isoc}\,(B_{2h+3-1-1}; r), \\ |A(\mathcal{P}_{\{1,2\}})/\mathbf{S}_r| &= \text{Isoc}\,(B_{2h+3-1-2}; r).\end{aligned}$$

It is clear that

$$|A(\mathcal{P}_{\{1,2,3\}})/\mathbf{S}_r| = \text{Isoc}\,(S_h, ; r).$$

Now, by Theorems 5.1 and 5.2, we have

$$\text{Isoc}\,(\mathbb{S}_h, \{x_1, x_2, x_3\}; r) = (-1)^3 \text{Isoc}\,(S_k; r) + \sum_{t=0}^{2} (-1)^t \binom{3}{t} \text{Isoc}\,(S_{2h+3-t-1}; r). \qquad \square$$

In general, by using Theorem 5.1, one can express the number Isoc $(S, B; r)$ of connected r-fold branched coverings of the surface S with branch set B in terms of the numbers Isoc $(S_k; r)$ and Isoc $(B_\beta; r)$ [37].

Theorem 5.5. *Let S be either S_h or N_k and let B be a set of b points on S. Let B_m be the bouquet of m circles. Then the number of connected r-fold branched coverings of S with branch set B is*

$$\text{Isoc}\,(S_h, B; r) = (-1)^b \,\text{Isoc}\,(S_h; r) + \sum_{t=0}^{b-1} (-1)^t \binom{b}{t} \text{Isoc}\,(B_{2h+b-t-1}; r)$$

and

$$\operatorname{Isoc}(N_k,B;r) = (-1)^b \operatorname{Isoc}(N_k;r) + \sum_{t=0}^{b-1}(-1)^t\binom{b}{t}\operatorname{Isoc}(B_{k+b-t-1};r).$$

Let $\mathcal{D}_r$ be a bordered surface with fundamental group F_r. The following theorem was obtained in [32].

Theorem 5.6. *Let B be a b-subset of the bordered surface $\mathcal{D}_r$. Then the number of connected n -fold branched coverings of the bordered surface $\mathcal{D}_r$ with branch set B is*

$$\operatorname{Isoc}(\mathcal{D}_r,B;n) = \sum_{t=0}^{b}(-1)^t\binom{b}{t}\operatorname{Isoc}(B_{r+b-t};n),$$

where $\mathfrak{B}_m$ is a bouquet of m circles.

Combining the V.A. Liskovets theorem and Theorem 5.6 we have the following result:

Theorem 5.7. *Let B be a b-subset of the bordered surface $\mathcal{D}_r$. Then the number of connected n-fold branched coverings of the bordered surface $\mathcal{D}_r$ with branch set B is*

$$\operatorname{Isoc}(\mathcal{D}_r,B;n) = \frac{1}{n}\sum_{m|n}\sum_{d|\frac{n}{m}}\mu\left(\frac{n}{md}\right)d\,T_m(d),$$

where $T_m(d)$ is a polynomial of d defined by

$$T_m(d) = m\sum_{k=1}^{m}\frac{(-1)^{k+1}}{k}\sum_{\substack{n_1+\cdots+n_k=m\\ n_1,..,n_k\geq 1}}(n_1!\ldots n_k!d^m)^{r-1}(n_1!\ldots n_k!d^m-1)^b.$$

We illustrate this theorem by the following examples.

Example 5.8. Let B, $|B| = b \geq 0$ be a branch set of the bordered surface $\mathcal{D}$ with fundamental group F_r and $\nu = r-1$. Then

$$\begin{aligned}
&\operatorname{Isoc}(\mathcal{D}_r,B;2) = 2\cdot 2^\nu - 0^b,\\
&\operatorname{Isoc}(\mathcal{D}_r,B;3) = 6^\nu\cdot 5^b + 3^\nu\cdot 2^b - 2^\nu,\\
&\operatorname{Isoc}(\mathcal{D}_r,B;4) = 24^\nu\cdot 23^b + 8^\nu\cdot 7^b - 6^\nu\cdot 5^b.
\end{aligned}$$

We remark that the above formulas are non-trivial even for a disc $\mathcal{D} = \mathcal{D}_0$. In this case $\nu = -1$ and we have

$$\begin{aligned}
&\operatorname{Isoc}(\mathcal{D},B;2) = 1 - 0^b,\\
&\operatorname{Isoc}(\mathcal{D},B;3) = \frac{1}{6}\cdot 5^b + \frac{1}{3}\cdot 2^b - \frac{1}{2},\\
&\operatorname{Isoc}(\mathcal{D},B;4) = \frac{1}{24}\cdot 23^b + \frac{1}{8}\cdot 7^b - \frac{1}{6}\cdot 5^b.
\end{aligned}$$

5.2 *Regular branched surface coverings*

For a finite group $\mathcal{A}$, let Isoc $(S, B; \mathcal{A})$ denote the number of connected branched $\mathcal{A}$-coverings of the surface S with branch set B. Notice that any two connected regular branched coverings of S cannot be isomorphic if their covering transformation groups (or voltage groups) are not isomorphic. Hence, the following equation comes from the fact that every connected regular r-fold branched covering of S is isomorphic to a connected branched $\mathcal{A}$-covering of S for some group $\mathcal{A}$ of order r. The number $\text{Isoc}^R(S, B; r)$ of isomorphism classes of regular r-fold branched coverings of S with branch set B is

$$\text{Isoc}^R(S, B; r) = \sum_{\mathcal{A}} \text{Isoc}\,(S, B; \mathcal{A}),$$

where the sum is over all representatives of isomorphism classes of groups of order r.

We define an equivalence relation $\sim$ on the set of all generating β-tuples $(\sigma_1, \ldots, \sigma_\beta)$ in $\mathcal{A} \times \cdots \times \mathcal{A}$ by $(\sigma_1, \ldots, \sigma_\beta) \sim (\sigma_1', \ldots, \sigma_\beta')$ if and only if there exists a group automorphism φ on $\mathcal{A}$ such that $\varphi(\sigma_i) = \sigma_i'$ for each $i = 1, 2, \ldots, \beta$. For convenience, let Isoc $(B_\beta; \mathcal{A})$ be the number of elements in $\mathcal{A} \times \cdots \times \mathcal{A}/\sim$.

Using reasoning similar to Theorem 5.5, one can use unbranched coverings to enumerate branched ones [37].

Theorem 5.9. *Let S be either S_h or N_k and let B be a set of b points on S. Let B_m be the bouquet of m circles and let $\mathcal{A}$ be a finite group. Then the number of connected branched $\mathcal{A}$-coverings of S with branch set B is*

$$\text{Isoc}\,(S_h, B; \mathcal{A}) = (-1)^b\,\text{Isoc}\,(S_h; \mathcal{A}) + \sum_{t=0}^{b-1} (-1)^t \binom{b}{t} \text{Isoc}\,(B_{2h+b-t-1}; \mathcal{A}),$$

and

$$\text{Isoc}\,(N_k, B; \mathcal{A}) = (-1)^b\,\text{Isoc}\,(N_k; \mathcal{A}) + \sum_{t=0}^{b-1} (-1)^t \binom{b}{t} \text{Isoc}\,(B_{k+b-t-1}; \mathcal{A}).$$

Kwak et al. [37] enumerated branched $\mathcal{A}$-coverings of a surface. To state this, we need further notation. For an irreducible character ξ of $\mathcal{A}$, let

$$c_\xi = \frac{1}{|\mathcal{A}|} \sum_{g \in \mathcal{A}} \xi(g^2) = \begin{cases} 1 & \text{if } \rho \text{ is real,} \\ -1 & \text{if } \xi \text{ is real but } \rho \text{ is not real,} \\ 0 & \text{if } \xi \text{ is not real} \end{cases}$$

with the representation ρ corresponding to ξ. Now, by the result in [16, 18], Theorem 5.9 can be rephrased as follows.

Theorem 5.10. *Let S be either S_h or N_k and let B be a set of b points on S. Let $\mathcal{A}$ be a finite group. Then number of connected branched $\mathcal{A}$-coverings of S with branch set B is*

$$\text{Isoc}\,(S_h, B; \mathcal{A}) = \sum_{K \le A} \frac{\mu(K)\,|K|^{2h-1}}{|\text{Aut}\,(\mathcal{A})|} \left((|K| - 1)^b + (-1)^b \sum_{\xi} \xi(1)^{2-2h} \right),$$

and

$$\text{Isoc}\,(N_k, B; \mathcal{A}) \sum_{K \le A} \frac{\mu(K)\,|K|^{k-1}}{|\text{Aut}\,(\mathcal{A})|} \left((|K| - 1)^b + (-1)^b \sum_{\xi} c_\xi^k \xi(1)^{2-k} \right),$$

where ξ ranges over all irreducible characters of K except the principal one (i.e., $\xi = 1$).

We observe that if $\mathcal{A}$ is a finite abelian group, then every irreducible character is of degree 1. So, for each subgroup K of $\mathcal{A}$,

$$\sum_{\xi} \xi(1)^{2-2h} = |K| - 1, \quad \text{and} \quad \sum_{\xi} c_{\xi}^{k} \xi(1)^{2-k} = 2^{\lambda(K)} - 1,$$

where the sum is over all irreducible characters of K except the principal one and $\lambda(K)$ is the number of direct summands of K whose orders are even.

Note that Theorem 5.10 is efficient if the lattice structure of subgroups of $\mathcal{A}$ and their characters are known.

In [37], one can find an enumeration formula for Isoc $(S_h; \mathcal{A})$ and Isoc $(N_k; \mathcal{A})$ for any finite abelian group $\mathcal{A}$ which does not involve the lattice structure of subgroups of $\mathcal{A}$. By using it and Theorem 3.4 in [15], one can obtain another enumeration formula from Theorem 5.9 which does not involve the lattice structure of subgroups of finite abelian group $\mathcal{A}$.

5.3 *Orientable branched surface coverings of nonorientable surfaces*

Using reasoning similar to Theorem 5.5, one can use unbranched coverings to enumerate branched ones [37].

Theorem 5.11. *Let N_k be a non-orientable surface of genus k and let B be a b-subset of N_k. Then, every connected branched orientable covering of N_k must be even-fold, and for any r, the number of the isomorphism classes of connected branched orientable 2r-fold coverings of N_k with branch set B is*

$$\operatorname{Isoc}^{\mathcal{O}}(N_k, B; 2r) = (-1)^b \operatorname{Isoc}^{\mathcal{O}}(N_k; 2r) + \sum_{t=0}^{b-1} (-1)^t \operatorname{Isoc}^{\mathcal{B}}(B_{b+k-t-1}; 2r).$$

Notice that $\operatorname{Isoc}^{\mathcal{B}}(B_\beta; 2r)$ is computed in Theorem 3.11. Hence, by Theorems 2.11, 5.11 and 3.11, one can find a computation formula for the numbers $\operatorname{Isoc}^{\mathcal{O}}(N_k, B; 2r)$.

Using reasoning similar to Theorem 5.11, we can have

$$\operatorname{Isoc}^{\mathcal{O}}(N_k, B; \mathcal{A}) = (-1)^b \operatorname{Isoc}^{\mathcal{O}}(N_k; \mathcal{A}) + \sum_{t=0}^{b-1} (-1)^t \operatorname{Isoc}^{\mathcal{B}}(B_{b+k-t-1}; \mathcal{A}).$$

Now, we aim to introduce another formula to compute the number $\operatorname{Isoc}^{\mathcal{O}}(N_k, B; \mathcal{A})$ for any finite group $\mathcal{A}$. The formula involves character theory and lattice structures of certain subgroups of $\mathcal{A}$. To do this, we need more terminologies.

For a subgroup $\mathcal{S}$ of $\mathcal{A}$, let Aut $(\mathcal{A}, \mathcal{S})$ be the set of group automorphisms $\mathcal{A}$ which preserve $\mathcal{S}$. Let $\mathcal{S}$ be a subgroup of index 2 in $\mathcal{A}$ and fix an element $t \in \mathcal{A} - \mathcal{S}$. Then for each $\xi \in \operatorname{Irr}(\mathcal{S})$ the character ξ_t defined by $\xi_t(s) = \xi(tst^{-1})$ $(s \in \mathcal{S})$ is also an irreducible character of $\mathcal{S}$. An irreducible character ξ of $\mathcal{S}$ is said to be of type 1 (or $\xi \in \Im_1(\mathcal{S})$) if ξ and ξ_t are distinct, and of type 2 (or $\xi \in \Im_2(\mathcal{S})$) otherwise. It is known [38, 39] that $\xi \in \Im_1(\mathcal{S})$ if and only if there exists an irreducible character $\hat{\xi}$ of $\mathcal{A}$ such that $\hat{\xi}_{\mathcal{S}} = \xi + \xi_t$, and that $\xi \in \Im_2(\mathcal{S})$ if and only if there exists an irreducible character $\hat{\xi}$ of $\mathcal{A}$ such that $\hat{\xi}_{\mathcal{S}} = \xi$, where $\hat{\xi}_{\mathcal{S}}$ is the restriction of $\hat{\xi}$ to $\mathcal{S}$. We say that two subgroups $\mathcal{S}_1$ and $\mathcal{S}_2$ of a group $\mathcal{A}$ are *similar* if there exists an automorphism σ on $\mathcal{A}$ such that $\sigma(\mathcal{S}_1) = \mathcal{S}_2$. Now, we are ready to state the following results in [27].

Theorem 5.12. *Let $\mathcal{A}$ be a finite group and let B be a b-subset of a nonorientable surface N_k. Then the number* $\mathrm{Isoc}^O(N_k, B; \mathcal{A})$ *of equivalence classes of connected branched orientable $\mathcal{A}$-coverings of N_k with branch set B is*

$$\mathrm{Isoc}^O(N_k, B; \mathcal{A}) = \sum_{\mathcal{S}} \sum_{\substack{K \leq \mathcal{A} \\ K \neq K \cap \mathcal{S}}} \frac{\mu(K)\,|K|^{k-1}}{2^{k-1}|\mathrm{Aut}\,(\mathcal{A}, \mathcal{S})|} \left(\left(\frac{|K|}{2} - 1 \right)^b + (-1)^b \sum_{\xi} d_{\xi}^k \xi(1)^{2-k} \right),$$

where $\mathcal{S}$ ranges over the representatives of similarity classes of subgroups of index 2 in $\mathcal{A}$, ξ does all irreducible characters of $K \cap \mathcal{S}$ except the principal character, μ is the Möbius function, and $d_\xi = c_{\hat{\xi}} - c_\xi$ if $\xi \in \Im_1(\mathcal{S})$ and $d_\xi = 2c_{\hat{\xi}} - c_\xi$ if $\xi \in \Im_2(\mathcal{S})$.

Corollary 5.13. *Let $\mathcal{A}$ be a finite abelian group and let B be a b-subset of a nonorientable surface $\mathbb{S}_k$. Then we have*

$$\begin{aligned} &\mathrm{Isoc}^O(N_k, B; \mathcal{A}) \\ &= \begin{cases} \displaystyle\sum_{\mathcal{S}} \sum_{\substack{K \leq \mathcal{A} \\ K \neq K \cap \mathcal{S}}} \frac{\mu(K)\,|K|^{k-1}}{2^{k-1}|\mathrm{Aut}\,(\mathcal{A}, \mathcal{S})|} \left(\left(\frac{|K|}{2} - 1 \right)^b + (-1)^b \sum_{\xi} c_\xi \xi(g^2) \right) & \text{if } k \text{ is odd,} \\ \displaystyle\sum_{\mathcal{S}} \sum_{\substack{K \leq \mathcal{A} \\ K \neq K \cap \mathcal{S}}} \frac{\mu(K)\,|K|^{k-1}}{2^{k-1}|\mathrm{Aut}\,(\mathcal{A}, \mathcal{S})|} \left(\left(\frac{|K|}{2} - 1 \right)^b + (-1)^b \sum_{\xi} c_\xi \right) & \text{if } k \text{ is even,} \end{cases} \end{aligned}$$

where $\mathcal{S}$ ranges over the representatives of similarity classes of subgroups of index 2 in $\mathcal{A}$, and ξ does all irreducible characters of $K \cap \mathcal{S}$ except the principal character, and g is a fixed element in $K - \mathcal{S}$.

We observe that the number $\mathrm{Isoc}^{RO}(N_k, B; n)$ of equivalence classes of regular branched connected orientable n-fold coverings of a nonorientable surface N_k with branch set B is equal to

$$\mathrm{Isoc}^{RO}(N_k, B; n) = \sum_{\mathcal{A}} \mathrm{Isoc}^O(N_k, B; \mathcal{A}),$$

where $\mathcal{A}$ ranges over the representatives of isomorphism classes of groups of order n. Hence, by Theorem 5.12. and Corollary 5.13., one can express the numbers $\mathrm{Isoc}^{RO}(N_k, B; n)$ in terms of irreducible characters of groups of order n and those of their subgroups of index 2. For example, we can see that

$$\mathrm{Isoc}^{RO}(N_k, B; 2p) = \begin{cases} \dfrac{2}{p-1}(p^{k-1} - 1) & \text{if } b = 0, \\ p^{k-2}((p-1)^{b-1}(p+1) + (-1)^b) & \text{if } b \neq 0, \end{cases}$$

where B is a b-subset of N_k and p is an odd prime.

6 HURWITZ ENUMERATION PROBLEM

6.1 *Branched coverings with prescribed ramification types*

Let B be a branch set of a branched covering $\pi : T \to S$. At each point $x \in \pi^{-1}(B)$, the projection π is topologically equivalent to the complex map $z \to z^k$ for a natural number k. We call x the *branch* *point* of π and the number k the *order* of x. Denote by s_k^p the number of branch points of order k of the map π in the preimage $\pi^{-1}(b_p)$, where $p = 1, 2, \ldots, r$ and $k = 1, 2, \ldots, n$. We call $r \times n$ matrix $\sigma = (s_k^p)$ the *ramification type* of the covering π.

Let S and σ be as above and let g be the genus of the surface S. Then, the classical Hurwitz enumeration problem can be stated in the following way.

Hurwitz enumeration problem. *Determine the number $N_{n,g,\sigma}$ of nonequivalent coverings of multiplicity n of a surface S of genus g with a given ramification type σ.*

Hurwitz [34], [40] constructed a generating function for the number of nonequivalent coverings of the sphere having only simple branch points (of order two). Röhrl [41] obtained upper and lower estimates for the number of nonequivalent coverings with a given ramification type. Some partial solutions of the problem were obtained in [4], [37] and [42]. In particular, the number of coverings with a given branch set without restriction on the ramification type were obtained in [37]. The complete solution of the Hurwitz enumeration problem is contained in [43]. The solution is given in terms of irreducible characters of the symmetric group which makes it very complicated. It was known just a few cases [5], [36], [44], [45] when it is possible to avoid characters of symmetric groups for calculation the number of coverings. Recently, some new results (see [46], [47] and [48]) were obtained to make it clear that, in some cases, the number of coverings can be expressed in terms of the number theoretical functions. For instance, this takes a place for the covering whose branch orders coincide with multiplicity [49].

Now, we represent a solution of Hurwitz problem for closed orientable surfaces. Let $\pi : T \to S$ be a branched covering with branch set $B = \{b_1, b_2, \ldots, b_r\}$ of the ramification type $\sigma = (s_k^p)_{\substack{p=1,2,\ldots,r \\ k=1,2,\ldots,n}}$. The set B will be considered fixed in what follows. By $(1^{s_1}2^{s_2}\cdots n^{s_n})$, we denote a permutation of $\mathbf{S}_n$ consisting of s_k cycles of length k, $k = 1, 2, \ldots, n$. It follows from the results of Hurwitz that each covering π with ramification type σ is uniquely defined by the ordered tuple of permutations

$$(a_1, b_1, \ldots, a_g, b_g, (1^{s_1^1}\cdots n^{s_n^1}), (1^{s_1^2}\cdots n^{s_n^2}), \ldots, (1^{s_1^r}\cdots n^{s_n^r})) \in \mathbf{S}_n^{2g+r} \tag{1}$$

satisfying the relation

$$\prod_{i=1}^{g}[a_i, b_i]\prod_{p=1}^{r}(1^{s_1^p}2^{s_2^p}\cdots n^{s_n^p}) = 1 \tag{2}$$

and generating a transitive subgroup of $\mathbf{S}_n$ (transitive tuples). By Theorem 5.1 two coverings are equivalent if and only if the corresponding tuples are conjugate via a permutation from $\mathbf{S}_n$. The proof of these facts can be found, for example, in [36] and [50].

Denote by $\mathcal{B}_{n,g,\sigma}$ the set of all tuples of the form Eq.(1) satisfying equation Eq.(2) and select in $\mathcal{B}_{n,g,\sigma}$ a subset $\mathcal{T}_{n,g,\sigma}$ formed by transitive tuples. We set $B_{n,g,\sigma} = |\mathcal{B}_{n,g,\sigma}|$ and $T_{n,g,\sigma} = |\mathcal{T}_{n,g,\sigma}|$. The following results have been obtained in [43].

Theorem 6.1. *The number $B_{n,g,\sigma}$ of elements of the set $\mathcal{B}_{n,g,\sigma}$ is defined by the formula*

$$n! \sum_{\lambda\in\mathrm{Irr}_n}\prod_{p=1}^{r}\frac{\chi^{\lambda}_{s_1^p s_2^p\cdots s_n^p}}{1^{s_1^p}s_1^p!\cdot 2^{s_2^p}s_2^p!\cdots n^{s_n^p}s_n^p!}\left(\frac{n!}{f^{\lambda}}\right)^{2g-2+r}, \tag{3}$$

where Irr_n *is the set of all irreducible representations of the group* $\mathbf{S}_n$, f^{λ} *is the degree and* $\chi^{\lambda}_{s_1^p s_2^p\cdots s_n^p}$ *the character of the permutation* $(1^{s_1}2^{s_2}\cdots n^{s_n})$ *corresponding to the representation* λ.

Theorem 6.2. *The number $T_{n,g,\sigma}$ of elements of the set $\mathcal{T}_{n,g,\sigma}$ is defined by the formula*

$$\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k} \sum_{\substack{n_1+n_2+\cdots+n_k=n \\ \sigma_1+\sigma_2+\cdots+\sigma_k=\sigma}} \binom{n}{n_1, n_2, \ldots, n_k} B_{n_1,g,\sigma_1} \cdot B_{n_2,g,\sigma_2} \cdots B_{n_k,g,\sigma_k}. \tag{4}$$

Denote by $\mu(n)$, $\varphi(n)$ and $\Phi(x,n)$ the Möbius, Euler and von Sterneck-Ramanujan functions respectively. The relationship between them is given by the formula

$$\Phi(x,n) = \frac{\varphi(n)}{\varphi\left(\frac{n}{(x,n)}\right)} \mu\left(\frac{n}{(x,n)}\right),$$

where (x,n) is the greatest common divisor of x and n. It was shown by O. Hölder that $\Phi(x,n)$ coincides with the Ramanujan sum $\sum_{(d,n)=1} \exp\left(\frac{2ikd}{n}\right)$.

Theorem 6.3. *The number of non-equivalent n-fold coverings of a closed orientable surface of genus g, with given ramification type $\tau = (t_s^p)_{\substack{p=1,\ldots,r \\ s=1,\ldots,n}}$, is given by the formula*

$$N_{n,g,\tau} = \frac{1}{n} \sum_{\substack{\ell|v \\ m\ell=n}} \sum_{\frac{\ell}{(t,\ell)}|d|\ell} \mu\left(\frac{\ell}{d}\right) \frac{d^{(2g-2+r)m+1}}{(m-1)!}$$

$$\times \sum_{\{j_{k,p}^s\}} T_{m,g,\sigma} \sum_{x=1}^{d} \prod_{s,k,p} \left[\frac{\Phi(x,\frac{s}{k})}{d}\right]^{j_{k,p}^s} \prod_{k,p} \binom{s_k^p}{j_{k,p}^1, \ldots, j_{k,p}^{md}}, \tag{5}$$

where $t = \mathrm{GCD}\{t_s^p, p = 1, \ldots, r,\ s = 1, \ldots, n\}, v = \mathrm{GCD}\{st_s^p, p = 1, \ldots, r,\ s = 1, \ldots, n\}, s_k^p = \sum_{s=1}^{md} j_{k,p}^s$, the sum $\sum_{\{j_{k,p}^s\}}$ is taken over all collections $\{j_{k,p}^s\}$ such that

$$\sum_{\substack{1 \le k \le \frac{st_s^p}{\ell} \\ \frac{s}{(s,d)}|k|s}} kj_{k,p}^s = \frac{st_s^p}{\ell},\ \ s = 1, \ldots, md,\ p = 1, \ldots, r \tag{6}$$

and $j_{k,p}^s = 0$, if at least one of the conditions

$$1 \le k \le \frac{st_s^p}{\ell} \quad \text{and} \quad \frac{s}{(s,d)}|k|s \tag{7}$$

fails. The indices in the products $\prod_{s,k,p}$ and $\prod_{k,p}$ varies in the limits $s = 1, \ldots, md, p = 1, \ldots, r$, $k = 1, \ldots, m$, and $T_{m,g,\sigma} = T_{m,g,(s_k^p)_{\substack{k=1,\ldots,m \\ p=1,\ldots,r}}}$ is defined by (4).

Corollary 6.4. *The number of nonequivalent n-fold coverings of a closed orientable surface of genus g, with given ramification type $\sigma = (s_k^p)_{\substack{k=1,\ldots,m \\ p=1,\ldots,r}}$ has the following asymptotic:*

$$N_{n,g,\sigma} \sim 2(n!)^{2g-2} \prod_{p=1}^{r} \frac{n!}{1^{s_1^p} \cdot s_1^p! \cdot \ \ldots\ \cdot n^{s_n^p} \cdot s_n^p!},\ \ g \to \infty. \tag{8}$$

The proof of Theorem 6.3 given in [43] is rather complicated, Here, we indicate a new proof based on the main counting principal (Theorem 3.1) and on the results of the paper [25].

Let $\rho : \tilde{S} \to S$ be an n-fold covering of surface S with ramification type $\tau = (t_s^p)_{\substack{p=1,\dots,r\\ s=1,\dots,n}}$.

We represent ρ as a composition of two maps $\rho = \mu \circ \lambda$, where $\lambda = \lambda_{\mathbb{Z}_\ell} : \tilde{S} \to O = \tilde{S}/\mathbb{Z}_\ell$ is a regular $\mathbb{Z}_\ell$-covering and $\mu : O \to S$ is an m-fold covering with ramification type $\sigma = (s_k^p)_{\substack{p=1,\dots,r\\ k=1,\dots m}}$. We have to find the ramification type of λ and the signature of the fundamental group of cyclic orbifold $O = \tilde{S}/\mathbb{Z}_\ell$. Let $x_p \in S$ be one of the points in the branched set of $\rho : \tilde{S} \to S$ and $\tilde{x}_p \in \mu^{-1}(x_p)$. We set $\mathrm{ord}_\mu(\tilde{x}_p) = k$. Since λ is a regular covering the order function ord_λ is constant along $\lambda^{-1}(\tilde{x}_p)$. We take any $\tilde{\tilde{x}}_p \in \lambda^{-1}(\tilde{x}_p)$ and put $\mathrm{ord}_\lambda(\tilde{\tilde{x}}) = s/k$ for a suitable s. In this case

$$\mathrm{ord}_\rho(\tilde{\tilde{x}}_p) = \mathrm{ord}_\lambda(\tilde{\tilde{x}}_p)\,\mathrm{ord}_\mu(\tilde{x}_p) = s/k \cdot k = s.$$

Consider the set

$$J_{k,p}^s = \{\tilde{x} \in \mu^{-1}(x_p) : \mathrm{ord}_\rho(\tilde{\tilde{x}}) = s \quad \text{for any } \tilde{\tilde{x}} \in \lambda^{-1}(\tilde{x})$$

and stand $j_{k,p}^s = |J_{k,p}^s|$ for cardinality of $J_{k,p}^s$. Since λ is a regular ℓ-fold covering its local ramification type over each point $\tilde{x} \in J_{k,p}^s$ is equal to $\left(\frac{s}{k}\right)^{\frac{\ell k}{s}}$. Hence, the ramification type of λ, totally, is given by

$$\left\{\left(\frac{s}{k}\right)^{\frac{\ell k}{s} j_{k,p}^s} : s = 1, \dots, n,\, p = 1, \dots, r,\, k = 1, \dots, m\right\}.$$

Now, we can conclude that the Fuchsian group $F = \pi_1^{orb}(O)$ has the following signature

$$\left\{\gamma;\ \left(\frac{s}{k}\right)^{j_{k,p}^s},\ s = 1, \dots, n,\, p = 1, \dots, r,\, k = 1, \dots, m\right\},$$

where γ is genus of underlying surface of O. We recall that Fuchsian group of the signature $\{\gamma;\, m_1, m_2, \dots, m_r\}$ has the following presentation

$$F = \langle a_1, b_1, \dots, a_\gamma, b_\gamma, .x_1, \dots, x_r : \prod_{i=1}^{\gamma}[a_i\, b_i]\prod_{j=1}^{r} x_j = x_1^{m_1} = \dots = x_r^{m_r} = 1\rangle.$$

The signature $\{\gamma;\, m_1^{k_1}, m_2^{k_2}, \dots, m_r^{k_r}\}$ is equivalent to

$$\{\gamma;\, \underbrace{m_1, \dots, m_1}_{k_1}, \dots, \underbrace{m_r, \dots, m_r}_{k_r}\}.$$

Denote by $\mathrm{Epi}^\circ(\Gamma,\, \mathbb{Z}_\ell)$ the set of order preserving epimorphisms from Γ onto $\mathbb{Z}_\ell$. By the version of Theorem 3.1 given in [25] we have the following formula

$$N_{n,g,\tau} = \frac{1}{n}\sum_{\substack{\ell | n\\ m\ell = n}}\ \sum_{\substack{\lambda:\tilde{S}\to\tilde{S}/\mathbb{Z}_\ell\\ \rho=\mu\circ\lambda}} |\mathrm{Epi}^\circ(\pi_1^{orb}(\tilde{S}/\mathbb{Z}_\ell),\, \mathbb{Z}_\ell)|\, M_{m,g,\sigma},$$

where $M_{m,g,\sigma} = \frac{1}{(m-1)!}T_{m,g,\sigma}$ is the number of rooted n-fold coverings of S with ramification type σ.

Moreover, it was shown in [25] that if $F = \pi_1^{orb}(\tilde{S}/\mathbb{Z}_\ell)$ is the above presented Fuchsian group, then

$$|\mathrm{Epi}^\circ(F,\, \mathbb{Z}_\ell)| = \sum_{M|d|\ell} \mu\left(\frac{\ell}{d}\right) d^{2\gamma}\, E_d(m_1,\, \ldots, m_r),$$

where γ is the genus of an orbifold $O = \tilde{S}/\mathbb{Z}_\ell,\;\; E_d(m_1,\, \ldots, m_r) = \frac{1}{d}\sum_{x=1}^{d} \Phi(x, m_1)\, \Phi(x, m_2) \cdots \Phi(x, m_r)$, and $M = \mathrm{LCM}\{m_1,\, \ldots, m_r\}$ is the least common multiple of $\{m_1,\, \ldots, m_r\}$.

Since $s_k^p = \sum_s j_{k,p}^s$, we have $\prod_{k,p} \binom{s_k^p}{j_{k,p}^1, \cdots j_{k,p}^{md}}$ possibilities to create a decomposition $\rho = \mu \circ \lambda$ with prescribed values $j_{k,p}^s$. Combining this results with the Riemann-Hurwitz relation

$$2\gamma - 2 = m(2g - 2 + r) - \sum_{s,k,p} j_{k,p}^s$$

we obtain the statement equivalent to Theorem 6.3.

We observe that the number Iso $(N_k, B; S; r)$ has not been determined yet for any surface S and r. When the fold number r is odd, this can be completed if one can count the connected branched coverings of a nonorientable surface with arbitrarily prescribed ramification type because any odd fold branched covering surface of a nonorientable surface is also nonorientable.

6.2 *Distributions*

For any two surfaces S and $\tilde{S}$, let Iso $(S, B; \tilde{S}; r)$ (resp. $\mathrm{Iso}^R(S, B; \tilde{S}; r)$) denote the number of r-fold branched (resp. regular) coverings $p : \tilde{S} \to S$ with branch set B. Similarly, we let Iso $(S, B; \tilde{S}; \mathcal{A})$ denote the number of branched $\mathcal{A}$-coverings $p : \tilde{S} \to S$ with branch set B.

From Theorem 6.3, one can obtain a computational formula for the numbers Iso $(S_h, B; S; r)$ for any surface S and r, because any branched covering of an orientable surface is also orientable. But, it has not yet been determined that Iso $(N_k, B; S; r)$ for any surface S and r.

In contrast, the number $\mathrm{Iso}^R(S, B; \tilde{S}; r)$ was completely determined. It is clear that Iso $(S, B; \tilde{S}; 2) = \mathrm{Iso}^R(S, B; \tilde{S}; 2)$. For a prime number p, Kwak et al. [36, 45, 51] computed the numbers $\mathrm{Iso}^R(S, B; \tilde{S}; p)$, Iso $(S, B; \tilde{S}; \mathbb{D}_p)$, and Iso $(S, B; \tilde{S}; m\mathbb{Z}_p)$. For more general cases, Jones [16, 17] obtained a formula that counts the number of connected branched $\mathcal{A}$-coverings of a surface with a prescribed ramification type. Using this, one can derive a computational formula for Iso $(S_i, B; S_j; \mathcal{A})$ for any group $\mathcal{A}$ and Iso $(N_i, B; N_j; \mathcal{A})$ for any group $\mathcal{A}$ that does not contain any subgroup of index 2. Kwak et al. [33] obtained a formula that counts the number of connected branched orientable $\mathcal{A}$-coverings of a nonorientable surface when $\mathcal{A}$ is abelian. Goulden et al. [27] obtained a formula for the number of connected branched orientable $\mathcal{A}$-coverings of a nonorientable surface with a prescribed ramification type. It gives a computational formula for the number Iso $(N_i, B; S_j; \mathcal{A})$ and hence, $\mathrm{Iso}^R(N_i, B; S_j; r)$. Notice that one can obtain a computational formula for $\mathrm{Iso}^R(S, B; \tilde{S}; r)$ for any two surfaces S and $\tilde{S}$ by combining this and the results in [16, 17]. For example, by the Riemann-Hurwitz equation, we can see that the number $|B|$ of branch points of a branched $\mathcal{A}$-covering $p : \mathbf{S}_n \to N_2$ is one 1 or 2. If it is 1, then $|\mathcal{A}| = 6$ or 8, and if it is 2, then $|\mathcal{A}| = 4$. Now, by the classification of finite groups, one can determine that

$$\mathrm{Isoc}^R(N_2, B; S_3; n) = \begin{cases} 4 & \text{if } n = 4 \text{ and } |B| = 2, \\ 3 & \text{if } n = 6 \text{ and } |B| = 1, \\ 6 & \text{if } n = 8 \text{ and } |B| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

For a prime p, we can completely determine the number $\mathrm{Iso}^R(S, B; \tilde{S}; p)$ as follows.

Theorem 6.5. *Let B be a b-subset of a surface S and let p be a prime.*

(1) *If $S = S_h$, then*

$$\mathrm{Iso}^R(S_h, B; \tilde{S}; p) = \begin{cases} \dfrac{p^{2h} - 1}{p - 1} & \text{if } \tilde{S} = S_{1+p(h-1)},\ b = 0, \\ p^{2h-1}((p-1)^{b-1} + (-1)^b) & \text{if } \tilde{S} = S_{ph+\frac{p-1}{2}(b-2)},\ b \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *If $S = N_k$, then*

$$\mathrm{Iso}^R(N_k, B; \tilde{S}; 2) = \begin{cases} 1 & \text{if } \tilde{S} = S_{k-1},\ b = 0, \\ 2^k - 2 & \text{if } \tilde{S} = N_{2(k-1)},\ k \neq 1,\ b = 0, \\ 2^k & \text{if } \tilde{S} = N_{2(k-1)+b},\ b \neq 0,\ b = \text{even}, \\ 0 & \text{otherwise,} \end{cases}$$

and for any odd prime p,

$$\mathrm{Iso}^R(N_k, B; \tilde{S}; p) = \begin{cases} \dfrac{p^{k-1} - 1}{p - 1} & \text{if } \tilde{S} = N_{p(k-2)+2},\ b = 0, \\ p^{k-1}(p-1)^{b-1} & \text{if } \tilde{S} = N_{p(k-2)+b(p-1)+2},\ b \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

7 CONCLUDING REMARKS

There are a few more aspects of the branched covering theory which are not covered by this paper. Two coverings $p : \tilde{X} \to X$ and $q : \tilde{Y} \to Y$ are called *homeomorphic* if there are homeomorphisms $h : X \to Y$ and $\tilde{h} : \tilde{X} \to \tilde{Y}$ such that $h \circ p = q \circ \tilde{h}$. It was discovered in classical papers by Luröth and Clebsch that there is only one equivalence class of coverings sphere by sphere with simple branched points. Later, the homeomorphic coverings given by polynomial were calculated by S. Zdravkovska [52] and [53]. Some new invariants of homeomorphic coverings of sphere were suggested by A. Protopopov ([54], [55]). The beautiful examples of non-homeomorphic coverings with the same ramification type were constructed by G. Jones and A. Zvonkin [56]. The classes of regular non-homeomorphic coverings with abelian covering groups were independently calculated by S. Natanzon and E.Vinberg.

A lot of papers on coverings are related with well-know de Franchis theorem:
The number of holomorphic maps $H(S_g, S_{g'})$ of a genus g Riemann surface S_g onto genus g' Riemann surface $S_{g'}$, $g \geq g' > 1$, is finite and depends on genus g only.

The best known upper bound for $H(S_g, S_{g'})$ was done by Masaharu Tanabe [57]. See also papers [58], [59] and [60] for revelent questions.

The existence of branched coverings between surfaces with prescribed branch data is still open problem. For recent advance and discussion see paper by E. Pervova and C. Petronio [61].

And, finally there is a deep relationship between branched coverings and the intersection theory of complex manifolds. For introduction and main results in this direction we refer the reader to papers [7], [8] and [9].

REFERENCES

[1] W.S. Massey, *A basic course in algebraic topology*, Springer-Verlag (1991).

[2] A. Hatcher, *Algebraic Topology*, Cambridge University Press, Cambridge, 2002.

[3] R.P. Stanley, *Enumerative combinatorics, Volume 2,* Cambridge University Press, Cambridge, 1999, xii+581 pp.

[4] A.D. Mednykh and G.G. Pozdnyakova, Number of nonequivalent coverings over a non-orientable compact surface, *Siber. Math. J.* 27 (1986), 99–106.

[5] A.D. Mednykh, On the number of subgroups in the fundamental group of a closed surface, *Comm. Algebra* 16 (1988), 2137–2148.

[6] V. Liskovets and A. Mednykh, On the number of disconnected coverings over manifold, *Preprint* (2007).

[7] T. Ekedahl, S. Lando, M. Shapiro, A. Vainshtein, On Hurwitz numbers and Hodge integrals, *CR Acad. Sci. Paris Ser. I Math.* 328 (12) (1999) 1175–1180. math.AG/9902104;

[8] T. Ekedahl, S. Lando, M. Shapiro, A. Vainshtein, Hurwitz numbers and intersections on moduli spaces of curves, *Invent. Math.* 146 (2) (2001) 297–327, math.AG/0004096.

[9] A. Okounkov, R. Pandharipande, Gromov-Witten theory, Hurwitz theory, and completed cycles, *Ann. of Math.* (2) 163(2) (2006), 517–560.

[10] J.H. Kwak and J. Lee, Isomorphism classes of graph bundles, *Canad. J. Math.* XLII (1990), 747–761.

[11] M. Hall, Jr., Subgroups of finite index in free groups, *Canadian J. Math.* 1 (1949), 187–190.

[12] V. Liskovets, On the enumeration of subgroups of a free group, *Dokl. Akad. Nauk BSSR.* 15 (1971), 6–9.

[13] M. Hofmeister, A note on counting connected graph covering projections, *SIAM J. Discrete Math.* 11 (1998), 286–292.

[14] J.H. Kwak and J. Lee, Enumeration of connected graph coverings, *J. Graph Theory* 23 (1996), 105–109.

[15] J.H. Kwak, J. Chun and J. Lee, Enumeration of regular graph coverings having finite abelian covering transformation groups, *SIAM J. Discrete Math.* 11 (1998), 273–285.

[16] G. Jones and V. Liskovets, Enumarating subgroups of finite index, in: *Proceedings of Com^{2}MaC Mini-Workshop on Hurwitz Theory and Ramifications (January 13–18, 2003),* editors J.H. Kwak and A.D. Mednykh, Combinatorial and Computational Mathematics Center, Pohang University of Science and Technology, Pohang, 2003.

[17] G.A. Jones, Counting subgroups of non-Euclidean crystallographic groups, *Math. Scand.* 84 (1999), 23–39.

[18] A.D. Mednykh, On unramified coverings of compact Riemann surfaces, *Soviet Math. Dokl.* 20 (1979), 85–88.

[19] I.P. Goulden, J.H. Kwak and J. Lee, Enumerating branched orientable surface coverings over a non-orientable surface, *Discrete Math.* 303 (2005), 42–55.

[20] V. Liskovets, Reductive enumeration under mutually orthogonal group actions, *Acta Applicandae Mathematicae* 52 (1998), 91–120.

[21] A.D. Mednykh, A New Method for Counting Coverings over Manifold with Finitely Generated Group, *Doklady Mathematics* 74(1) (2006), 498–502.

[22] H. Tamanoi, Generalized orbifold Euler characteristics of symmetric products and equivariant Morava K-theory, *Algebr. Geom. Topol*, 1 (2001), 115–141.

[23] H. Tamanoi, Generalized orbifold Euler characteristics of symmetric orbifolds and covering spaces. *Algebr. Geom. Topol*, 3 (2003), 791–856.

[24] A. Breda, A.D. Mednykh, R. Nedela, Counting unrooted unsensed maps on closed orientable surface, to appear.

[25] A.D. Mednykh, R. Nedela, Counting unrooted hypermaps on closed orientable surface, *Proceedings of the 18th International Conference on Formal Power Series and Algebraic Combinatorics, June 19–23, 2006*, San Diego, California, (2006), 1–19.

[26] J.H. Kwak, A.D. Mednykh and R. Nedela, Enumeration of orientable coverings over a non-orientable manifold, to appear in *Discrete Mathematics and Theoretical Computer Science.*

[27] I.P. Goulden, J.H. Kwak and J. Lee, Distribution of regular branched surface coverings, *European J. Combin.* 25 (2004), 437–455.

[28] V. Liskovets and A. Mednykh, The number of non-equivalent unbranched n-fold coverings of the Klein bottle., *preprint* (2002), com2mac.postech.ac.kr/papers/2002/02-06.pdf

[29] M. Petkovšek, T. Pisanski, Counting Disconnected Structures: Chemical Trees, Fullerenes, I-graphs, and others, *Croatica Chemica Acta* 78(4) (2005), 563–567.

[30] On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/njas/sequences/Seis.html

[31] P. Hall, The Euclidean functions of a group, *Quart. J. Math. Oxford* 7 (1936), 134–151.

[32] J.H. Kwak and A.D. Mednykh, Enumerating branched coverings over surfaces with boundaries, *European Journal of Combinatorics* 25 (2004), 23–34.

[33] J.H. Kwak, J. Lee and Y. Shin, Balanced coverings of a signed graph and some regular branched orientable surface coverings over a non-orientable surface, *Discrete Math.* 275 (2004), 177–193.

[34] A. Hurwitz, Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten, *Math. Ann.* 39 (1891), 1–61.

[35] J.L. Gross and T.W. Tucker, Generating all graph coverings by permutation voltage assignments, *Discrete Math.* 18 (1977), 273–283.

[36] J.H. Kwak, S. Kim and J. Lee, Distributions of regular branched prime-fold coverings of surfaces, *Discrete Math.* 156 (1996), 141–170.

[37] J.H. Kwak, J. Lee and A.D. Mednykh, Enumerating surface branched coverings from unbranched ones, *LMS J. Comput. Math.* 6 (2003), 89–104.

[38] G. James and M. Liebeck, *Representations and characters of groups,* Cambridge University Press, Cambridge, 1993.

[39] W. Ledermann, *Introduction to characters* (*2nd ed.*), Cambridge University Press, Cambridge, 1987.

[40] A. Hurwitz, Über die Anzahl der Riemann'sche Flächen mit gegebenen Verzweigungspunkten, *Math. Ann.* 55 (1902), 53–66.

[41] H. Rohrl, Unbounded coverings of Riemann surfaces and extensions of rings of meromorphic functions, *Trans. Amer. Math. Soc.* 107(2) (1963), 320–346.

[42] A.D. Mednykh, Hurwitz problem on the number of nonequivalent coverings of a compact Riemann surface, *Siber. Math. J.* 23 (1982), 415–420.

[43] A.D. Mednykh, Nonequivalent coverings over Riemann surfaces with a prescribed ramification type, *Siber. Mat. Zh.* 25 (1984), 606–625.

[44] A.D. Mednykh, Branched coverings of Riemann surfaces whose branch orders coincide with multiplicity, *Comm. Algebra* 18(5) (1990), 1517–1533.

[45] J.H. Kwak and J. Lee, Distributions of branched $\mathbb{D}_p$-coverings of surfaces, *Discrete Math.* 183 (1998), 193–212.

[46] I.P. Goulden and D.M. Jackson, The number of ramified coverings of the sphere by the double torus, and a general form for higher genera, *J. Combinatorial Theory* (A) 88, 1999, 259–275.

[47] I.P. Goulden and D.M. Jackson, A proof of a conjecture for the number of ramified coverings of the sphere by the torus, *J. Combinatorial Theory* (A) 88, 1999, 246–258.

[48] I.P. Goulden, D.M. Jackson and A. Vainshtein, The number of ramified coverings of the sphere by the torus and surfaces of higher genera, *Annals of Combinatorics* 4, 2000, 27–46.

[49] J.H. Kwak and A.D. Mednykh, Enumeration of branched coverings of closed orientable surfaces whose branch orders coincide with multiplicity, *Studia Scientiarum Mathematicarum Hungarica* 44 (2007), 215–223.

[50] C.L. Ezell, Branch point structure of covering maps onto nonorientable surfaces, *Trans. Amer. Math. Soc.* 243 (1978), 123–133.

[51] J. Lee and J. Kim, Enumeration of the branched $m\mathbb{Z}_p$-coverings of surfaces, *European J. Combin.* 22 (2001), 1125–1138.

[52] S. Zdravkovska, The topological classification of polynomial mappings. *Uspehi Mat. Nauk* 25 154(4) (1970), 179–180.

[53] A.G. Khovanskii, S. Zdravkovska, Branched covers of S^2 and braid groups. *J. Knot Theory Ramifications* 5 (1996), no. 1, 55–75.

[54] A.N. Protopopov, Homeomorphisms of branched coverings of a two-dimensional sphere, *Dokl. Akad. Nauk SSSR* 290(4) (1986), 792–795.

[55] A.N. Protopopov, Topological classification of branched coverings of a two-dimensional sphere, *J. Soviet Math.* 52(1) (1990), 2832–2846.

[56] G.A. Jones, A. Zvonkin, Alexander, Orbits of braid groups on cacti. *Mosc. Math. J.* 2 (2002), no. 1, 127–160, 200.

[57] M. Tanabe, Bounds on the number of holomorphic maps of compact Riemann surfaces, *Proc. Amer. Math. Soc.* 133(10) (2005), 3057–3064.

[58] H. Martens, Observations on morphisms of closed Riemann surfaces, *Bull. London Math. Soc.* 10 (1978), 209–212.

[59] H. Martens, Observations on morphisms of closed Riemann surfaces II, *Bull. London Math. Soc.* 20 (1988), 253–254.

[60] A. Howard, A.J. Sommese, On the theorem of de Franchis, *Ann. Scoula. Norm. Sup. Pisa Cl. Sci.* (4) 10 (1983), 429–436.

[61] E. Pervova, C. Petronio, On the existence of branched coverings between surfaces with prescribed branch data, *I. Algebr. Geom. Topol.* 6 (2006), 1957–1985.

[62] J.W. Alexander, Note on Riemann spaces, *Bull. Amer. Math. Soc.* 26 (1920), 370–372.

[62] J.L. Gross and T.W. Tucker, *Topological Graph Theory*, Wiley (1987).

[63] A.D. Mednykh, Determination of the number of nonequivalent coverings over a compact Riemann surface, *Soviet Math. Dokl.* 19 (1978), 318–320.

[64] S. Monni, Jun S. Song, Yun S. Song, The Hurwitz enumeration problem of branched covers and Hodge integrals, *J. Geom. Phys.* 50 (2004), no. 1–4, 223–256.

[65] M. Škoviera, A contribution to the theory of voltage graphs, *Discrete Math.* 61 (1986), 281–292.

[66] V.D. Tonchev, *Combinatorial Configurations Designs, Codes, Graphs, English version*, Wiley (1988).

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Combinatorial facets of Hurwitz numbers

S.K. Lando
State University—Higher School of Economics, Institute for System Research RAS and the Poncelet Laboratory, Independent University of Moscow

ABSTRACT: Hurwitz numbers were introduced by A. Hurwitz in the end of the nineteenth century. They enumerate ramified coverings of two-dimensional surfaces. They also have many other manifestations: as connection coefficients in symmetric groups, as numbers enumerating certain classes of graphs, as Gromov–Witten invariants of complex curves. Certain series of Hurwitz numbers can be expressed by nice explicit formulas, and the corresponding generating functions provide solutions to integrable hierarchies of mathematical physics. The paper surveys recent progress in understanding Hurwitz numbers, with stress made on their combinatorial rather than geometric nature.

Hurwitz numbers were introduced by A. Hurwitz in the end of the nineteenth century. They enumerate ramified coverings of two-dimensional surfaces with prescribed ramification types. Recently, Hurwitz numbers attracted a close attention of many researchers because of their appearance in a variety of important applications including the geometry of moduli spaces of algebraic curves and meromorphic functions, the Gromov–Witten invariants of algebraic curves, and integrable hierarchies of mathematical physics. In the present paper, we survey recent progress in understanding the combinatorial properties of Hurwitz numbers.

Hurwitz's original approach [13, 14] treats Hurwitz numbers by means of characters of symmetric groups. Numerous publications, of which we mention only [12, 25], follow the same way. However, a direct application of this approach leads to complicated formulas, which does not say much about the behavior of the answers as parameters vary. In contrast, Hurwitz himself gave in [14] a very simple and unexpected formula enumerating ramified coverings of the sphere by the sphere with a single point of degenerate ramification (see Sec. 3). Many other species of Hurwitz numbers also admit very explicit and clear expressions. It was understood recently that these simple formulas reflect a simple underlying geometry, see [6, 19, 23, 24].

In the present paper, we concentrate on combinatorial approaches to Hurwitz numbers. The only geometric fact we mention is the ELSV formula expressing simple Hurwitz numbers in terms of intersection indices on moduli spaces of algebraic curves, because it is the only known way to deduce many important combinatorial properties. On the other hand, by using purely combinatorial (including symmetric group representations) methods one can obtain such important results as the cut-and-join equation for the generating function for simple Hurwitz numbers [8], the Bousquet-Mélout–Schaeffer formula for the number of representations of a given permutation as a product of a given number of permutations [2], the Toda hierarchy for the generating function for double Hurwitz numbers [27], and the KP hierarchy for the generating function for simple Hurwitz numbers [18].

The paper is organized as follows. In Sec. 1 we give a definition of simple and various other species of Hurwitz numbers in terms of decompositions of permutations into products. We also describe their relationship with the problem of enumerating ramified coverings. Section 2 is devoted to the cut-and-join equation, a simple, but powerful tool for studying simple Hurwitz numbers. In Sec. 3 we present certain explicit formulas for Hurwitz numbers enumerating ramified coverings of the sphere by the sphere, which is, in a sense, the simplest possible case. In Sec. 4 we discuss formulas describing the behavior of Hurwitz numbers as the degree of the covering grows preserving the degenerate ramification type. The corresponding generating functions belong to a certain algebra of power series also described in this section. Section 5 produces a brief introduction to the theory of Kadomtsev–Petviashvili integrable hierarchy of partial differential equations, and in Sec. 6 we prove that the generating function for simple connected Hurwitz numbers is a solution to this hierarchy. Section 7 reproduces the ELSV formula, which is necessary to obtain the results in Sec. 4 and many others. Finally, in Sec. 8 we give more details about shifted symmetric functions which appear naturally in Sec. 5 and discuss possible generalizations of Hurwitz numbers.

I am obliged to M. Kazarian for numerous clarifying discussions. Various parts of this text were presented as talks in the University of Utrecht, Netherlands, Mittag-Leffler Institute and KTH, Stockholm, Sweden, and the Laboratory of Combinatorial and Computational Mathematics of the Pohang University of Science and Technology, Pohang, South Korea. I am grateful to D. Siersma, T. Ekedahl, C. Faber, and J.H. Kwak for the opportunity to give these talks.

1 HURWITZ NUMBERS

1.1 *Simple and general Hurwitz numbers*

Let S_n denote the symmetric group consisting of permutations of n elements $\{1, 2, \dots, n\}$. Any permutation $\sigma \in S_n$ can be represented as a product of transpositions, and there are many such representations. For a given m, we are interested in enumeration of m-tuples of transpositions $\tau_1, \dots, \tau_m$ whose product is a given permutation σ,

$$\sigma = \tau_m \circ \cdots \circ \tau_1.$$

The following statements are clear:

- the number of such representations depends on the cyclic type of the permutation σ rather than on the permutation itself;
- there is a minimal number $m_{\min} = m_{\min}(\sigma)$ for which such a representation exists, and this minimal number is $n - c(\sigma)$, where $c(\sigma)$ is the number of cycles in σ. Indeed, the minimal number of transpositions whose product is a cycle of length l is $l - 1$;
- all values of m for which the number of representations is nonzero have the same parity, which coincides with the parity of the permutation σ.

Now we are ready to give a precise definition of a simple Hurwitz number.

Definition 1. Let μ be a partition of n, $\mu \vdash n$. The *simple Hurwitz number* $h^{\circ}_{m;\mu}$ is defined as

$$h^{\circ}_{m;\mu} = \frac{1}{n!} |\{(\tau_1, \dots, \tau_m), \tau_i \in C_2(S_n) | \tau_m \circ \cdots \circ \tau_1 \in C_\mu(S_n)\}|.$$

Here $C_2(S_n)$ denotes the set of all transpositions in S_n, and $C_\mu(S_n)$ is the set of all permutations of cyclic type $\mu \vdash n$ in S_n, so that, in particular, $C_2(S_n) = C_{1^{n-2}2^1}(S_n)$. The *connected simple Hurwitz number* $h_{m;\mu}$ is defined in a similar way, but we take into account only m-tuples of transpositions such that the subgroup $\langle \tau_1, \dots, \tau_m \rangle \subset S_n$ they generate acts transitively on the set $\{1, \dots, n\}$.

The terminology has a topological origin and will be explained later. Let us compute several simple Hurwitz numbers. Below, we denote partitions in one of the two equivalent ways: either as a sequence of decreasing parts, $\mu = (\mu_1, \mu_2, \dots)$, where $\mu_1 \ge \mu_2 \ge \dots$, with only finitely many nonzero parts, or in the multiplicative form $1^{k_1} 2^{k_2} \dots$, where k_i denotes the multiplicity of the part i in the partition, all but finitely many multiplicities being 0 (and the corresponding parts omitted in the notation).

Example 1. Let $n = 3$ and let $\mu = 3^1$. Then the product of any two distinct transpositions produces a cyclic (of length 3) permutation, and the subgroup generated by these two transpositions coincides with S_3, whence acts transitively. Thus

$$h^\circ_{2;3^1} = h_{2;3^1} = \frac{1}{6} \cdot 6 = 1,$$

since there are $3 \cdot 2 = 6$ ordered pairs of distinct transpositions.

Note that if a simple Hurwitz number and the corresponding connected simple Hurwitz number both are nonzero, then they coincide if and only if the permutation σ is cyclic: in this case the subgroup of the symmetric group generated by the permutations τ_i automatically acts transitively, while in all other cases this statement is false.

Example 2. Let $n = 4$ and let $\mu = 4^1$. A cyclic permutation of length 4 can be represented as a product of 3 transpositions, and this is the minimal possible number of transpositions in the decomposition. There are $6^3 = 216$ ordered triples of transpositions.

A product of 3 transpositions, being an odd permutation, can be either a cyclic permutation (of cyclic type 4^1), or a transposition (of cyclic type $1^2 2^1$). The cycle can be obtained if either the two transpositions τ_1, τ_2 are independent, and τ_3 mixes the two permuted parts together ($6 \cdot 4 = 24$ ways), or if τ_1, τ_2 have one element in common, and τ_3 permutes the fourth element ($6 \cdot 4 \cdot 3 = 72$ ways). This yields the following value of the Hurwitz numbers:

$$h^\circ_{3;4^1} = h_{3;4^1} = \frac{1}{24} \cdot (24 + 72) = 4.$$

As the order of the symmetric group and the complexity of the partition grow, the direct computation becomes more involved, and we give only one example in addition.

Example 3. Let $n = 3$ and let $\mu = 1^1 2^1$ be the type of a transposition. Of course, a transposition can be represented as a single transposition. But it also admits a representation as a product of 3 transpositions. Moreover, the product of any triple of transpositions, being an odd permutation, is a transposition. Hence

$$h^\circ_{3;1^1 2^1} = \frac{1}{6} \cdot 3^3 = \frac{9}{2}.$$

Among the $3^3 = 27$ triples of transpositions, 3 correspond to subgroups acting nontransitively (those consisting of triples of coinciding transpositions). Thus

$$h_{3;1^1 2^1} = \frac{1}{6} \cdot (27 - 3) = 4.$$

This example shows that Hurwitz numbers are not necessarily integers. This is true even for the simplest case,

$$h^\circ_{1;2^1} = h_{1;2^1} = \frac{1}{2} \cdot 1 = \frac{1}{2}.$$

More generally, for a tuple $\mu_1, \dots, \mu_m$ of partitions of n, we can consider general Hurwitz numbers enumerating representations of the identity permutation as the product of the form

$$\sigma_m \circ \cdots \circ \sigma_1,$$

where each permutation σ_i has the cyclic type μ_i, $1 \le i \le m$. (For simple Hurwitz numbers, all the permutations but one are transpositions, and the last permutation is σ^{-1}, whose cyclic type coincides with that of σ). The *general Hurwitz number* is defined as the number of m-tuples of permutations $\sigma_1, \dots, \sigma_m$ of given cyclic types whose product is the identity permutation, divided by $n!$. *Connected Hurwitz numbers* are defined similarly, but with the restriction that the subgroup $\langle \sigma_1, \dots, \sigma_m \rangle \subset S_n$ generated by the permutations σ_i must act transitively. We do not introduce notation for general Hurwitz numbers, since we are not going to use them in our survey.

1.2 *Topological interpretation*

Hurwitz numbers naturally arise in the problem of enumeration of ramified coverings of the 2-sphere. Below, we consider only oriented two-dimensional surfaces without boundary. An orientation preserving continuous mapping $f : E_1 \to E_2$ of two surfaces is called a *covering* if it is a local homeomorphism, that is, for each point $t \in E_2$ there is a disk neighborhood $U = U(t) \subset E_2$ such that its total preimage $f^{-1}(U) \subset E_1$ is a disjoint union of disks, and the restriction of f to each of these disks is a homeomorphism. If E_2 is connected, then the number of disks in the preimage of any disk neighborhood U is the same whatever is the point t, and this number (which may well be infinite) is called the *degree* of the covering.

A *ramified covering* is a continuous mapping $f : E_1 \to E_2$ that becomes a covering after puncturing the target surface E_2 at finitely many points and such that each of the punctures possesses a disk neighborhood whose total preimage is a disjoint union of disks. Locally, at a neighborhood of each point in E_1, a ramified covering looks like $z \mapsto z^k$, where z is an appropriate complex local coordinate. For all but finitely many points in E_1, the value of k is 1, and it is greater than 1 for some preimages of the punctures. It is called the *degree* of the preimage. For any point $t \in E_2$, the sum of the degrees of all its preimages is the same, and it is called the *degree* of the ramified covering. In other words, the degrees of the preimages of any point form a partition of the degree of the covering. For a ramified covering of degree n, all partitions different from 1^n constitute the *ramification type* of the covering. Below, we shall consider finite ramified coverings of the 2-sphere S^2 by compact oriented two-dimensional surfaces.

Consider the ramified covering $z \mapsto z^k$ of the unit disk by the unit disk. As a nonzero point in the target disk goes around 0 and returns to its initial position, its k preimages experience a cyclic permutation of length k. This property allows one to associate to a ramified covering of the sphere a tuple of permutations.

Let f: $E \to S^2$ be a ramified covering of degree n, and let $t_1, \dots, t_m \in S^2$ be all its points of ramification. Pick a point $t \in S^2$ distinct from all t_i and connect it with the points t_i by smooth nonintersecting segments, whose cyclic order at t coincides with the numbering. Now make each segment into a narrow path γ_i around the ramification point in the positive direction. Then the path γ_i induces a permutation σ_i of the fiber $f^{-1}(t)$. The cyclic type of the permutation σ_i coincides with the partition given by the degrees of the preimages in $f^{-1}(t_i)$, and the product $\sigma_m \circ \cdots \circ \sigma_1$ is the identity permutation of the fiber $f^{-1}(t)$, since the product of the paths $\gamma_m \circ \cdots \circ \gamma_1$ is contractible in the punctured sphere $S^2 \setminus \{t_1, \dots, t_m\}$.

The m-tuple of permutations of the fiber determines the covering uniquely. By numbering the preimages $f^{-1}(t)$ of the generic point from 1 to n, we can make each permutation σ_i into a permutation of the set $\{1, 2, \dots, n\}$. Since there are $n!$ possible numberings, we conclude that Hurwitz numbers enumerate ramified coverings of the 2-sphere, with prescribed ramification types. The covering surface is connected if and only if the subgroup of S_n generated by the permutations σ_i acts transitively on the fiber $f^{-1}(t)$, which justifies the definition of connected Hurwitz numbers.

Let $E \to S^2$ be a ramified covering. The Riemann–Hurwitz formula allows one to recover the Euler characteristic $\chi(E)$ of the covering surface E from the ramification type. We shall use this formula only for the case of simple Hurwitz numbers, where it acquires the form

$$m = |\mu| + c(\mu) - \chi(E).$$

Here μ is a partition of $n = |\mu|$, $c(\mu)$ is the number of parts in the partition, and m is the number of transpositions. If the covering surface is connected, then its Euler characteristic is $\chi(E) = 2 - 2g$, where g is the genus of the surface. Hence the number m of points of simple ramification can be considered as a substitute for the genus of the covering surface.

1.3 *Double Hurwitz numbers*

In addition to simple Hurwitz numbers, double Hurwitz numbers are of special interest. The latter enumerate decompositions of a product $\sigma_1 \circ \sigma_2$ of a pair of permutations into a product of transpositions. These numbers enumerate ramified coverings of the sphere with two points of degenerate ramification. By definition,

$$h^{\circ}_{m;\mu_1,\mu_2} = \frac{1}{n!}|\{(\tau_1,\dots,\tau_m), \tau_i \in C_2(S_n)|\tau_1 \circ \cdots \circ \tau_m = \sigma_2 \circ \sigma_1, \sigma_j \in C_{\mu_j}(S_n)\}|,$$

where μ_1, μ_2 are two partitions of n.

Double Hurwitz numbers arise naturally in the computation of equivariant Gromov–Witten invariants of the projective line, see [31, 27].

2 CUT-AND-JOIN EQUATION

Collect the simple Hurwitz numbers into two generating functions:

$$H^{\circ}(u;p_1,p_2,\dots) = \sum_{m=1}^{\infty}\sum_{\mu} h^{\circ}_{m;\mu} p_{\mu_1} p_{\mu_2} \dots \frac{u^m}{m!}; \tag{1}$$

$$H(u;p_1,p_2,\dots) = \sum_{m=1}^{\infty}\sum_{\mu} h_{m;\mu} p_{\mu_1} p_{\mu_2} \dots \frac{u^m}{m!}, \tag{2}$$

where in each case μ runs over the set of all partitions.

A very general combinatorial construction justifies the following relationship between these two generating functions.

Proposition 4. *We have $H^{\circ} = \exp(H)$.*

This assertion allows one to translate statements about simple Hurwitz numbers into statements about connected simple Hurwitz numbers and vice versa.

Theorem 5 (cut-and-join equation, [8]). *The generating function H° for simple Hurwitz numbers satisfies the following partial differential equation:*

$$\frac{\partial H^{\circ}}{\partial u} = \frac{1}{2}\sum_{n=1}^{\infty}\sum_{i+j=n}\left((i+j)p_i p_j \frac{\partial}{\partial p_{i+j}} + ij p_{i+j}\frac{\partial^2}{\partial p_i \partial p_j}\right)H^{\circ}. \tag{3}$$

Before proving the theorem, let us note that the cut-and-join equation provides an explicit formula for the generating function H°. Indeed, assign to the variable p_i the weight i, $i = 1, 2, \dots$, so that a monomial $p_1^{k_1} p_2^{k_2} \dots$ has the weight $k_1 + 2k_2 + \cdots$. Then the function H° can be represented as the sum of the functions $H^{\circ} = H^{\circ}_0 + H^{\circ}_1 + \cdots$, where $H^{\circ}_k = H^{\circ}_k(u;p_1,p_2,\dots)$ is the sum of the monomials of weight k in H°. Each H°_k is a sum of finitely many monomials in p_i (their number is that of partitions of k) whose coefficients are power series in u. Since both operators $\frac{\partial}{\partial u}$ on the left and

$$A = \frac{1}{2}\sum_{n=1}^{\infty}\sum_{i+j=n}\left((i+j)p_ip_j\frac{\partial}{\partial p_{i+j}} + ijp_{i+j}\frac{\partial^2}{\partial p_i \partial p_j}\right)$$

on the right of Eq. (3) preserve the weights of the monomials, this equation is decomposed into the direct sum of finite dimensional equations, one for each of the functions H_k°.

The initial conditions are provided by the fact that there is a unique connected covering of the 2-sphere without ramification points, which is the identical covering of degree 1. This yields

$$H(0;p_1,p_2,\dots) = p_1,$$

whence

$$H^\circ(0;p_1,p_2,\dots) = e^{p_1},$$

or

$$H_k^\circ(0;p_1,p_2,\dots) = \frac{p_1^k}{k!}.$$

For a given k, the finite dimensional cut-and-join equation can be solved explicitly. Let us look at examples. The vector space of quasihomogeneous polynomials in p_i of weight 1 is spanned by the unique monomial p_1. The operator A takes this monomial to 0, whence $H_1^\circ = p_1$. The vector space of polynomials of weight 2 is spanned by two monomials, namely, p_1^2 and p_2. We have

$$A : p_1^2 \mapsto p_2; \quad A : p_2 \mapsto p_1^2.$$

Hence the eigenvectors of the operator A are the Schur polynomials

$$s_{2^1} = \frac{1}{2}(p_1^2 + p_2); \quad s_{1^2} = \frac{1}{2}(p_1^2 - p_2),$$

and the eigenvalues are 1 and -1, respectively. Taking the initial conditions $H_2^\circ(0;p_1,\dots) = p_1^2/2$ into account, we obtain

$$H_2^\circ = \frac{1}{2}s_{2^1}e^u + \frac{1}{2}s_{1^2}e^{-u}.$$

More generally, for arbitrary k, the Schur polynomials s_μ, $\mu \vdash k$, form a complete set of eigenvectors of the operator A restricted to the subspace of degree k quasihomogeneous polynomials, with eigenvalues given by the function

$$f_2(\mu) = \frac{1}{2}\sum_{i=1}^{\infty}\left(\left(\mu_i + \frac{1}{2} - i\right)^2 - \left(\frac{1}{2} - i\right)^2\right)$$

(we shall see the reasons for this and justify the notation f_2 in Sec. 6.1 below). Together with the initial conditions this yields

$$H_k^\circ(u;p_1,p_2,\dots) = \sum_{\mu \vdash k} s_\mu(1,0,0,\dots)s_\mu e^{f_2(\mu)u}.$$

Another, and maybe simpler way of looking at the function H° is to expand it in a power series in u,

$$H^\circ(u;p_1,p_2,\dots) = \sum_{k=0}^{\infty} H^\circ_{(k)}(p_1,p_2,\dots)\frac{u^k}{k!}.$$

Then the cut-and-join equation can be rewritten as the recurrence

$$H^\circ_{(k+1)} = \frac{1}{2}\sum_{n=1}^{\infty}\sum_{i+j=n}\left((i+j)p_ip_j\frac{\partial}{\partial p_{i+j}} + ijp_{i+j}\frac{\partial^2}{\partial p_i \partial p_j}\right)H^\circ_{(k)}.$$

Starting with $H^\circ_{(0)} = e^{p_1}$, we immediately obtain the first few terms of the expansion:

$$H^\circ(u;p_1,p_2,\dots) = e^{p_1}\left(1 + \frac{1}{2}p_2\frac{u}{1!} + \left(p_1^2 + \frac{1}{2}p_2^2 + p_3\right)\frac{u^2}{2!} + \cdots\right).$$

Note that the application of the operator on the right-hand side of the cut-and-join equation to the function $H^\circ_{(k)}$ always produces finitely many nonzero terms, although the operator itself contains infinitely many of them. The reason is that the function $H^\circ_{(k)}$ has the form e^{p_1} times a polynomial in $p_1,\dots,p_k$, and its derivatives over each p_l with $l > k$ vanish.

Proof of the cut-and-join equation. The cut-and-join equation describes what happens if one of the transpositions in the decomposition of a given permutation is glued with the distinguished permutation, that is, we replace the representation

$$\sigma = \tau_m \circ \tau_{m-1} \circ \cdots \circ \tau_1$$

by the representation

$$\tau_m \circ \sigma = \tau_{m-1} \circ \cdots \circ \tau_1$$

(here we used the fact that τ_m^2 is the identity permutation). Decreasing of the number of transpositions on the right by one reflects the derivation with respect to u on the left of the cut-and-join equation (3), since this procedure diminishes the degree of u by 1.

Multiplication by a transposition τ_m can change the permutation σ in one of the two different ways: either τ_m exchanges two elements belonging to the same cycle of σ, or the elements it exchanges belong to distinct cycles. In the first case, a cycle in σ is split into two cycles the sum of whose lengths coincides with the length of the initial one. In the second case, conversely, two cycles are glued into a single cycle of length equal to the sum of the lengths of the two. Each of the two summands on the right of the cut-and-join equation is in charge of the corresponding possibility. The coefficients reflect the number of ways to choose two elements to be transposed by τ_m: for each of the $i+j$ elements in a cycle of length $i+j$ an appropriate pair can be chosen in a unique way (if we fix the cyclic order), while in two cycles, of length i and j, respectively, there are ij choices for a pair whose transposition glues them together. The theorem is proved.

In Sec. 6.1, we shall rewrite this proof into a more conceptual language.

3 CERTAIN FORMULAS FOR RATIONAL HURWITZ NUMBERS

Hurwitz numbers are said to be *rational* if the number of transpositions in the decomposition is the minimal possible one. The terminology comes from the fact that these numbers enumerate ramified coverings of the sphere by the sphere, that is, rational functions. Thus, rational Hurwitz numbers are, in a sense, the simplest species of Hurwitz numbers, and there are a number of explicit formulas for them.

The first such formula is a formula, due to Hurwitz (1902), for rational connected simple Hurwitz numbers.

Theorem 6 ([14]). *We have*

$$h_{|\mu|+n-2;\mu} = (|\mu|+n-2)!\prod_{i=1}^{n}\frac{\mu_i^{\mu_i}}{\mu_i!}|\mu|^{n-3},$$

where $\mu = (\mu_1,\dots,\mu_n)$ is a partition of $|\mu| = \mu_1 + \cdots + \mu_n$.

Here $|\mu| + n - 2$ is the minimal number of transpositions in a product that can produce a permutation of cyclic type μ. In fact, Hurwitz did not publish the proof of his formula stating that it is too long for a journal paper. The first proof was given in [8], and the ELSV formula provides an alternative geometric proof [6].

Another instance of formulas for rational Hurwitz numbers is the following

Theorem 7 ([8]). *The number of factorizations of a cyclic permutation in S_n into a product of permutations of cyclic types $\nu_1,\dots,\nu_k$, $\nu_i \dashv n$, is*

$$n^{k-1}\frac{(c(\nu_1)-1)!}{|\mathrm{Aut}(\nu_1)|}\cdots\frac{(c(\nu_k)-1)!}{|\mathrm{Aut}(\nu_k)|},$$

where $c(\nu)$ denotes the number of parts in a partition ν, and $|\mathrm{Aut}(\nu)|$ is the order of the automorphism group of the partition (for $\nu = 1^{\ell_1}\dots n^{\ell_n}$, we have $|\mathrm{Aut}(\nu)| = \ell_1!\dots\ell_n!$).

The proof in [8] is purely combinatorial. Once again, the geometric proof was given in [22].

The formula due to Bousquet-Mélou and Schaeffer enumerates decompositions of a given permutation into a product of a given number of permutations, whatever are their types. It reads as follows.

Theorem 8 ([2]). *Denote by $G_\mu(r)$ the number of r-tuples of permutations whose product is a permutation of cyclic type μ, divided by $n!$, $\mu \vdash n$. We have*

$$G_\mu(r) = r\frac{((r-1)n-1)!}{((r-1)n-c(\mu)+2)!}\prod_i\binom{r\mu_i-1}{\mu_i}\mu_i,$$

where $c(\mu)$ is the number of parts in μ.

The original proof got a simplification in [11]. Similarly to the previous two formulas, this one also must have a geometric proof, which is still lacking.

4 THE STRING AND THE DILATON EQUATION, AND ENUMERATION OF PLANTED TREES

Minimal factorizations of a cyclic permutation into transpositions are in one-to-one correspondence with rooted label trees, which yields, by the Cayley formula,

$$h_{n-1;n} = n^{n-1}.$$

The exponential generating function for these numbers,

$$Y(q)=\sum_{n=1}^{\infty} h_{n-1;n}\frac{q^n}{n!}=\sum_{n=1}^{\infty} n^{n-1}\frac{q^n}{n!}=\frac{1}{1!}q+\frac{2}{2!}q^2+\frac{9}{3!}q^3+\frac{64}{4!}q^4+\cdots,$$

together with the exponential generating function

$$Z(q)=\sum_{n=1}^{\infty} n^n\frac{q^n}{n!}=\frac{1}{1!}q+\frac{4}{2!}q^2+\frac{27}{3!}q^3+\cdots.$$

generate a very interesting algebra of power series. Although the functions Y and Z look very similar, their behavior with respect to multiplication is quite different. We denote by $\mathcal{A}$ the algebra of power series generated by Y and Z. Note that the functions Y and Z are algebraically dependent:

$$Z(q)=\frac{1}{1-Y(q)}.$$

Denote by $h_{g,n;\mu_1,\dots,\mu_k}$ the Hurwitz number enumerating, with the weight equal to the inverse order of the automorphism group of the covering, ramified coverings of the 2-sphere by surfaces of genus g possessing the following properties:

- over given k points in S^2, the ramification types are $\mu_1,\dots,\mu_k$, and, in addition, there are necessarily many (that is, $n-|\mu_i|$) simple sheets over each of these points;
- besides these k points of degenerate ramification, there is a required number of given points of simple ramification.

Consider the exponential generating function for these numbers:

$$H_{g;\,\mu_1,\dots,\mu_k}(q)=\sum_{n=1}^{\infty} h_{g,n;\,\mu_1,\dots,\mu_k}\frac{q^n}{n!}.$$

Theorem 9 ([10, 39, 40]). *For any set of partitions $\mu_1,\dots,\mu_k$ and any g, with the exception of the case $g=1,k=0$, the generating function $H_{g;\mu_1,\dots,\mu_k}(q)$ belongs to the algebra $\mathcal{A}$.*

In the case of a single point of degenerate ramification, Theorem 9 acquires the form due to M. Kazarian.

Theorem 10 ([17]). *Let $\mu=(\mu_1,\dots,\mu_p)$ be a partition, $|\mu|=\mu_1+\cdots+\mu_p$. Then*

$$H_{g;\,\mu}(q)=Y^m(q)(Z(q)+1)^{2g-2+p}\varphi_{g;\mu}(Z(q)),$$

where Y and Z are the generators of the algebra $\mathcal{A}$, and $\varphi_{g;\mu}$ is a polynomial of degree at most $3g-3+p$.

Theorem 10 allows one to obtain explicit formulas for certain series of simple Hurwitz numbers by computing only finitely many elements of these series. Namely, knowing $3g-2+p$ values, we can reconstruct the coefficients of the polynomial $\varphi_{g;\mu}$, whence the whole expression for the generating function $H_{g;\mu}$.

Theorem 9 is proved by induction on the number k of ramification points, the base being provided by Theorem 10. The main reason why Theorem 10 is true is that the Hurwitz numbers satisfy the so-called *string* and *dilaton* equations well known in the intersection theory on moduli spaces of complex curves of given genus. Simple Hurwitz numbers can be expressed in terms of this theory by means of the *ELSV formula* [5, 6], see Sec. 7 below.

Now we give a combinatorial interpretation of the string and the dilaton equations for planted trees enumeration, due to D. Zvonkine [39, 40]. Enumeration of planted trees generalizes the Cayley formula enumerating trees, according to which the power series Y is the exponential generating function for rooted marked trees.

The trees will be planted on certain simple graphs. Graphs we consider are undirected, and they may have loops and multiple edges. A rooted graph H is said to be *simple* if (i) it is connected; (ii) it contains no vertices of valency 1 except for, may be, the root and the vertices adjacent to the root, and it contains no vertices of valency 2 except for, may be, the root. Let G be a rooted connected graph, and let v be a vertex of valency 1 (a leaf) in G that is neither the root, nor a root's neighbor. Then the graph $S_v(G)$ is obtained from G by erasing the vertex v together with the edge connecting it with a vertex in G. For a vertex w of valency 2 that is not the root, the graph $D_w(G)$ is obtained by deleting w with further merging the two outgoing half-edges thus making them into a single edge.

Applying operations S and D to appropriate vertices of a rooted connected graph in an arbitrary order, we obtain a simple graph, which is independent of the order of the operations we have applied. This simple graph H is called the *base* of the initial graph G, and we say that G is a *forest planted on* H.

Denote by $f_H(n)$ the weighted number of rooted graphs with $n+1$ vertices whose base is H and whose vertices different from the root are marked by distinct numbers from 1 to n. The weight in question is inverse to the order of the symmetry group of the marked graph. Now introduce the generating function

$$F_H(q) = \sum_{n=0}^{\infty} \left(f_H(n) \frac{q^n}{n!} \right)$$

where the summation is carried over all forests planted on H. Then

$$F_H(q) = \frac{1}{|\mathrm{Aut}(H)|} Y^{|V(H)|}(1+Z)^{|E(H)|}. \tag{4}$$

here $|V(H)|$ is the number of vertices in H, the root not taken into account, and $|E(H)|$ is the number of edges in H. Thus the generating function $F_H(q)$ lies in the algebra $\mathcal{A}$.

The proof of Eq. (4) is simple: the factor $Y^{|V(H)|}$ enumerates trees attached to the vertices of the base graph H, while the factor $(1+Z)^{|E(H)|}$ enumerates trees attached to the edges of the base graph H. Each tree of the first kind has a single root which is the vertex identified with the corresponding vertex of H. Each tree of the second kind has two distinguished vertices, namely, the two vertices that are the closest ones to the ends of the edge in H (note that these two vertices can coincide). There is a unique path in a tree connecting any given pair of vertices, and this path is identified with a segment in the edge to which the tree is attached. The generating function $1+Z$ is exactly the one enumerating marked trees with two distinguished vertices.

What the generating functions for the planted trees and for the Hurwitz numbers have in common, which justifies their belonging to the algebra $\mathcal{A}$, is the associated string and dilaton equations. Denote by $\langle \tau_{d_1} \dots \tau_{d_n} \rangle_H$ the weighted number of marked graphs with the base H with the vertex i having valency $d_i + 1$, $i = 1, \dots, n$. In particular,

$$f_H(n) = \sum_{d_1,\dots,d_n} \langle \tau_{d_1} \dots \tau_{d_n} \rangle_H.$$

Then the following relations hold:

$$\langle \tau_{d_1} \dots \tau_{d_n} \tau_0 \rangle_H = \langle \tau_{d_1 - 1} \dots \tau_{d_n} \rangle_H + \dots + \langle \tau_{d_1} \dots \tau_{d_n - 1} \rangle_H \quad \text{(string relation)}$$

$$\langle \tau_{d_1} \dots \tau_{d_n} \tau_1 \rangle_H = (2g - 2 + n) \langle \tau_{d_1} \dots \tau_{d_n} \rangle_H \quad \text{(dilaton relation)}$$

Here $g = b_1(H)$ is the first Betti number of H, that is, the number of independent cycles in it, and by the Euler formula we have $2 - 2g = |E(H)| - |V(H)| + 1$. The string relation describes the behavior of the number $\langle \tau_{d_1} \dots \tau_{d_n} \rangle_H$ under the operation S which deletes a leaf (a vertex of valency 1), while the dilaton equation describes the behavior of this number under the operation D which deletes a vertex of valency 2. The proof of both is immediate.

5 THE KP EQUATIONS AND SEMIINFINITE GRASSMANNIAN

The Kadomtsev–Petviashvili hierarchy is a completely integrable system of partial differential equations playing an important role in mathematical physics. A general theory of Kadomtsev–Petviashvili equations, due to Sato, interprets solutions to these equations as semiinfinite planes, that is, points in the semiinfinite Grassmannian. In this section, we present a brief overlook of Sato's construction. Proving that a given function is a solution, is reduced thus to identification of the semiinfinite plane corresponding to this function. There is no need, in particular, to know the explicit form of the equations. For the function $H(u;p_1,p_2,\dots)$, which is the generating function for simple Hurwitz numbers, we shall make this identification in the next section.

5.1 *Grassmannian embeddings and Plücker equations*

Consider the Grassmannian $G(2,4)$ of vector 2-planes in the 4-space $V \equiv \mathbb{C}^4$. Any 2-plane in V can be represented by the wedge product $\varphi_1 \wedge \varphi_2$ of any pair φ_1, φ_2 of linearly independent vectors in it. This wedge product is well defined up to a constant factor; it determines the 2-plane uniquely and thus defines an embedding of $G(2,4)$ into the projectivization of the wedge square of V, $G(2,4) \hookrightarrow P\Lambda^2 V$. An immediate generalization of this construction produces an embedding of any Grassmannian $G(k,n)$ of k-planes in n-space V into the projectivization $P\Lambda^k V$.

The *Plücker equations* are the equations of the image of this embedding. Note that the dimension of $G(k,n)$ is $k(n-k)$, while the dimension of $P\Lambda^k V$ is $\binom{n}{k} - 1$, whence, generally speaking, the image of the embedding does not coincide with the whole projectivized wedge product $P\Lambda^k V$. For example, the image of the embedding of $G(2,4)$ into $P\Lambda^2 V$ is a hypersurface in the 5-dimensional projective space.

Let us find the equation of this hypersurface. Pick a basis e_1, e_2, e_3, e_4 in V. Then $\Lambda^2 V$ is endowed with the natural basis $f_{ij} = e_i \wedge e_j$, $1 \le i < j \le 4$, and the corresponding natural coordinate system y_{ij}. The image of the embedding of the Grassmannian consists of decomposable vectors. By definition of the wedge product, for a pair of vectors (a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4), the image of the plane spanned by these two vectors has the projective coordinates

$$y_{ij} = \begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix} = a_i b_j - a_j b_i.$$

An immediate calculation shows that these coordinates satisfy the homogeneous equation

$$y_{12}y_{34} - y_{13}y_{24} + y_{14}y_{23} = 0,$$

and this is the Plücker equation of the image.

For general values of n and k, the Plücker equations still are quadratic equations. In other words, *the ideal in the ring of polynomials consisting of polynomials vanishing on the image of the Plücker embedding is generated by quadratic polynomials.*

5.2 *Space of Laurent series*

Take for the space V the infinite dimensional vector space of formal Laurent series in one variable. Elements of this space have the form $c_{-k}z^{-k} + c_{-k+1}z^{-k+1} + \cdots$. The powers z^k, $k = \dots, -2, -1, 0, 1, 2, \dots$ form the *standard* basis in V. By definition, the *semi-infinite wedge* *product* $\Lambda^{\frac{\infty}{2}} V$ is the vector space freely spanned by the vectors

$$v_\mu = z^{m_1} \wedge z^{m_2} \wedge z^{m_3} \wedge \dots, \qquad m_1 > m_2 > m_3 > \dots, \qquad m_i = \mu_i - i,$$

where μ is a partition, $\mu = (\mu_1, \mu_2, \mu_3, \dots)$, $\mu_1 \geq \mu_2 \geq \mu_3 \geq \dots$, and all but finitely many parts are 0. In particular, $m_i = -i$ for all i large enough.

The *vacuum vector*

$$v_\emptyset = z^{-1} \wedge z^{-2} \wedge z^{-3} \wedge \dots$$

corresponds to the empty partition. Similarly, we have

$$v_{1^1} = z^0 \wedge z^{-2} \wedge z^{-3} \wedge \dots, \qquad v_{2^1} = z^1 \wedge z^{-2} \wedge z^{-3} \wedge \dots,$$
$$v_{1^2} = z^0 \wedge z^{-1} \wedge z^{-3} \wedge \dots,$$

and so on.

5.3 *The boson-fermion correspondence*

Numbering basic vectors in the semiinfinite wedge product $\Lambda^{\frac{\infty}{2}} V$ by partitions establishes a natural vector space isomorphism between this space and the vector space of power series in infinitely many variables $p_1, p_2, \dots$. This isomorphism takes a basic vector v_μ to the Schur polynomial $s_\mu = s_\mu(p_1, p_2, \dots)$. The latter is a quasihomogeneous polynomial, of degree $|\mu|$, in the variables p_i, with the degree of p_i set to be i.

The *Schur polynomial* corresponding to a one-part partition is defined by the expansion

$$s_0 + s_1 z + s_2 z^2 + s_3 z^3 + s_4 z^4 + \dots = e^{p_1 z + p_2 \frac{z^2}{2} + p_3 \frac{z^3}{3} + \dots},$$

and for a general partition λ it is given by the determinant

$$s_\lambda = \det ||s_{\lambda_j - j + i}||. \tag{5}$$

The indices i,j here run over the set $\{1, 2, \dots, n\}$ for n large enough, and since $\lambda_i = 0$ for i sufficiently large, the determinant, whence s_λ, is independent of n. Here are a few first Schur polynomials:

$$s_0 = 1, \quad s_{1^1} = p_1, \quad s_{2^1} = \frac{1}{2}(p_1^2 + p_2), \quad s_{3^1} = \frac{1}{6}(p_1^3 + 3p_1p_2 + 2p_3),$$
$$s_{1^2} = \frac{1}{2}(p_1^2 - p_2), \quad s_{1^1 2^1} = \frac{1}{3}(p_1^3 - p_3), \quad s_{1^3} = \frac{1}{6}(p_1^3 - 3p_1p_2 + 2p_3).$$

5.4 *Semiinfinite Grassmannian and the KP equations*

The *semiinfinite Grassmannian* $G(\frac{\infty}{2}, \infty)$ consists of decomposable vectors in $P\Lambda^{\frac{\infty}{2}}$, that is, of vectors of the form

$$\varphi_1(z) \wedge \varphi_2(z) \wedge \varphi_3(z) \wedge \dots,$$

where each φ_i is a Laurent power series in z and, for i large enough, the leading term in the expansion of φ_i is z^{-i}:

$$\varphi_i(z) = z^{-i} + c_{i1} z^{-i+1} + c_{i2} z^{-i+2} + \cdots.$$

Definition 2. The *Hirota equations* are the Plücker equations of the embedding of the semiinfinite Grassmannian in the projectivized semiinfinite wedge product $P\Lambda^{\frac{\infty}{2}}V$. Solutions to the Hirota equations (that is, semiinfinite planes) are called *τ-functions* for the hierarchy.

As polynomial equations for the coefficients of the expansions of τ-functions, the Hirota equations can be treated as partial differential equations for the functions themselves. Being Plücker equations, the Hirota equations are quadratic in τ.

Definition 3. The form the Hirota equations take for the logarithms of τ-functions under the boson-fermion correspondence is called the *Kadomtsev–Petviashvili*, or *KP, equations*.

In other words, any solution to the KP equations can be obtained as the result of the following procedure:

- take a semiinfinite plane $\varphi_1(z) \wedge \varphi_2(z) \wedge \dots$ in V;
- by expanding, rewrite the corresponding point in the semiinfinite Grassmannian as a linear combination of the basic vectors v_λ and normalize so as the coefficient of $v_\emptyset$ becomes 1;
- replace in this linear combination each vector v_λ by the corresponding Schur polynomial $s_\lambda(p_1,p_2,\dots)$, which produces a series in infinitely many variables $p_1,p_2,\dots$;
- take the logarithm of the resulting series.

Example 11. The first KP equation for an unknown function $W = W(p_1,p_2,\dots)$ looks like

$$\frac{\partial^2 W}{\partial p_2^2} = \frac{\partial^2 W}{\partial p_1 \partial p_3} - \frac{1}{2}\left(\frac{\partial^2 W}{\partial p_1^2}\right)^2 - \frac{1}{12}\frac{\partial^4 W}{\partial p_1^4}$$

(pay attention to the fact that it is homogeneous, in a natural sense). Take $\varphi_1(z) = z^{-1} + az^0 + bz^1$, $a, b \in \mathbb{C}$, and set $\varphi_i(z) = z^{-i}$ for $i \geq 2$. Then the implementation of the above procedure yields:

$$\varphi_1 \wedge \varphi_2 \wedge \dots = v_\emptyset + av_{1^1} + bv_{2^1} \mapsto 1 + ap_1 + \frac{1}{2}b(p_1^2 + p_2).$$

Now,

$$W(p_1,p_2) = \log\left(1 + ap_1 + \frac{1}{2}b(p_1^2 + p_2)\right)$$

is a solution to the first KP equation (and, of course, to all of them). The fact that it is a solution to the first KP equation can be verified directly, but the verification is laborious.

5.5 *Action of the diagonal matrices*

Linear transformations of the vector space V of Laurent polynomials induce linear transformations of the semiinfinite wedge product $\Lambda^{\frac{\infty}{2}}V$. Since linear transformations of V take planes in V to planes, the induced transformations preserve the embedded Grassmannian. In this section we consider the action of those transformations that can be represented by diagonal matrices in the basis $\{z^k\}$ in V, $k \in \mathbb{Z}$: these are the only transformations we need in the study of simple Hurwitz numbers. By obvious reasons, the induced action on $\Lambda^{\frac{\infty}{2}}V$, written in the basis v_λ, also is diagonal.

Example 12. Consider the linear transformation $V \to V$ which multiplies z^{-1} by a constant a preserving all the other basic vectors. Clearly, the action of this transformation on $\Lambda^{\frac{\infty}{2}}V$, written in the basis v_λ, multiplies by a each basic vector containing z^{-1} in its decomposition ($v_\emptyset, v_{1^2}$, and so on), and preserves all other basic vectors (v_{1^1}, v_{2^1}, and so on). The requirement that z^{-1} enters the decomposition of a vector v_λ means that the partition λ contains a part λ_i such that $\lambda_i - i = -1$. Note that any partition can have at most one such part, since the parts λ_i follow in a decreasing order, while the sequence i grows strictly.

An important consequence of this example is that the eigenvalue of the action on $\Lambda^{\frac{\infty}{2}} V$ of a diagonal matrix on V corresponding to the eigenvector v_λ *depends symmetrically on the differences* $\lambda_i - i$. In other words, it belongs to the ring of so-called shifted symmetric functions.

Definition 4. A function on partitions $\lambda = (\lambda_1, \lambda_2, \dots)$ is said to be *shifted symmetric* if it is symmetric under permutations of the parts $\lambda_i - i$.

Let us stress once again that the parts $\lambda_1, \lambda_2, \dots$ of the partition λ go in the non increasing order, $\lambda_1 \geq \lambda_2 \geq \dots$, and all but finitely many of them are 0. The definition of a shifted symmetric function bases heavily on this order.

The space of shifted-symmetric functions depending on infinitely many variables is the projective limit Γ of spaces Γ_k of shifted symmetric functions depending on k variables. (In [28], the algebra Γ is denoted by Λ^*. We use a different notation in order to prevent confusion with the wedge products). The limit is taken with respect to the projections $\Gamma_{k+1} \to \Gamma_k$ obtained by setting the last argument equal to 0. All complex-valued shifted symmetric functions form an algebra. This algebra was introduced and thoroughly studied in [20]. The reason for introducing it is that the characters of certain natural elements in the centers of group algebras of symmetric groups are shifted symmetric.

Now, we have a naturally defined action on $\Lambda^{\frac{\infty}{2}} V$ of any diagonal matrix $z^k \mapsto a_k z^k$, $a_k \neq 0$, with *finitely many entries a_k with negative indices different from* 1. Indeed, were there infinitely many such coefficients, in order to compute the action of the corresponding matrix on a basic vector, say $v_\emptyset$, we would have to compute the product of infinitely many entries. Fortunately, the action on the *projectivized* space $P\Lambda^{\frac{\infty}{2}} V$, which is the main subject of our interest, can be extended to the action of diagonal matrices with infinitely many entries a_k with negative indices different from 1. Indeed, since we are interested in the action on the projectivized space, only the ratio of the eigenvalues of the basic eigenvectors matters, and this ratio is well defined for an arbitrary diagonal matrix.

Indeed, any two basic vectors $v_\lambda, v_\mu \in \Lambda^{\frac{\infty}{2}} V$ have a common tail: their decompositions are different in the beginning, but coincide after some position, say K. Hence the ratio of the corresponding eignevalues is just $\frac{a_{\lambda_1 - 1} \cdots a_{\lambda_K - K}}{a_{\mu_1 - 1} \cdots a_{\mu_K - K}}$ (and this explains why we impose the restriction that the diagonal entries of the matrix must not vanish). That is, we must define the action of a diagonal matrix on $\Lambda^{\frac{\infty}{2}} V$ in a way that preserves this ratio of eigenvalues. Thus the result depends only on the eigenvalue of the vacuum vector $v_\emptyset$, which can be chosen arbitrarily. The most natural normalization is to choose this eigenvalue to be 1. This yields the following induced action on $\Lambda^{\frac{\infty}{2}} V$ of a diagonal matrix (a_k) on V:

$$v_\lambda \mapsto \left(\prod_{i=1}^{\infty} \frac{a_{\lambda_i - i}}{a_{-i}} \right) v_\lambda .$$

The product in the brackets is well defined, since all but finitely many factors are 1. The action of the torus of diagonal matrices on the projectivized semiinfinite external product of V is just the inductive limit of the actions of the tori T_K consisting of diagonal matrices with diagonal entries a_i equal to 1 for $i = -(K+1), -(K+2), \dots$.

Since the action of the infinite dimensional torus $\bigoplus_{i \in \mathbb{Z}} (\mathbb{C}^*)_i$ on the projectivized semiinfinite wedge product is well defined, it also defines an action of the corresponding Lie algebra.

The latter action also is diagonal, and a diagonal matrix $(\alpha_i)_{i\in\mathbb{Z}}$ (with not necessarily nonzero entries) belonging to the Lie algebra acts on a basic vector v_λ by

$$v_\lambda \mapsto \left(\sum_{j=1}^{\infty}(\alpha_{\lambda_j-j}-\alpha_{-j})\right)v_\lambda.$$

5.6 *The KP hierarchy and the r-KdV hierarchies*

The r-KdV hierarchy, $r=2,3,\dots$, is a reduction of the KP hierarchy. Consider subspaces in V that are invariant under multiplication by z^r. Semiinfinite such subspaces form a sub-Grassmannian $G_r(\frac{\infty}{2},\infty)\subset G(\frac{\infty}{2},\infty)$. By definition, logarithms of the corresponding τ-functions are *solutions to the r-KdV hierarchies*. Under the boson-fermion correspondence, these logarithms are those solutions of the KP hierarchy that are independent of the coordinates p_i whose index i is divisible by r. The 2-KdV hierarchy is also referred to as just the KdV hierarchy.

The KP-hierarchy and the r-KdV hierarchies can be also deduced in another way. Consider *pseudodifferential operators* as operators on the space of functions on $\mathbb{C}$ of the form

$$a_k(z)\partial^k+a_{k-1}(z)\partial^{k-1}+\cdots+a_0(z)+a_{-1}(z)\partial^{-1}+a_{-2}(z)\partial^{-2}+\cdots, \qquad (6)$$

where ∂ is the operator of differentiation with respect to z, $\partial=d/dz$, and ∂^{-1} is the formal inverse operator. It commutes with ∂, $\partial\circ\partial^{-1}=\partial^{-1}\circ\partial$ is the identity operator, and the commutation relation with the operator of multiplication by a function $a(z)$ looks like

$$[\partial^{-1},a(z)]=-a'(z)\partial^{-1}+a''(z)\partial^{-2}-\cdots.$$

This rule allows one to represent any product of pseudodifferential operators in the standard form (6). A pseudodifferential operator is just a *differential operator* if the coefficients $a_i(z)$ are 0 for all negative i.

We denote the *positive part* of a pseudodifferential operator A by A_+; for a pseudodifferential operator presented in the standard form (6), this is the differential operator

$$a_k(z)\partial^k+a_{k-1}(z)\partial^{k-1}+\cdots+a_0(z).$$

For a family of pseudodifferential operators

$$Q=\partial+\alpha_{-1}(z;t_1,t_2,\dots)\partial^{-1}+\alpha_{-2}(z;t_1,t_2,\dots)\partial^{-2}+\cdots,$$

consider the sequence $Q_k=(Q^k)_+$. The operator Q_k is a differential operator of order k. Since $[Q^k,Q]=0$ for any k, the commutator $[Q_k,Q]$ of any such differential operator with Q is a pseudodifferential operator whose positive part is 0. This allows one to consider the system of differential equations

$$\frac{\partial Q}{\partial t_k}=[Q_k,Q],\quad k=1,2,3,\dots.$$

These differential equations are equations of the deformations of the coefficients α_{-i} of the operator Q in variables t_k, and these are the KP equations.

Remark 13. The KP equations for the unknown functions α_i in variables t_j thus obtained are related to the KP equations for semiinfinite planes in the space of Laurent polynomials in the following way. Denote by γ_i the residues (that is, coefficients of ∂^{-1}) of the operators Q^i:

$$\gamma_i(z;t_1,t_2,\dots)=\mathrm{Res}(Q^i),\quad i=1,2,\dots.$$

Then the functions γ_i can be expressed in terms of α_i by means of a triangular change of variables.

The r-KdV equations are specializations of the KP equations to the case where the operator Q is the rth root of a genuine differential operator

$$Q^r = \partial^r + \beta_2(z;t_1,t_2,\dots)\partial^{r-2} + \dots + \beta_r(z;t_1,t_2,\dots).$$

In this case, all the operators $Q^{mr} = Q_{mr}$, $m = 1,2,3,\dots$ commute with $Q^r = Q_r$, and we can consider the system of equations

$$\frac{\partial Q}{\partial t_k} = [Q_k, Q^r], \quad k = 1,2,3,\dots.$$

These equations, the r-KdV equations, are the equations on the unknown functions $\beta_2,\dots,\beta_r$, which are an alternative set of unknowns for $\alpha_{-1},\dots,\alpha_{1-r}$. Obviously, their solutions are independent of t_{mr} for $m = 1,2,3,\dots$. This system of equations is known to be completely integrable, which means, in particular, that it has a solution for any initial conditions $b_i(z) = \beta_i(z;0,0,\dots)$, $i = 2,\dots,r$.

As an example, let us write out the first equation in the KdV (= 2-KdV) hierarchy. For this hierarchy, the operator $Q^2 = Q_2$ is the second order differential operator

$$Q^2 = \partial^2 + U(z;t_1,t_3,t_5,\dots)$$

(we omit the variables with even indices, since $U = B_2$ is independent of them). The operator Q has the form

$$Q = \partial + \frac{1}{2}U\partial^{-1} - \frac{1}{4}U'\partial^{-2} + \cdots,$$

where prime denotes the z-derivative. Two first negative powers of ∂ in Q are sufficient to determine the differential operator Q_3:

$$Q_3 = (Q^3)_+ = \partial^3 + \frac{3}{2}U\partial + \frac{3}{4}U'.$$

Now, the commutator looks like

$$[Q_3, Q^2] = \frac{3}{2}U'U + \frac{1}{4}U''',$$

and the first equation of the hierarchy, the *KdV equation*, is

$$\frac{\partial U}{\partial t_3} = \frac{3}{2}U'U + \frac{1}{4}U'''.$$

6 SYMMETRIC GROUP REPRESENTATIONS

In this section, we prove that the generating series $H(u;p_1,p_2,\dots)$ for simple Hurwitz numbers is a solution to the KP hierarchy for each value of the parameter u. This statement is true for $u = 0$, since $H(0;p_1,p_2,\dots) = p_1$: the (nonramified) identical covering $S^2 \to S^2$ is the only one without points of simple ramification. For general value of u, the statement follows from the fact that $\exp(H)$ is an integral curve of a vector field in $P\Lambda^{\frac{\infty}{2}}V$ tangent to the semiinfinite Grassmannian. This vector field is induced by a linear transformation $V \to V$, which is diagonal in the standard basis z^k. Namely, this is the transformation $z^k \mapsto \left(k-\frac{1}{2}\right)^2 z^k$.

6.1 *Expressing Hurwitz numbers in terms of characters of symmetric groups*

Let S_n denote the symmetric group of permutations of n elements, and let $\mathbb{C}[S_n]$ be the $n!$-dimensional group algebra of this group. For each partition κ of n, denote by $C_\kappa \in \mathbb{C}[S_n]$ the sum of all permutations in S_n having the cyclic type κ. We will use a special notation C_1 for the class C_{1^n} of the unit permutation, which is the unit of the algebra $\mathbb{C}[S_n]$, and C_2 for the sum $C_{1^{n-2}2^1}$ of all transpositions. For any κ, the element C_κ is a central element in $\mathbb{C}[S_n]$. These elements span the center of $\mathbb{C}[S_n]$.

Example 14. The center of the group algebra $\mathbb{C}[S_3]$ is spanned by the three elements $C_1 = \mathrm{id}$, $C_2 = (12) + (23) + (13)$, and $C_3 = (231) + (312)$.

The simple Hurwitz numbers possess the following natural interpretation. Take the product of the class C_κ with the mth power of the class C_2. Then $h^\circ_{m;\kappa}$ is nothing but the coefficient of C_1 in the product $C_\kappa C_2^m$ divided by $n!$.

Example 15. For $n = 3$, $\kappa = 3^1$, and $m = 4$, we have

$$C_3C_2^4 = 54C_1 + 27C_3,$$

whence

$$h^\circ_{4;3^1} = h_{4;3^1} = \frac{54}{6} = 9.$$

(Let us explain how the coefficient 54 of the class C_1 in the above formula is obtained. Each of the 27 products of three transpositions in S_3 is a transposition. Taking for the fourth transposition one of the two transpositions different from the product we obtain 54 cyclic permutations, each producing the identity permutation when multiplied by exactly one element in C_3).

The coefficient of C_1 in a central element of the group algebra can be extracted by computing the trace of the action of this element on $\mathbb{C}[S_n]$ by multiplication either on the left or on the right. Indeed, multiplication by any permutation in S_n except for the identity element, being a permutation without fixed points of the basis in $\mathbb{C}[S_n]$, has zero trace. Hence multiplication by any basic element C_κ except for C_1 has zero trace, while the trace of multiplication by C_1 is $n!$, the dimension of the space of representation.

For each finite group G, there is a natural algebra isomorphism between its group algebra and the direct sum of the algebras of automorphisms of all its irreducible representations:

$$\mathbb{C}[G] = \oplus\,\mathrm{End}(V_i),$$

where the sum on the right is carried over all irreducible representations V_i of G. The irreducible representations of the symmetric group S_n are in a natural one-to-one correspondence with the partitions of n, whence, for $G = S_n$, we obtain

$$\mathbb{C}[S_n] = \bigoplus_{\mu\vdash n} \mathrm{End}(V_\mu). \tag{7}$$

Consider the central element

$$P = \sum_{\kappa\vdash n} p_\kappa C_\kappa \in \mathbb{C}[S_n][p_1, p_2, \dots],$$

where $p_\kappa = p_{\kappa_1}p_{\kappa_2}\dots$ is the monomial in formal variables and the summation is carried over all partitions κ of n. Now take the trace of the central element PC_2^m applied to both sides of the isomorphism (7). On the left, we obtain

$$n! \sum_{\kappa \vdash n} h^\circ_{m;\kappa} p_\kappa .$$

On the right, the trace can be computed by rearranging the sums:

$$\begin{aligned}
\operatorname{tr} PC_2^m &= \sum_{\kappa \vdash n} \operatorname{tr} p_\kappa C_\kappa C_2^m \\
&= \sum_{\mu \vdash n} \left(\operatorname{tr} \sum_{\kappa \vdash n} p_\kappa C_\kappa C_2^m \right) |_{\mathrm{End}(V_\mu)} \\
&= \sum_{\mu \vdash n} (f_2(\mu))^m s_\mu(p).
\end{aligned}$$

Here $f_2(\mu)$ is the trace of the action of the central element C_2 on the irreducible representation V_μ and $s_\mu(p)$ is, by (yet another) definition, the *Schur polynomial* corresponding to the partition μ,

$$s_\mu(p) = \sum_{\kappa \vdash |\mu|} p_\kappa \operatorname{tr} C_\kappa |_{V_\mu}.$$

The equivalence of the two definitions of the Schur polynomials is a standard fact known as the Frobenius theorem; the proof can be found, for example, in [33]. Finally, we obtain

$$\sum_{\kappa \vdash n} h^\circ_{m;\kappa} p_\kappa = \sum_{\mu \vdash n} s_\mu(1,0,0,\dots) s_\mu(p) f_2(\mu)^m .$$

After multiplication by $u^m/m!$ and summation over all m and n we conclude that

$$H^\circ(u; p_1, p_2, \dots) = \sum_\mu s_\mu(1,0,0,\dots) s_\mu(p) e^{f_2(\mu)u}.$$

6.2 *Toda equations for double Hurwitz numbers*

Double Hurwitz numbers $h^\circ_{m;\mu,\nu}$ were introduced in Sec. 1.3 as numbers enumerating ramified coverings of the sphere with two points of degenerate ramification, μ and ν being the corresponding ramification types. Introduce the generating series for double Hurwitz numbers:

$$H^\circ_{\mathrm{double}}(u; p_1, p_2, \dots, q_1, q_2, \dots) = \sum_{m=0}^{\infty} \sum_{\mu,\nu,|\mu|=|\nu|} h^\circ_{m;\mu,\nu} p_{\mu_1} p_{\mu_2} \dots q_{\nu_1} q_{\nu_2} \dots \frac{u^m}{m!}.$$

Here the second summation is carried over all pairs of partitions of the same number, and the two families of variables, p_i and q_j, are indexed by the parts of the corresponding partition. A theorem similar to that for simple Hurwitz numbers is valid for double Hurwitz numbers.

Theorem 16 ([27]). *The logarithm H_{double} of the generating function $H^\circ_{\mathrm{double}}$ is a one-parameter family of solutions to the Toda lattice hierarchy of partial differential equations.*

The Toda lattice hierarchy of partial differential equations was introduced by Ueno and Takasaki in [37]. We refer the reader to that paper for the details. It is similar in nature to the KP hierarchy. Okoun'kov's proof of the theorem is based on the following explicit form of the function $H^\circ_{\mathrm{double}}$:

$$H^\circ_{\mathrm{double}} = \sum_\mu e^{f_2(\mu)u} s_\mu(p_1, p_2, \dots) s_\mu(q_1, q_2, \dots),$$

which is obtained exactly in the same way as the formula for the simple Hurwitz numbers in the previous section.

7 THE ELSV FORMULA

The ELSV formula expresses simple Hurwitz numbers in terms of intersection indices of certain cohomology classes on moduli spaces of complex curves with marked points. In spite of its geometric origin, it has a number of combinatorial consequences. It reads

$$h_{m;b_1,\dots,b_n} = m! \prod_{i=1}^n \frac{b_i^{b_i}}{b_i!} \int_{\overline{\mathcal{M}}_{g;n}} \frac{1 - \lambda_1 + \lambda_2 - \dots \pm \lambda_g}{(1 - b_1\psi_1) \cdots (1 - b_n\psi_n)}. \tag{8}$$

Here $m = 2g - 2 + n + b_1 + \dots + b_n$ and $\overline{\mathcal{M}}_{g;n}$ denotes the moduli space of stable complex curves of genus g with n marked points; ψ_i and λ_j denote certain cohomology classes on these spaces. We do not give their definition, since we are going only to use the fact that $\psi_i \in H^2(\overline{\mathcal{M}}_{g;n})$ for all i and $\lambda_j \in H^{2j}(\overline{\mathcal{M}}_{g;n})$. An immediate corollary of the ELSV formula is the following statement.

Corollary 17. *The simple Hurwitz numbers $h_{m;b_1,\dots,b_n}$ have the form*

$$h_{m;b_1,\dots,b_n} = \prod_{i=1}^n \frac{b_i^{b_i}}{b_i!} P_m(b_1, \dots, b_n),$$

where P_m is a symmetric polynomial of n variables, which is the sum of homogeneous polynomials of degrees between $n + 2g - 3$ and $n + 3g - 2$.

This statement has been conjectured in [10]. The ELSV formula also leads to several explicit formulas for simple Hurwitz numbers in the cases where the necessary intersection indices are known from geometric argument. For example,

Proposition 18. *The connected simple Hurwitz numbers enumerating coverings of the sphere by the torus are*

$$h_{m;b_1,\dots,b_n} = \frac{m!}{24} \prod_{i=1}^n \frac{b_i^{b_i}}{b_i!} \left(e_1^n - \sum_{i=2}^n (j-2)! e_i e_1^{n-i} - e_1^{n-1} \right),$$

where $m = b_1 + \dots + b_n + n$ and e_i, $i = 1, \dots, n$, are the elementary symmetric functions in $b_1, \dots, b_n$, $e_1 = b_1 + \dots + b_n$.

This formula was conjectured in [10] and the first proof, using purely combinatorial tools, was given in [9].

It was indicated in Sec. 4 (see Theorems 9, 10) that certain generating functions for the Hurwitz numbers belong to the algebra $\mathcal{A}$ of power series generated by two functions Y and Z. The only known proof of this fact is based on the properties of the intersection indices of the classes ψ_i and λ_j entering the ELSV formula. Namely, introduce notation

$$\langle \tau_{d_1} \dots \tau_{d_n} \rangle_j = \int_{\overline{\mathcal{M}}_{g;n}} \lambda_j \psi_1^{d_1} \dots \psi_n^{d_n}.$$

Here the genus g is chosen so as to make the degree of the integrand coincide with the dimension of the moduli space $\overline{\mathcal{M}}_{g;n}$. Then the value $\langle \tau_{d_1} \dots \tau_{d_n} \rangle_j$ satisfies the string and the dilaton equation

$$\begin{aligned} \langle \tau_{d_1} \dots \tau_{d_n} \tau_0 \rangle_j &= \langle \tau_{d_1 - 1} \dots \tau_{d_n} \rangle_j + \dots + \langle \tau_{d_1} \dots \tau_{d_n - 1} \rangle_j \text{ (string relation)} \\ \langle \tau_{d_1} \dots \tau_{d_n} \tau_1 \rangle_j &= (2g - 2 + n) \langle \tau_{d_1} \dots \tau_{d_n} \rangle_j \qquad \text{(dilaton relation)} \end{aligned}$$

for each $j = 0, 1, 2, \dots$. The proof of this fact, although not a complicated one, heavily bases on the geometry of the moduli spaces of curves.

8 SHIFTED SYMMETRIC FUNCTIONS AND COMPLETED CYCLES

8.1 *Universal classes*

The center of the group algebra $\mathbb{C}[S_N]$ of the symmetric group S_N is spanned by the classes $C_\lambda(S_N)$, where λ is a partition of N. The class $C_\lambda(S_N)$ is the sum of all permutations with the cyclic type λ. For example, $C_{1^{N-2}2^1}(S_N)$ is the sum of all transpositions in S_N.

It is convenient, however, to introduce certain classes in the centers of group algebras for all symmetric groups simultaneously. Let λ be a partition of an integer n. For an arbitrary integer N, choose n elements out of $\{1, \dots, N\}$ and consider in $\mathbb{C}[S_N]$ the sum of all permutations of these n elements, of cyclic type λ, all the other $N - n$ elements being fixed. Denote by $\widetilde{C}_\lambda$ the element in the center of $\mathbb{C}[S_N]$ which is the sum of all such permutations, for all $\binom{N}{n}$ choices of the n elements out of N. (If $n > N$, then $\widetilde{C}_\lambda = 0 \in \mathbb{C}[S_N]$; if $n = N$, then $\widetilde{C}_\lambda = C_\lambda(S_N)$).

For example, the class $\widetilde{C}_{1^1}$ can be understood as the sum of identity permutations, with a distinguished element in each permutation. In other words, the class $\widetilde{C}_{1^1}$ is the same as the class $N\widetilde{C}_\emptyset = NC_{1^N}(S_N)$. Similarly, the class $\widetilde{C}_{1^2}$ coincides with the class $\frac{N(N-1)}{2}\widetilde{C}_\emptyset$: there are $\binom{N}{2} = \frac{N(N-1)}{2}$ ways to pick two elements in the identity permutation.

The classes $\widetilde{C}_\lambda$ have the following advantage when compared to the classes $C_\lambda(S_N)$: the products of the classes $\widetilde{C}_\lambda$ can be expressed as universal linear combinations of these classes, *which are independent of the order N of the symmetric group*. For example, the equation

$$\widetilde{C}_{2^1}\widetilde{C}_{1^2} = \widetilde{C}_{2^1} + 2\widetilde{C}_{1^1 2^1} + \widetilde{C}_{1^2 2^1}$$

is valid in the center of the group algebra $\mathbb{C}[S_N]$ of any symmetric group S_N, for arbitrary N.

The universality means that there is a natural inclusion of the center of $\mathbb{C}[S_N]$ into that of $\mathbb{C}[S_{N+1}]$ for any N. Tending N to infinity, we obtain a universal center of the group algebra, which can be identified with the infinite dimensional vector space freely spanned by the elements $\widetilde{C}_\lambda$, for arbitrary partitions λ. This space also is endowed with an algebra structure.

This algebra is isomorphic to the algebra Γ of shifted symmetric functions defined in Sec. 5.5. The latter can be considered as the algebra of functions on partitions. As a vector space, it is spanned by the functions f_λ indexed by partitions. By definition, the value of the function f_λ on a partition μ is the value of the character χ_λ on the representation V_μ. The *Frobenius characteristic mapping* $\widetilde{C}_\lambda \mapsto f_\lambda$ establishes an isomorphism between the two algebras.

8.2 *Completed cycles and r-Hurwitz numbers*

Simple Hurwitz numbers count decompositions of a given permutation into a product of transpositions. It is a natural idea to generalize them by replacing transpositions by permutations in other specific classes. For example, why not consider 3-cycles $\widetilde{C}_3$? Besides pure curiosity, these numbers are presumably related to the geometry of moduli spaces of 2-spin structures on algebraic curves (whatever this means). However, such a straightforward approach fails. Namely, enumerative formulas for decompositions of a given permutation in a product of 3-cycles lose elegance, when compared to that for Hurwitz numbers, and their relationship with both mathematical physics and geometry is broken. The same is true for k-cycles for any $k \geq 3$. Fortunately, consistency can be restored by replacing k-cycles $\widetilde{C}_k$ with certain linear combinations of the classes $\widetilde{C}_\lambda$, for certain partitions λ.

Definition 5 ([30]). The *completed r-cycle* $\overline{C}_k$ is the preimage under the Frobenius characteristic map of the kth power function

$$(\mu_1, \mu_2, \dots) \mapsto \frac{1}{k} \sum_{i=1}^{\infty} \left(\left(\mu_i - i + \frac{1}{2} \right)^k - \left(\frac{1}{2} - i \right)^k \right).$$

We have explained the reasons why the kth power function must be of such a form in Sec. 5.5 (we use a normalization differing from that in [30] by a constant).

Let us give formulas for few first completed cycles among which we know that the completed 2-cycle simply coincides with the ordinary 2-cycle:

$$\begin{aligned} \overline{C}_1 &= \widetilde{C}_{1^1} \\ \overline{C}_2 &= \widetilde{C}_{2^1} \\ \overline{C}_3 &= \widetilde{C}_{3^1} + \widetilde{C}_{1^2} + \frac{1}{12} \widetilde{C}_{1^1} \\ \overline{C}_4 &= \widetilde{C}_{4^1} + 2\widetilde{C}_{1^1 2^1} + \frac{5}{4} \widetilde{C}_{2^1}. \end{aligned}$$

These formulas explain the origin of the term "completed cycle": the expansion of a class $\overline{C}_k$ as a linear combination of the classes $\widetilde{C}_\lambda$ starts with the class of the k-cycle $\widetilde{C}_{k^1}$, and then terms of smaller order follow. Explicit formulas for the coefficients on the right of the expressions for all completed cycles can be found in [30].

Now we can define the generalized Hurwitz numbers.

Definition 6. The simple r-Hurwitz number for an integer m and a partition μ is the coefficient of $\widetilde{C}_\mu$ in the mth power of the completed r-cycle,

$$h^{(r)\circ}_{m;\mu} = [\widetilde{C}_\mu](\overline{C}_r)^m.$$

The simple r-Hurwitz numbers are collected into the generating function

$$H^{(r)\circ}(u; p_1, p_2, \dots) = \sum_{m=0}^{\infty} \sum_{\mu} h^{(r)\circ}_{m;\mu} p_{\mu_1} p_{\mu_2} \dots \frac{u^m}{m!},$$

and its logarithm $H^{(r)}(u; p_1, p_2, \dots) = \log H^{(r)\circ}(u; p_1, p_2, \dots)$ is the generating function for connected simple r-Hurwitz numbers.

The definition of the r-Hurwitz numbers and explanation in Sec. 5.5 immediately imply

Theorem 19. *The function $H^{(r)}(u; p_1, p_2, \dots)$ is a one-parameter family of solutions to the KP hierarchy of partial differential equations.*

Indeed, this one-parameter family is induced by the diagonal Lie algebra transformation of the vector space V of Laurent polynomials taking the vector z^k to $\frac{1}{r}\left(k-\frac{1}{2}\right)^r z^k$, $k=\dots,-2,-1,0,1,2,\dots$.

A similar theorem is valid for generating functions defined by any finite linear combination of completed cycles. In this case the eigenvalues $\frac{1}{r}\left(k-\frac{1}{2}\right)^r$ are replaced by an appropriate polynomial in k, which can be arbitrary.

The relationship of r-Hurwitz numbers defined by means of the completed cycles to the geometry of moduli spaces of $(r-1)$-spin structures on algebraic curves is less clear at the moment, and this question is a subject of further investigation.

ACKNOWLEDGEMENTS

S.K. Lando was supported by the following quotes: NWO-RFBR 047.011.2004.026 RFBR 05-01-01012a GIMP ANR-05-BLAN-0029-01 RFBR 08-01-00110-a

REFERENCES

[1] V.I. Arnold, *Topological classification of complex trigonometric polynomials and the combinatorics of graphs with an identical number of vertices and edges*, (Russian) Funktional. Anal. i Prilozhen. **30** (1996), no. 1, 1–17, 96; translation in Funct. Anal. Appl. **30** (1996), no. 1, 1–14.

[2] M. Bousquet-Mélou, G. Schaeffer, *Enumeration of planar constellations*, Adv. in Apl. Math., **24**, 337–368 (2000).

[3] E. Date, M. Kashivara, M. Jimbo, T. Miwa, *Transformation groups for soliton equations*, in: Proc. of RIMS Symposium on Non-Linear Integrable Systems, Singapore, World Science Publ. Co., 39–119 (1983).

[4] P. Deligne, D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. No. **36**, 75–109 (1969).

[5] T. Ekedahl, S.K. Lando, M. Shapiro, A. Vainshtein, *On Hurwitz numbers and Hodge integrals*, C.R. Acad. Sci. Paris Sér I Math., **328**, 1175–1180 (1999).

[6] T. Ekedahl, S.K. Lando, M. Shapiro, A. Vainshtein, *Hurwitz numbers and intersections on moduli spaces of curves*, Invent. Math., **146**, 297–327 (2001).

[7] L. Euler, *De serie Lambertina plurimisque eius insignibus proprietaribus*, Acta academiae scientarum Petropolitanae 1779: II, 1783, 29–51.

[8] I.P. Goulden, D.M. Jackson, *Transitive factorisation into transpositions and holomorphic mappings on the sphere*, Proc. Amer. Math. Soc., **125**, no. 1, 51–60 (1997).

[9] I.P. Goulden, D.M. Jackson, *A proof of a conjecture for the number of ramified coverings of the sphere by the torus*, J. Comb. Theory, Ser. A, **88**, 246–258 (1999).

[10] I.P. Goulden, D.M. Jackson, R. Vakil, *The Gromov–Witten potential of a point, Hurwitz numbers, and Hodge integrals*, Proc. London Math. Soc. (3), **83**, 563–581 (2001).

[11] I.P. Goulden, L.G. Serrano, *A simple recurrence for covers of the sphere with branch points of arbitrary ramification*, Annals of Combinatorics, **10**, 431–441 (2006).

[12] A. Goupil, G. Schaeffer, *Factoring N-Cycles and Counting Maps of Given Genus*, Europ. J. Combinatorics, **19**, 819–834 (1998).

[13] A. Hurwitz, *Über Riemann'sche Flächen mit gegebenen Verzweigungpunkten*, Math. Ann., **39**, 1–61 (1891).

[14] A. Hurwitz, *Über die Anzal der Riemann'sche Flächen mit gegebenen Verzweigungpunkten*, Math. Ann., **55**, 51–60 (1902).

[15] D.M. Jackson, *Counting cycles in permutations by group characters, with an application to a topological problem*, Trans. AMS, **299**, 785–801 (1987).

[16] V. Kac, A. Schwarz, *Geometric interpretation for the partition function of 2D gravity*, Phys. Lett. B, **257**, no. 3–4, 329–334 (1991).

[17] M. Kazarian, *On combinatorial computations of Hurwitz numbers* (*after D. Zvonkine*), preprint (2006).

[18] M. Kazarian, S. Lando, *An algebro-geometric proof of Witten's conjecture*, J. Amer. Math. Soc., **20**, 1079–1089 (2007).

[19] M. Kazarian, S. Lando, *On intersection theory on Hurwitz spaces*, Izv. Ross. Akad. Nauk Ser. Mat., **68**, no. 5, 91–122 (2004); translation in Izv. Math. **68**, no. 5, 935–964 (2004).

[20] S. Kerov, G. Olshanski, *Polynomial functions on the set of Young diagrams*, C. R. Acad. Sci. Paris Sér I Math., **319**, no. 2, 121–126 (1994).

[21] M. Kontsevich, *Intersection theory on the moduli space of curves and the Airy function*, Comm. Math. Phys., **147**, 1–23 (1992).

[22] S.K. Lando, A.K. Zvonkin, *Graphs on surfaces and their applications*, Springer (2004).

[23] S.K. Lando, D. Zvonkine, *On multiplicities of the Lyashko-Looijenga mapping on strata of the discriminant*, Funktsional. Anal. i Prilozhen., **33**, no. 3, 21–34, (1999); translation in Funct. Anal. Appl., **33**, no. 3, 178–188 (1999).

[24] S.K. Lando, D. Zvonkine, *Counting Ramified Coverings and Intersection Theory on Spaces of Rational Functions I (Cohomology of Hurwitz Spaces)*, Moscow Math. J., **7** (1), 85–107 (2007).

[25] A.D. Mednykh, *Nonequivalent coverings of Riemann surfaces with a prescribed ramification type*, Siber. Math. J., **25**, 606–625 (1984).

[26] M. Mirzakhani, *Weil–Petersson volumes and intersection theory on the moduli space of curves*, J. Amer. Math. Soc., **20**, no. 1, 1–23 (2007).

[27] A. Okounkov, *Toda equations for Hurtwitz numbers*, Math. Res. Lett. **7**, no. 4, 447–453 (2000).

[28] A. Okounkov, G. Olshanski, *Shifted Schur functions*, Algebra i Analiz, **9**, no. 2, 73–146 (1997); translation in St.Petersburg Math. J., **9**, no. 2, 239–300 (1998).

[29] A. Okounkov, R. Pandharipande, *Gromov–Witten theory, Hurwitz numbers, and matrix models I*, math.AG/0101147 (2001).

[30] A. Okounkov, R. Pandharipande, *Gromov–Witten theory, Hurwitz theory, and completed cycles*, Ann. of Math. (2), **163**, no. 2, 517–560 (2006).

[31] Okounkov, A.; Pandharipande, R. The equivariant Gromov–Witten theory of P^1. Ann. of Math. (2) 163 (2006), no. 2, 561–605.

[32] R. Pandharipande, *The Toda equations and the Gromov–Witten theory of the Riemann sphere*, Lett. Math. Phys. **53**, no. 1, 59–74 (2000).

[33] B.E. Sagan, *The Symmetric Group*, Springer, 2001.

[34] M. Sato, Y. Sato, *Soliton equations as dynamical systems on infinite dimensional Grassmann manifolds*, in: Nonlinear partial differential equations in applied science, North-Holland, Amsterdam, 259–271 (1983).

[35] G. Segal, G. Wilson, *Loop groups and equations of the KdV type*, Inst. Hautes Études Sci. Publ. Math., no. 61, 5–65 (1985).

[36] B. Shapiro, M. Shapiro, A. Vainshtein, *Ramified coverings of S^2 with one degenerate branching point and enumeration of edge-ordered graphs*, in: Topics in Singularity Theory, Amer. Math. Soc., 219–227 (1997).

[37] K. Ueno, K. Takasaki, *Toda lattice hierarchy*, in: Adv. Studies in Pure Math., **4**, Group representations and Systems of Differential Equations, 1–95 (1984).

[38] E. Witten, *Two-dimensional gravity and intersection theory on moduli spaces*, Surveys in Differential Geometry, vol. 1, 243–269 (1991).

[39] D. Zvonkine, *An algebra of power series arising in the intersection theory of moduli spaces of curves and in the enumeration of ramified coverings of the sphere*, math.AG/0403092 (2004).

[40] D. Zvonkine, *Enumeration of ramified coverings of the sphere and 2-dimensional gravity*, math.AG/0506248 (2005).

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Groups and designs

Huiling Li
Department of Mathematics, Zhejiang University, Hangzhou, Zhejiang, China

ABSTRACT: In this talk we discuss the applications of finite permutation groups to combinatorial designs.
We will divide this talk into the following seven sections:

(1) Definition of $2-(v,k,\lambda)$ designs and examples;
(2) Automorphism groups of designs, elementary properties;
(3) The socle of $Aut(\mathcal{D})$, where $\mathcal{D}$ is a $2-(v,k,1)$ design;
(4) The studies on block transitive $2-(v,k,1)$ designs with k small,
(5) Some works on designs with block transitive and solvable automorphism groups;
(6) Simple groups of Lie type of low rank act on designs;
(7) Classical groups of high dimensions act on designs.

1 DEFINITION OF $2-(v,k,\lambda)$ DESIGNS AND EXAMPLES

Definition 1.1. *Let v,k,λ,t be integers such that $v>k>\lambda$. Let $\mathcal{P}$ be a set with v points, $\mathcal{B}$ be a collection of some k-subsets (called blocks) of $\mathcal{P}$. If every subsets of $\mathcal{P}$ with t points lies in exactly λ blocks, then the system $\mathcal{D}=(\mathcal{P},\mathcal{B})$ is called a $t-(v,k,\lambda)$ design.*

We give some examples.

Example 1.2. Let $\mathcal{P}=\{1,2,3,4,5,6,7\}$, $\mathcal{B}=\{B_1,B_2,\ldots,B_7\}$, where

$$B_1=\{1,2,4\},\quad B_2=\{2,3,5\},\quad B_3=\{3,4,6\},\quad B_4=\{4,5,7\},$$
$$B_5=\{5,6,1\},\quad B_6=\{6,7,2\},\quad B_7=\{7,1,3\}.$$

Then $(\mathcal{P},\mathcal{B})$ is a $2-(7,3,1)$ design.

Example 1.3 Projective Plane. Let V be a n-dimensional vector space over the field $GF(q)$, where $n\geq 3$. We regard the 1-dimensional subspaces as *points* of $\mathcal{P}$, and the 2-dimensional subspaces as *blocks* of $\mathcal{B}$, then $(\mathcal{P},\mathcal{B})$ is a $2-(q^2+q+1,q+1,1)$ design.

Clearly, Example 1.2 is an instance of Example 1.3, where $n=3$ and $q=2$.

Example 1.4 Affine Geometrie. Let $n\geq 2$ be an integer and V be a n-dimensional vector space over the field $GF(q)$. We regard the vectors of V as *points,* and the cosets of 1-dimensional subspaces as *blocks,* then we obtain a $2-(q^2,q,1)$ design.

Example 1.5 Netto system $N(q)$**.** Let q be a prime with $q \equiv 7(12)$.

Take the field $F = GF(q)$. Suppose that ϵ is a fixed primitive sixth root of unity in F and $A\Gamma L^2(1,q)$ is the group of all permutations of F of the form $x \to a^2x + b$, where $a, b \in F$ and $a \neq 0$.

Let F be the *point set,* and the set of images of the triple $\{0, 1, \epsilon\}$ under the action of $A\Gamma L^2(1,q)$ be *block set* $\mathcal{B}$. Then we get a $2-(q,3,1)$ design $(F,\mathcal{B})$.

Example 1.6 Witt-Bose-Shrikhande system. Take the group $G = SL(2,2^n)$ where $n \geq 3$. We define:

(i) The subgroups of G isomorphic to the dihedral group of order $2(2^n+1)$ are the *points*
(ii) The involutions of G are the *blocks.*
(iii) We say a point x is in a block B if the involution B is an element of the subgroup x. Then we obtain a $2-(2^{n-1}(2^n+1), 2^{n-1}, 1)$ design.

Example 1.7 Hermite Unital. The Hermite unital of order q is defined in a projective plane $PG_2(q^2)$. Let q be a prime power, then the field $GF(q^2)$ has an automorphism σ of order 2. Let V be a 3- dimensional vector space, then the 1-dimensional subgroups of V are the "points" of $PG_2(q^2)$, and the 2-dimensional subspaces are "lines". Use $[x,y,z]$ to represent the "point" which is generated by a vector (x,y,z) as a 1-dimensional subspace of V, where $(x,y,z) \neq (0,0,0)$, and $<a,b,c>$ represents the line consisting of all points $[x,y,z]$ which satisfy the condition $ax+by+cz=0$. We say a point $[x,y,z]$ or a line $<x,y,z>$ is *absolute* if $xx^\sigma + yy^\sigma + zz^\sigma = 0$.

Then the set $\mathcal{P}$ of all absolute points and the set $\mathcal{B}$ of all non-absolute lines constitute a $2-(q^3+1, q+1, 1)$ design, that is the Hermite unital of order q. (See [21])

Example 1.8 Ree Unital. Let $q = 3^{2n+1}$, and $G = {}^2G_2(q)$. we define:

- The points of the Ree unital of order q are the Sylow 3-subgroups of G, and
- The blocks are the involutions.
- A point is in a block if the involution normalizes the Sylow 3-subgroup.

Then we obtain a $2-(q^3+1, q+1, 1)$ design.

Note that some people call $2-(v,k,1)$ designs *finite linear spaces.*

Definition 1.9. *A finite linear space is an incidence structure consisting of a finite set of points* $\mathcal{P}$ *and a set of lines* $\mathcal{L}$ *in the power set of* $\mathcal{P}$ *such that any two points are incident with exactly one line.*

A linear space is called non-trivial if every line contains at least three points and there at least two points.

A linear space is called regular if all line are incident with the same number of points.

Thus $2-(v,k,1)$ *designs are just regular linear spaces.*

2 ELEMENTARY PROPERTIES

Suppose we are given a $t-(v,k,\lambda)$ design $\mathcal{D}$ and there are b blocks in $\mathcal{D}$.

Proposition 2.1.

(1) *b is determined by the parameters* t, v, k, λ*. Indeed,*

$$b = \lambda \frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)},$$

(2) *Every* $t-(v,k,\lambda)$ *design is also a* $(t-1)-(v,k,\lambda_0)$ *design, where*

$$\lambda_0 = \lambda\left(\frac{v-t+1}{k-t+1}\right).$$

(3) *Every point is in exactly r blocks, where*

$$r = \lambda\frac{(v-1)\cdots(v-t+1)}{(k-1)\cdots(k-t+1)}.$$

Proposition 2.2 (Fisher's inequality).

$$b \geq v.$$

3 AUTOMORPHISM GROUPS OF DESIGNS, ELEMENTARY PROPERTIES

Definition 3.1. *Let* $\mathcal{D} = (\mathcal{P},\mathcal{B})$ *be a* $t-(v,k,\lambda)$ *design,*
π *be a permutation of* $\mathcal{P}$.
If π *sends every block into a block, then* π *is called an automorphism of* $\mathcal{D}$.
The set of all automorphisms of $\mathcal{D}$ *forms a group, the automorphism group of* $\mathcal{D}$ *and denoted by* $Aut(\mathcal{D})$.

Definition 3.2. *Let* $G \leq Aut(\mathcal{D})$.
If G is transitive on the set $\mathcal{P}$*, then G is said to be point transitive.*
If G is primitive on set $\mathcal{P}$ *then G is said to be point primitive.*
If $Aut(\mathcal{D})$ *is point transitive (point primitive), then* $\mathcal{D}$ *is said to be point transitive (point primitive, respectively).*

By the definition of automorphisms every automorphism of $\mathcal{D}$ induces a permutation of set $\mathcal{B}$.

Definition 3.3. *Let* $G \leq Aut(\mathcal{D})$.
If G is transitive on the set $\mathcal{B}$, *then we say that G is block transitive.*
If G is primitive on the set $\mathcal{B}$, *then G is block primitive.*
If $Aut(\mathcal{D})$ *is block transitive (block primitive), then* $\mathcal{D}$ *is said to be block transitive (block primitive, respectively).*

Definition 3.4. *Let* $\mathcal{D} = (\mathcal{P},\mathcal{B})$ *is a* $t-(v,k,\lambda)$ *design, a pair* (p,B) *is called a flag, if* $p \in \mathcal{P}$, $B \in \mathcal{B}$ *and* $p \in B$.

If $G \leq Aut(\mathcal{D})$ is transitive on the set of flags, then G is *flag transitive.*
We have the following implications.

Theorem 3.5 (Block [1]). *Let* $\mathcal{D}$ *be a* $2-(v,k,1)$ *design. If* $G \leq Aut(\mathcal{D})$ *is block transitive, then G is point transitive.*

Theorem 3.6 (Higman and McLaughlin [20]). *Let* $\mathcal{D}$ *be a* $2-(v,k,1)$ *design. If* $G \leq Aut(\mathcal{D})$ *is flag transitive, then G is point primitive.*

We don't know whether the block primitivity implies the point primitivity. Instead we have a conjecture:

Conjecture A (Doyen and Delandtsheer). *Let $\mathcal{D}$ be a $2-(v,k,1)$ design. If $G \leq Aut(\mathcal{D})$ is block primitive, then G is point primitive.*

Several papers have been published on this conjecture:

Delandtsheer ([12]) proved that if $k < 30$, then this conjecture holds,

W. Liu proved that if $k \leq 40$, then the conjecture holds.

In [15] and [38] this conjecture is studied. We introduce the following parameters:

$$k_1 = (k,v), \quad k_2 = (k, v-1), \quad b_1 = (b,v), \quad b_2 = (b, v-1).$$

Then it is clear that

$$v = k_1 b_1, \quad r = k_2 b_2, \quad k = k_1 k_2, \quad b = b_1 b_2.$$

We observe that if G is block transitive and Φ is an orbit of G on the set of flags, then the size of Φ is a common multiple of b and v, namely $b_1 b_2 k_1 \| \Phi |$.

Thus we have the following Lemma:

Lemma 4.1. *For any block B, k_1 is a divisor of the size of any orbit of G_B on the points of B.*

From this we know that if $k_2 = 1$, that is $k|v$, then the all points in B form an orbit of G_B and so G is flag transitive. Thus we get an easy proof of the well-known theorem of Camina and Gagen [8]:

Theorem 4.2. *If G is block transitive and $k|v$, then G is flag transitive.*

This theorem obtained a series of generalizations:

Fang and Li proved (See [15]) that if $k_2 \leq 4$, then block transitivity implies flag transitivity,

Liu and Li (See [38]) showed that if $k_2 \leq 10$, this implication is also true.

Recently, Zhou and Ma proved that it is true when $k_2 \leq 12$.

Now we describe the idea of these works.

Let G be a block transitive automorphism group of a $2-(v,k,1)$ design $\mathcal{D} = (\mathcal{P}, B)$. We regard G as a permutation group on the point set $\mathcal{P}$. Let $P(B)^{(2)} = \{(\alpha,\beta)|\alpha \neq \beta \in B\}$. Then G_B acts on it. Let $\psi_1, \psi_2, \ldots, \psi_t$ be the orbits of G_B on it. Also we let $\Psi_1, \Psi_2, \ldots, \Psi_{r-1}$ be orbits of G in the set $\{(\alpha,\beta)|\alpha \neq \beta \in \mathcal{P}\}$. Then the map $\rho : \psi_i \to \Psi_j$ where $\psi_i \subseteq \Psi_j$ is a bijection from $\{\psi_1, \psi_2, \ldots, \psi_t\}$ to $\{\Psi_1, \Psi_2, \ldots, \Psi_{r-1}\}$. Thus $t = r-1$, and so we may assume that $\rho : \psi_i \to \Psi_i$. If $(\alpha,\beta) \in \psi_i \subseteq \Psi_i$, then $|\Psi_i| = |G : G_{\alpha,\beta}| = |G : G_B||G_B : G_{\alpha,\beta}| = b|\psi_i|$. If Δ is a G_α-orbit containing β, then $v|\Delta| = |\Psi_i| = b|\psi_i|$ and so $k_1|\Delta| = b_2|\psi_i|$. From this we have that $|\Delta| \equiv 0(mod\ b_2)$.

Lemma 4.3. *Let $\psi_1, \ldots, \psi_t$ be the orbits of G_B on the set $P(B)^{(2)}$ and $\Psi_1, \ldots, \Psi_s$ be the orbits of G on the set $\mathcal{P}^{(2)}$. Then:*

(1) **(See also H. Li [25])** *The map ρ which maps ψ_i to Ψ_j if $\psi_i \subseteq \Psi_j$ is bijective;*
(2) *Every subdegree is a multiple of b_2;*

Now let G be imprimitive on $\mathcal{P}$. Let $\mathcal{P} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \cdots \cup \mathcal{C}_c$, where $\mathcal{C}_i's$ are the imprimitivity blocks of G, and $|\mathcal{C}_i| = s$. Thus $v = sc$. Let $\alpha \in \mathcal{C}_1$. Since every suborbit has length a multiple of b_2, $c \equiv 1(mod\ \ b_2)$. Since $v \equiv 1(mod\ \ b_2)$, we know that $c \equiv 1(mod\ \ b_2)$.

Now suppose that $s = 1 + xb_2, c = 1 + yb_2$. Recall that $b_2 = (k, r)$. We have the following Lemma:

Lemma 4.4. *Suppose that G is imprimitive on $\mathcal{P}$ and $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_c\}$ is a complete set of imprimitivity blocks, and $s = 1 + xb_2$ and $c = 1 + yb_2$. Then we have:*

(1) *$xy < k_2^2$;*
(2) *Both $\frac{1}{2}xb_2$ and $\frac{1}{2}yb_2$ are integers;*
(3) *There are integers n, m such that*

$$s = \frac{\binom{k}{2} - n}{m}, \qquad c = \frac{\binom{k}{2} - m}{n}.$$

Proof.

(1) Since $v = sc = (1+xb_2)(1+yb_2) = 1+(x+y+xyb_2)b_2$ and $v-1 = r(k-1) = k_2b_2(k-1)$, we have $x + y + xyb_2 = k_2(k-1)$. Thus

$$xyb_2 < k_2(k-1),$$

and so

$$xyr < k_2^2(k-1) < k_2^2k.$$

But $r \geq k$, thus we obtain that $xy < k_2^2$.

(2) A pair of points $\{\alpha, \beta\}$ is said to be inner if α, β are in the same imprimitivity block. Since G is block transitive, every block possesses the same number of inner pairs. Suppose this number is n. Then we have $bn = \frac{v(s-1)}{2}$, or $n = \frac{xk_1}{2}$, which is an integer. Also, since

$$x + y + xyb_2 = k_2(k-1),$$

we have

$$1 + yb_2 = \frac{k(k-1) - yk_1}{xk_1}.$$

Since both xk_1 and $k(k-1)$ are even integers, so is yk_1. Hence $m = \frac{yk_2}{2}$ is an integer.

(3) Use the notation as above, we know that

$$c = 1 + yb_2 = \frac{\binom{k}{2} - m}{n}.$$

Also, since

$$x + y + xyb_2 = k_2(k-1),$$

we have

$$1 + xb_2 = \frac{k_2(k-1) - x}{y} = \frac{\binom{k}{2} - m}{n}.$$

Lemma 4.5. *The integer k_1 divides $(k_2+x)(k_2+y)$.*

Proof. We know that

$$v = \frac{k_2(k-1)-x}{y} \times \frac{k_2(k-1)-y}{x} = \frac{(k_2k-(k_2+x))(k_2k-(k_2+y))}{xy}.$$

So

$$vxy = (k_2k-(k_2+x))(k_2K-(k_2+y)).$$

But we know that $k_1|v$ and $k_1|k$, thus $k_1|(k_2+x)(k_2+y)$.

Thus if k_2 is given, we can use the following procedure to determine a series of integers $(x,y,k_1,k,n,m,s,c,v,b_2)$. In Step 1, we determine all possible values for x,y such that $xy < k_2^2$. Then, in next steps we determine other parameters. If for some values of (x,y) we can not find an integral value for n,m (in step 4) or s,c (in step 6), we will stop with these $x,y,k,\ldots$, take an other values for x,y and determine values for other parameters.

Step 1. Choose integers x,y such that $xy < k_2^2$;
Step 2. Choose integer k_1, such that $k_1|(k_2+x)(k_2+y)$ and $(k_1,k_2)=1$;
Step 3. Let $k = k_1k_2$, and $k \geq 3$;
Step 4. Calculate $n = \frac{xk_1}{2}$ and $m = \frac{yk_1}{2}$. If one of them is not an integer, then we droop $x,y,k_1,\ldots$ we just get; If they are all integers, we do the next step;
Step 5. Let

$$s = \frac{\binom{k}{2}-n}{m}, \qquad c = \frac{\binom{k}{2}-m}{n}.$$

If one of them is not integer, we stop and take other x,y and turn to (2);
Step 6. Let $v = sc$;
Step 7. Calculate $b_2 = \frac{s-1}{x}$ and $b_2 = \frac{c-1}{y}$;
Step 8. Let $b_1 = \frac{v}{k_1}$.

The following is the result of above procedure for $k_2 = 3$;

	x	y	k_1	k	n	m	s	c	v	b_2
Case 1	1	1	16	48	8	8	140	140	19600	139
Case 2	1	2	20	60	10	20	88	175	15400	87
Case 3	2	1	20	60	20	10	175	88	15400	87
Case 4	1	5	16	46	8	40	28	136	3808	27
Case 5	5	1	16	48	40	8	136	28	3808	27

By using the permutation group theory we can show that there is no permutation group having the parameters listed in the above table, and so we know that there is no a $2-(v,k,1)$ design with an automorphism group G which is block transitive, point imprimitive and for which $k_2 = 3$.

5 CLASSIFICATION OF DOUBLY TRANSITIVE DESIGNS

Kantor (1985) classified the designs with automorphism groups which are doubly transitive on the point sets. See [23]

Theorem 5.1. *Let $\mathcal{D}$ is a design with $\lambda = 1$ admitting an automorphism group 2-transitive on points. Then $\mathcal{D}$ is one of the following designs:*

(i) $PG(d,q)$;
(ii) $AG(d,q)$;
(iii) *Ree Unital;*
(iv) *One of two affine planes having* 3^4 *or* 3^6 *points, or*
(v) *One of designs having* $v = 3^6$ *and* $k = 3^2$.

6 CLASSIFICATION OF FLAG TRANSITIVE DESIGNS

In 1990, a team of six mathematicians completes a classification of flag transitive designs:

Theorem 6.1 [4]. *Suppose that G is a flag transitive group of automorphisms of the non-trivial linear space $\mathcal{S}$, then either*

1. $(\mathcal{S}, G)$ *is in one of the following cases:*
   (a) $\mathcal{S} = PG(d,q)$ *and* $PSL(d+1,q) \leq G \leq P\Gamma L(d+1,q)$*;*
   (b) $\mathcal{S}$ *is the Hermitean unital* $U_H(q)$ *and* $PSU(3,q) \leq G \leq P\Gamma U(3,q)$;
   (c) $\mathcal{S}$ *is the Ree unital of order* $q = 3^{2n+1}$ *and* ${}^2G_2(q) \leq G \leq Aut({}^2G_2(g))$;
   (d) $\mathcal{S}$ *is the Witt-Bose-Shrikhande Design associate with* $PSL(2,q)$ *where* $q = 2^n$ *with* $n \geq 3$, *and* $PSL(2,q) \leq G \leq P\Gamma L(2,q)$;
   (e) $\mathcal{S}$ *is a Desarguesian Affine Space and* $G_0 \leq \Gamma L(d,q)$*;*
   (f) $\mathcal{S}$ *is a non-Desarguesian Affine Space:* $\mathcal{S}$ *is an affine plane of order* q^2, *where* $q = 2^{2n+1}$ *with* $n \geq 1$ *and* ${}^2B_2(q) \geq G_0 \geq AUT({}^2B_2(q))$; $\mathcal{S}$ *is the Hering plane of order 27 and* $G_0 = SL(2,13)$ *or* $\mathcal{S}$ *is the nearfield plane of order 9;*
   (g) $\mathcal{S}$ *is one of two flag transitive linear spaces on* 3^9 *points withlines of size* 3^2. *or*
2. $\mathcal{S}$ *has* $q = p^s$ *points (p prime) and G is a subgroup of the group* $A\Gamma L(1,q)$ *of one-dimensional semilinear affine transformations.*

For the proof, see [13], [24], and [46].

7 THE SOCLES OF $Aut(\mathcal{D})$, WHERE $\mathcal{D}$ IS A $2-(v,k,1)$ DESIGN

After classification of flag transitive designs, the next important task is to classify all line transitive designs.

Camina proved the following theorem [5]:

Theorem 7.1. *Let G be a line-transitive, point-primitive automorphism group of a linear space $\mathcal{S}$. Then the socle of G is either elementary Abelian or simple.*

Then Camina and Praeger proved: [10]

Theorem 7.2. *Let G be a line-transitive, point-quasiprimitive automorphism group of a linear space $\mathcal{S}$. Then the socle of G is either elementary Abelian or simple.*

Here the quasiprimitivity is a concept suggested by C. Praeger.

A transitive permutation group G on a set Ω is called quasiprimitive if each nontrivial normal subgroup of G is transitive on Ω.

Thus a line transitive group $G \leq Aut(\mathcal{S})$ acts on the point set $\mathcal{P}$ in the following three form:

(1) G has a minimal normal subgroup acting intransitively on $\mathcal{P}$;
(2) G has an elementary Abelian normal subgroup acting on $\mathcal{P}$ regularly;
(3) G is almost simple.

Now most works published are on the groups in (3).

Perhaps this is because of the classification of finite simple groups.

Generally in case (3) we are given a linear space $\mathcal{S}$ and a group $G \leq Aut(\mathcal{S})$, such that $T \trianglelefteq G \leq Aut(T)$ where T is a finite simple group.

We face the following four possibilities:

(i) $G = T$ is primitive on $\mathcal{P}$.
(ii) $G = T$ is transitive but not primitive on $\mathcal{P}$.
(iii) $G \neq T$ and G is primitive on $\mathcal{P}$.
(iv) $G \neq T$ and G is transitive but not primitive on $\mathcal{P}$.

Of course, among these cases, (i) is the easiest to handle and (iv) the hardest.

8 THE STUDIES ON BLOCK TRANSITIVE $2-(v,k,1)$ DESIGNS WITH k SMALL

Here, $3 \leq k \leq 10$, say.

Results: For some small k, people determined all block transitive $2-(v,k,1)$ designs.

For $k = 4$: G is solvable: Camina and Siemons [7].
G is unsolvable: H. Li [25].
For $k = 5$: G is solvable: W. Tong and H. Li, [48];
G is unsolvable: G. Hang and H. Li [18].
For $k = 6, 7, 8$: G is solvable, Liu, [34, 35].
G is unsolvable: G. Han (for exceptional simple groups of Lie type, submitted.)

Method: For small k, one can easily list all permutation groups of degree k, transitive and intransitive.

Thus we know the possible structures of the group $G_B{}^B$, the group induced by G_B on the set of points of B.

Then we know the possible *rank* and possible *subdegrees* of the group G by Lemma 2.2.

By using this information, sometimes we can determine these designs.

Now we determine all block transitive $2-(v,3,1)$ designs. Let $\mathcal{D}$ be a $2-(v,3,1)$ design, then $b = \frac{v(v-1)}{6}$, $r = \frac{v-1}{2}$ and $\mathcal{D}$ has other parameters $k_1, k_2, \ldots$. Let $G \leq Aut(\mathcal{D})$. From the structures of G^B we can determine the rank, subdegrees of G. We list these as the following table:

Case	G^B	*rank of G*	*Subdegrees of G*	*Remark*
1	$\langle 1 \rangle$	7	$1, b_2, b_2, b_2, b_2, b_2, b_2$	$\|G\|$ *is odd*
2	$\langle (12) \rangle$	4	$1, 2b_2, 2b_2, 2b_2$	
3	$\langle (123) \rangle$	3	$1, 3b_2, 3b_2$	$\|G\|$ *is odd*
4	S_4	2	$1, 6b_2$	

In Cases 1 and 3, G is solvable since its order is odd. We can easily see that G is primitive on $\mathcal{P}$. Thus $v = p^c$ for some prime p and integer c. Since $|G|$ is odd, b_2 is odd and so $v \equiv 7(mod\ 12)$. Therefore $p \equiv 7(mod\ 12)$ and c is odd. If $c = 1$, then $G \leq AGL(1, v)$. If $c \geq 3$, then the maximum primitive divisor of $p^c - 1$ divides b_2. Thus by Hering's result we have $G \leq AGL(1, v)$.

Thus in Case 1, G is the semi direct product of Z_{p^c} by $Z_{\frac{p^c-1}{6}}$.

In Case 3, $G = AGL^2(1,p^c)$, that is, G consists of all maps $\rho : x \to ax+b$, where $a, b \in GF(p^c)$ with $a \neq 0$ being a square. Let $B = \{0, 1, \epsilon\}$ be the block of $\mathcal{D}$ containing 0 and 1. We have an element $\sigma : x \to ax + b$ of order 3 in G_B. Suppose it sends 0 to 1, sends 1 to ϵ and sends ϵ to 0. Then we have that $b = 1, a = \epsilon - 1$ and $0 = \epsilon^2 - \epsilon + 1$. This means that ϵ is a sixth root of unity. We conclude that $\mathcal{D}$ is a Netto system.

Case 2 does not occur. This can be seen by Theorem 2 of Camina and Siemons [7], which saying that if $G \leq Aut(\mathcal{D})$ is block transitive and every element in G^B fixes at most one point of B, then $|G|$ is odd or G is flag transitive on $\mathcal{D}$.

In Case 4, G is doubly transitive. From Kantor's result, we know that $\mathcal{D} = PG(d, 2)$ *or* $AG(d, 3)$.

We also use the following properties:

Lemma 8.1. *Let $\mathcal{S}$ be a $2-(v,k,1)$ design and g is an automorphism of $\mathcal{S}$. If f is the number of fixed points of g in $\mathcal{P}$, then $f \leq r + k - 3$.*

Lemma 8.2. *Let G be a block transitive automorphism group of a $2-(v,k,1)$ design. Let B be a block and H a subgroup of G_B. Assume that H satisfies the following two conditions:*

(i) *$|FixH \cap B| \geq 2$, and*
(ii) *If $K \leq G_B$ and $|FixK \cap B| \geq 2$ and K is conjugate to H in G then H is conjugate to K in G_B. Then either (a) $FixH \subseteq B$, or (b) the induced structure in FixH is a $2-(v_0,k_0,1)$ design, where $v_0 = |FixH| k_0 = |FixH \cap B|$. Further, $N_G(H)$ acts as a block transitive group on this design.*

These lemmas appeared in Camina and Siemons [7]. These are very useful properties.

9 SOME WORKS ON DESIGNS WITH BLOCK TRANSITIVE AND SOLVABLE AUTOMORPHISM GROUPS

Let me mention some papers on block transitive and solvable groups:

Theorem 9.1 (H. Li and W. Liu [27]). *Let $k \geq 3$ be a fixed positive integer and $(\mathcal{S}, G)$ be a pair, where $\mathcal{S}$ is a $2-(v,k,1)$ design and G be a group of automorphism group of $\mathcal{S}$ such that G is solvable and block transitive. If $v > (k^{\frac{3}{4}} + 1)^{\varphi(k(k-1))}$, then v is a prime power and G is flag transitive or $G \leq A\Gamma L(1, v)$.*

Thus for a fixed integer k, in order to list all possible $2-(v,k,1)$ designs with solvable and block transitive automorphism groups, we need to consider three cases:

(1) G is flag transitive;
(2) $G \leq A\Gamma L(1, v)$; and
(3) the "exceptional" case.

Even if we know what the group G is, the structure of $\mathcal{S}$ still is unknown. In this case computer calculation is needed.

The proof of Theorem 5.1 is based on the results of Hering on solvable linear groups (See [19]).

Let p be a prime and n, t be integers. We say that t is a primitive divisor of $p^n - 1$ if $t|p^n - 1$ but t does not divide $p^k - 1$ for all $k < n$. It is known that $p^n - 1$ always possesses a primitive divisor unless $n = 1$ and $p = 2, n = 2$ and $p + 1 = 2^s$ for some s, and $p = 2$ and $n = 6$.

Now we use $\Phi_n(x)$ to denote the nth cyclotomic polynomial, $\Phi_n(p)$ is its value at a prime p. We set $\Phi_n^*(p) = \Phi_n(p)/f^\alpha$ where $f = (n, \Phi_n(p))$ and α satisfies that $f^\alpha | \Phi_n(p)$ but $f^{\alpha+1}$ does not divide $\Phi_n(p)$. The $\Phi_n^*(p)$ is the maximum primitive divisor of $p^n - 1$. Hering proved that: Let U be a solvable subgroup of $GL(n,p)$, $r|(|U|, \Phi_n^*(p))$, and $R \neq 1$ be an r-subgroup of U. If $R \trianglelefteq U$, then $U \leq \Gamma L(1, p^n)$. If U is not normal in U, then U has a normal subgroup N such that $N = TZ(N)$

where T is an extra-special group of order 2^{2a+1}, and $r = n + 1 = 2^a + 1$ for some $a \geq 1$, $Z(N)$ is a cyclic group of order 2 or 4 and $T \cap Z(N) = Z(T), N \leq S$, where S is the closure of R in U, and $Z(N) \leq C_U(T) = Z(U)$. Note if we let V be a vector space over $GF(b)$ and U acts on it, then R irreducibly acts on V.

The sketch of the proof of Theorem 9.1
Suppose $G \leq Aut(\mathcal{D})$ is block transitive and solvable and $v > (k^{\frac{3}{4}} + 1)^{\varphi(k(k-1))}$.

(1) We can easily show that $v > \left(\left(\begin{smallmatrix} k \\ 2 \end{smallmatrix}\right) - 1\right)^2$. Then by Lemma 2.3,3, G is primitive on $\mathcal{P}$. Thus we may assume that $v = p^n$, where p is a prime and n an integer, and G has a normal subgroup which is elementary and regular on the point set $\mathcal{P}$. We identity this normal group with $\mathcal{P}$, thus we view $\mathcal{P}$ as a vector space over $GF(p)$. Let G_0 be the stabilizer in G of zero vector.

In the following we suppose that p is odd and $n \geq 6$, and prove that the theorem holds in this case. For other cases we can prove the theorem in the same way.

We will show that some primitive divisor of $p^n - 1$ will divide b_2. Recall that $v - 1 = k_2 b_2 (k-1)$.

(2) Suppose $n > \phi(k_2)$ and $n > \phi(k-1)$. Then any prime divisor s of $k_2(k-1)$ satisfies $p^{\phi(k_2)} \equiv 1(mod\ s)$ and $p^{\phi(k-1)} \equiv 1(mod\ s)$. In other words, $s | p^{\phi(k_2)} - 1$ and $s | p^{\phi(k-1)} - 1$. Hence s is not a primitive divisor of $p^n - 1$. But $p^n - 1$ does have a primitive divisor r and so $r | b_2$.

(3) Now suppose that $n \leq \phi(k_2)$ and $n \leq \phi(k-1)$. Then $n < \phi(k_2(k-1))$. Take the least integer d satisfying $p^d \equiv 1(mod\ \ k_2), p^d \equiv 1(mod\ \ k-1)$. Then, since $p^n - 1 \equiv 1(mod\ k_2)$ and $p^n - 1 \equiv 1(mod\ \ k-1)$, we must have $d | n$. If $d < n$, then all prime divisors of $k_2(k-1)$ are not primitive divisors of $p^n - 1$. Thus b_2 has a prime divisor which is a primitive divisor of $p^n - 1$.

(4) If $d = n$. Then $n | \phi(k_2(k-1))$. Suppose that f is the greatest prime divisor of n. Then $f | \phi(k_2)$ or $f | \phi(k-1)$. So $f < k$ and we have

$$\Phi_n^*(p) = \Phi_n(p)/f \geq \Phi_n(p)/k \geq (p-1)^{\phi(n)}/k \geq (p-1)^4/k$$

$$\geq (k^{\frac{3}{4}})^4/k = k^3/k = k^2 > k(k-1)$$

In particular, $\Phi_n^*(p) > k_2(k-1)$. So $\Phi_n^*(p)$ does not divide $k_2(k-1)$. Thus b_2 has a primitive divisor of $p^n - 1$.

(5) Thus there is a primitive prime divisor r of $p^n - 1$, such that $r | b_2$. Since G is block transitive r is a divisor of the order of G. t $\mathcal{P}$. Thus we can regard $\mathcal{P}$ as a subgroup of G and also as a vector space over the field $GF(p)$. Let R be a Sylow subgroup of G_0. If R is normal in G_o, then $U \leq GL(1,p^n)$ and so $G \leq A\Gamma L(1,p^n)$. If R is not a normal subgroup of G_0, then by Hering's result, we know that G_0 has element of order 2 which sends every vector to its negative. In this case G is flag transitive on $\mathcal{D}$ by Lemma 5 of [7].

10 SIMPLE GROUPS OF LIE TYPE OF LOW RANK ACT ON DESIGNS

Results: Some works is about the case where the socle of G is a simple group T of Lie type of low rank. We list some of them

$A_1(q)$: W. Liu [33];
${}^2B_2(q)$: W. Liu,H. Li and C. Ma, [40]
${}^2G_2(q)$: W. Liu, [41], S. Zhou [49, 51]
$PSU(3,q)$: W. Liu [31]
$PSL(3,q)$: N. Gill [16]
$G_2(q)$: W. Liu [36, 37];

${}^3D_4(q)$: W. Liu [30, 32, 43]
${}^2F_4(q)$: S. Zhou [50].

For each of these simple groups, people have a list of its maximal subgroups. Thus we have some knowledge of all primitive permutation representations of these simple groups. If we suppose the group G is one of these simple groups and suppose that G acts primitively on the set $\mathcal{P}$, then from this knowledge we can sometimes easily determine the pair $(\mathcal{S}, G)$ or disprove its existence. If we just assume the socle is one of them or that G acts transitively on $\mathcal{P}$ new ideas are needed. But the problem in some cases is hard and in some cases is not.

As an example we give the sketch of the proof of the following theorem.(See [40])

Theorem 10.1. *Let $\mathcal{D}$ be a $2-(v,k,1)$ design and $G \le Aut(\mathcal{D})$ be block primitive, then the socle of G is not isomorphic to $Sz(q)$.*

First, we list some properties of $Sz(q)$.

Let $q = 2^{2m+1}$. Then $Sz(q)$ is defined as a subgroup of $GL(4,q)$. The order of $Sz(q)$ is $q^2(q^2+1)$ $(q-1)$, and $Sz(q)$ are the only finite simple groups whose orders are prime to 3.

Let $G = Sz(q)$. G has the following subgroups:

- Let F be a Sylow 2-subgroup of G. F has order q^2, has exponent 4, and $F' = Z(F)$. $Z(F)$ has order q and is elementary Abelian. All involutions of F are in $Z(F)$. The normalizer $N_G(F) = FH$ of F is a semi-direct product of F by a cyclic subgroup H of order $q-1$, and H acts regularly on the set of all involutions of F.
- The normalizer $N_G(H)$ of H is a semi-direct product of H by a cyclic subgroup of order 2.
- G has a cyclic subgroup A_1 of order $q + 2t + 1$, where $t = 2^m$. The normalizer $N_G(A_1)$ is a semi-direct product of A_1 by a cyclic subgroup of order 4.
- G has a cyclic subgroup A_2 of order $q - 2t + 1$, where $t = 2^m$. The normalizer $N_G(A_2)$ is a semi-direct product of A_2 by a cyclic subgroup of order 4.
- If q_0 is a power of 2 such that $q = {q_0}^s$ for some s, then G has subgroups isomorphic to $Sz(q_0)$.

The maximal subgroups of G are all determined. Let $Sz(q_0)$ denotes a fixed subgroup of G where $q = q_0^s$ with s a prime. Then $N_G(F), N_G(H), N_G(A_1), N_G(A_2)$ and $Sz(q_0)$ and their all conjugates are the maximal subgroups of G.

From this list of maximal subgroups of G we know that if p is an odd prime, then a Sylow p-subgroup S of G is cyclic and its normalizer is conjugate to one of $N_G(H), N_G(A_1), N_G(A_2)$.

Now suppose $\mathcal{D}$ is a $2-(c,k,1)$ design, $G \le Aut(\mathcal{D})$ is block primitive. Let the socle T of G is isomorphic to $Sz(q)$. We prove the theorem in several steps:

Step 1. We may assume that $G \simeq Sz(q)$.
Since G is block primitive, G_B is maximal. Then T transitively acts on $\mathcal{P}$. Since $G_B \cap T$ is maximal in T, T primitively acts on $\mathcal{P}$. Thus T satisfies all hypothesis of the Theorem. In the following we assume that $G \simeq Sz(q)$.

Step 2. We can show that G_α is conjugate to one of $N_G(H), N_G(A_1), N_G(A_2)$ or $N_G(F)$.
By Kantor's result we know that $\mathcal{D}$ is not a projective plane. Thus there is a prime p (a significant prime) such that $p|b$ but $(p,v) = 1$. Let S be a Sylow subgroup of G_α, then S is also a Sylow subgroup of G and α is its only fixed point. Thus $N_G(S) \le G_\alpha$. Hence by the subgroup structure of $Sz(q)$ we know that G_α is conjugate to one of $N_G(H), N_G(A_1), N_G(A_2)$ and $N_G(F)$.

Step 3. G_α is not conjugate to $N_G(F)$.
If G_α is conjugate to $N_G(F)$, then G doubly transitively acts on $\mathcal{P}$. By Kantor'r result, we know this is impossible. From this we know that v is even.

Step 4. We calculate the possible number of fixed points in $\mathcal{P}$ of an involution of G.
Let z be a fixed involution in G and let N be the number of fixed points of z on $\mathcal{P}$. We consider the set of pairs (i,α) where i is an involution, α is a point in $\mathcal{P}$ and $i \in G_\alpha$.

By using two methods to determine the number of the size of the set of such pairs, we have

$$e(G)N = |\mathcal{P}| \cdot e(G_\alpha),$$

where $e(G)$ and $e(G_\alpha)$ are the numbers of involutions in G and in G_α, respectively. So

$$N = \frac{|G\!:\!G_\alpha| \cdot e(G_\alpha)}{e(G)}.$$

But $e(G) = (q^2 + 1)(q - 1)$, thus

$$N = \frac{q^2 \cdot e(G_\alpha)}{|G_\alpha|}.$$

From this we know that, if $G_\alpha \simeq N_G(H)$, then $N = q^2/2$; if $G_\alpha \simeq N_G(A_1)$ or $G_\alpha \simeq N_G(A_2)$, then $N = q^2/4$.

Step 5. In any one maximal subgroup of G, all involutions are conjugate to each other.
In $N_G(H), N_G(A_1)$ or $N_G(A_2)$, the Sylow 2-subgroups are cyclic, so the conclusion is obvious. Since H acts regularly on the set of involutions of F, any two involutions of F are conjugate in F. If the maximal subgroup is $Sz(q_0)$ for some q_0, the conclusion is also obvious.

Step 6. The final contradiction.
Let z be an involution in F, then $z \in G_B$ for some B. Let $Q = \langle z \rangle$, then Q satisfies all conditions of Lemma 4.2. Hence by Lemma 4.2, either (a) $FixQ \subseteq B$, or (b) $FixQ$ has a structure of a $2-(v_0, k_0, 1)$ design $\mathcal{D}_0$, where $v_0 = |FixQ|$ and $k_0 = |FixQ \cap B|$. Moreover, $N_G(Q)$ is block transitive on $\mathcal{D}_0$.
If (b) occurs, then $v_0 = q^2/2$ or $q^2/4$, and so v_0 is a power of 2. Let $\mathcal{D}_0$ has b_0 blocks, since $N_G(Q) = F$ is block transitive on $\mathcal{D}_0$ we have $b_0 \big| |F| = q^2$. From this we know that $v_0 | b_0$, thus b_0/v_0 is a power of 2. But since $b_0 | v_0(v_0 - 1)$, b_0/v_0 is odd. Thus we must have that $b_0 = v_0$, that is $\mathcal{D}_0$ is a projective plane. But since v_0 is even, this is impossible.
Now suppose that (a) occurs, then $FixQ \subseteq B$. Since v is even, k is also even. Thus if a block B_1 of $\mathcal{D}$ is fixed by z then $B_1 \cap FixQ = \emptyset$, and so z has $k/2$ orbits of lenght 2 on B_1. Hence $\mathcal{P} - B$ is a disjoint union of some blocks B' fixed by z and $B' \neq B$. Thus we know that $|\mathcal{P} - B| = v - k$ is a multiple of k, and so $k|v$. By Camina's theorem $\mathcal{D}$ is flag transitive. But by the classification of flag transitive designs, this is impossible.

11 CLASSICAL GROUPS OF HIGH DIMENSIONS ACT ON DESIGNS

In 2003, Camina, Neumann and Praeger published a paper [6], in which they proved the following result:

Theorem 11.1. *Suppose that $T \trianglelefteq G \leq Aut(T)$, where $T = Alt(n)$ and $n \geq 5$. If G acts as a line-transitive automorphism group of a non-trivial linear space $\mathcal{S}$ then $\mathcal{S} = PG_1(3,2)$ and $G = Alt(7)$ or $G = Alt(8)$.*

This is a surprising result for us.

Recently, another paper was submitted, in which a theorem on the case where G is a large dimensional classical group is proved. This theorem resolves the problem of classification of the pairs $(\mathcal{S}, G)$ where G is a large dimensional classical groups, that is, as groups of Lie type, the rank of G are high. In Section 6 we saw a series results on groups of Lie type with low rank. Thus we need results on groups with middle rank, that is on the classical groups of middle dimension and simple exceptional groups of Lie type, such as $E_8(q), E_7(q)$ and so on.

To finish this talk I would like to mention two theorems:

Theorem 11.2 (Gill [17]). *Suppose that a group G has socle a group of Lie type of characteristic p. Suppose furthermore that g acts transitively upon the lines of a linear space $\mathcal{S}$ with significant prime p. Then G acts flag transitively on $\mathcal{S}$ and we have one of the following examples:*

- $U_3(q) \leq G \leq P\Gamma U(3,q)$ and $\mathcal{S}$ is a Hermitean unital;
- ${}^2G_2(q) \leq G \leq Aut({}^2G_2(q))$ and $\mathcal{S}$ is a Ree unital.

Theorem 11.3 (H. Li and Y. Liu [31]). *Let $\mathcal{S}$ be a $2-(v,k,1)$ design and $G \leq Aut(\mathcal{S})$ be block transitive. If G is a simple group of Lie type and the point stabilizers are maximal parabolic subgroups, then G is flag transitive. If G is classical, then the conclusion is also true provided the point stabilizers are parabolic.*

These theorem work to all groups of Lie type, no matter what are the rank of them.

REFERENCES

[1] R.E. Block, On the orbits of collineation groups, *Math. Z.*, **96**(1967), 33–49.

[2] H, D.R. Hughes and F.S. Piper, *Projective Planes*, Springer-Verlag, Berlin Heidelberg New York, 1973.

[3] N. Bourbaki, *Groupes et algebres de Lie*, Hermann, Paris, 1968. Chapters IV, V and VI.

[4] F. Buekenhout, A. Delandtsheer, J. Doyen, P. Kleidman, M.W. Liebeck and J. Saxl, Linear spaces with flag transitive automorphism groups, *Geom. Dedicata*, **36**(1990), 89–94.

[5] A. Camina, The socle of automorphism groups of linear spaces, *Bull. London Math. Soc.*, (3) **28**(1996), 269–272.

[6] A. Camina, P.M. Neumann and C. Praeger, Alternating groups acting on finite linear spaces, *Proc. London Math. Soc.*, **87**(2003), 29–53.

[7] A. Camina and J. Siemons, Block transitive automorphism groups of $2-(v,k,1)$ block designs, *J. Comb. Theory, Series A*, **51**(1989), 268–276.

[8] A. Camina and T.M. Gagen, Block transitive automorphism groups of designs, *J. of Algebra*, **86**(1984), 549–554.

[9] A. Camina and C. Praeger, Line-transitive automorphism groups of linear spaces, *Bull. London Math. Soc.*, **25**(1993), 309–313.

[10] A. Camina and C. Praeger, Line-transitive, point-quasiprimitive automorphism groups of finite linear spaces are affine or almost simple, *Aequationes Math.*, **61**(2001), 221–232.

[11] R.W. Carter, *Simple groups of Lie type*, Wiley-Interscience, New York, 1972.

[12] A. Delandtsheer, Line-transitive automorphism groups of finite linear spaces, *European J. Combin.*, **10**(1989), 161–169.

[13] A. Delandtsheer, Finite flag-transitive linear spaces with alternating socle, in "Algebraic Cmbinatorics and Applications (Gösseseinstein,1999)" (A. Betten et al Ed.) Lecture Notes in Computer Sciences and Engineering, pp. 79–88. Springer-Verlag, Berlin, 2001.

[14] A. Delandtsheer, J. Doyen, J. Siemons and C. Tamburini, Doubly transitive $2-(v,k,1)$ designs, *J. of Comb. Theory, Series A*, **43**(1986) 140–145.

[15] W. Fang and H. Li, A generalization of the Camina-Gagen theorem (in Chinese), *J. of Math.* (Wuhan), **12**(1991), 437–442.

[16] N. Gill, *PSL*$(3,q)$ and line transitive linear spaces, *Beitragen zur Algebra and Geometries*, To appear.

[17] N. Gill, Linear spaces with significant characteristic prime, *Innovations in Incidence Geometry*, **10**(2006), 109–118.

[18] G. Han and H. Li, Unsolvable block transitive automorphiam groups of $2-(v,k,1)$ designs, *J. Comb. Theory, Series A*, **114**(2007), 77–96.

[19] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, *Geom. Dedicata*, **2**(1974), 425–460.

[20] D.G. Higman and J.E. McLaughlin, Geometric ABA-groups, *Illinois J. Math.*, **5**(1969), 74–84.

[21] D.R. Hughes and F.C. Piper, *Design Theory* Cambridge University Press, 1985.

[22] W.M. Kantor, Primitive permutation groups of odd degree and an application to finite projective planes, *J. Algebra,* **106**(1987), 15–45.

[23] W.M. Kantor, Homogeneous designs and geometric lattices, *J. Comb. Theory, Series A*, **38**(1985), 66–74.

[24] P. Kleidman, The classification of finite linear spaces with flag-transitive automorphism groups of affine type, *J. Comb. theory, Series A*, **84**(1998), 196–235.

[25] H. Li, On block-transitive $2-(v,4,1)$ designs, *J. Comb. Theory, Series A,* **69**(1995), 115–124.

[26] H. Li and Y. Liu, Automorphism groups of linear spaces and parabolic subgroups, I, II, Submitted to *J. Comb. Theory, A.*

[27] H. Li and and W. Liu, Solvable block transitive automorphism groups of $2-(v,k,1)$ designs, *J. Comb. Theory, Series A,* **93**(2001), 182–191.

[28] H. Li and and W. Liu, Line-primitive $2-(v,k,1)$ designs with $\frac{k}{(k,v)} \leq 10$, *J. Comb. Theory, Series A,* **93**(2001), 153–167.

[29] Martin W. Liebeck, On the orders of maximal subroups of the finite classical groups, *Proc. London Math. Soc.*, **50**(1985), 426–446.

[30] W. Liu, Simple groups of Lie type ${}^3D_4(q)$ and $2-(v,k,1)$ designs, *Science in China (New Series),* **32**(2003), 526–536.

[31] W. Liu, Finite linear spaces admitting a projective group $PSU(3,q)$ with q even, *Linear Alg. and its Appl.,* **374**(2003), 291–309.

[32] W. Liu, Steinberg triality groups acting on $2-(v,k,1)$ designs, *Science in China (Series A)*, **46**(2003), 872–883.

[33] W. Liu, Finite linear spaces admitting a two dimensional projective linear space, *J. Comb.Theory, Series A.* **103**(2003), 209–222.

[34] W. Liu, Solvable block transitive automorphism groups of $2-(v,6,1)$ designs, *Acta Math. Sinica*, **43**(2000), 157–162.

[35] W. Liu, Solvable block transitive automorphism groups of $2-(v,7,1)$ designs, *Advances in Math. (China)*, **30**(2001), 55–62.

[36] W. Liu, The Chevalley groups $G_2(q)$ with q odd and $2-(v,k,1)$ designs, *Europ. J. Comb.*, **24**(2003), 331–346.

[37] W. Liu, The Chevalley groups $G_2(2^n)$ and $2-(v,k,1)$ designs, *Algebra Coll.*, **8**(2001), 471–480.

[38] W. Liu and H. Li, A generalization of the Camina-Gagen theorem (in Chinese) II, *Adv. of Math.* (Beijing), **25**(1996), 438–444.

[39] W. Liu and H. Li, Solvable block-transitive automorphism groups of finite $2-(v,k,1)$ designs, *J. Comb. Theory, Series A,* **44**(2001), 182–191.

[40] W. Liu, H. Li and C. Ma, Suzuki Groups and $2-(v,k,1)$ designs, *Europ. J. Combinatorics*, **22**(2001), 513–519.

[41] W. Liu, S. Li and L. Gong, Almost simple groups with socle $Re(q)$ acting on finite linear spaces, *Europ. J. Comb.,* **27**(2006), 788–800.

[42] W. Liu and J. Li, Finite projective planes admitting a projective linear group $PSL(2,q)$, *Linear Algebra and Its Appl.,* **413**(2006), 121–130.

[43] W. Liu, S. Dai and L. Gong, Almost simple groups with socle ${}^3D_4(q)$ acting on finite linear spaces *Science in China* **49**(2006), 1768–1776.

[44] W. Liu, H. Li and S. Zhou, Suzuki groups and $2-(v,k,1)$ designs, *Europ. J. Comb.*, **22**(2001), 513–519.

[45] C. Praeger and S. Zhou, Classification of line transitive point imprimitive linear spaces with line size at most 12, To appear in *Codes and Chryptography.*

[46] J. Saxl, On finite linear spaces with almost simple flag transitive automorphism groups, *J. of Comb. Theory, Series A*, **100**(2002), 302–343.

[47] H. Wielandt, *Finite Permutation Groups*, Acadmic Press, New York, 1964.

[48] W. Tong and H. Li, Solvable block transitive automorphism groups of $2-(v,5,1)$ designs, *Discrete Math.*, **260**(2003), 267–273.

[49] S. Zhou, Block primitive $2-(v,k,1)$ designs admitting a Ree group of characteristic two, *Designs, Codes and Crypt.*, **36**(2005), 159–169.

[50] S. Zhou and H. Li, The Ree Groups ${}^2F_4(q)$ and $2-(v,k,1)$ designs, *Ann, Math.*, **23A**(2002), 713–722.

[51] S. Zhou , Ree groups ${}^2G_2(q)$ and $2-(v,k,1)$ block designs (II), *Acta Math. Sinica,* **46**(2003), 824–928.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Injectivity radius of triangle group representations, with application to regular embeddings of hypermaps

Martin Mačaj
Comenius University, Bratislava, Slovakia

Jozef Širáň
Open University, UK, and STU, Bratislava, Slovakia

Mária Ipolyiová
M. Bel University, Banská Bystrica, Slovakia

ABSTRACT: We survey the algebraic background for constructing representations of triangle groups in linear groups over algebras arising from quotients of multivariate polynomial rings, leading to improvements of upper bounds on the order of epimorphic images of triangle group with a given injectivity radius and to bounds on the size of the associated hypermaps with a given planar width.

1 INTRODUCTION

Let (l, m, n) be a *hyperbolic* triple of positive integers, that is, $1/l + 1/m + 1/n < 1$. With such a triple we associate a face-3-coloured trivalent tessellation $U(l, m, n)$ of the hyperbolic plane $\mathcal{H}$, which can be described as follows. Faces of $U(l, m, n)$ coloured 1, 2, and 3 are congruent $2l$-gons, $2m$-gons, and $2n$-gons, respectively, and each vertex is incident to precisely one face of each colour. The underlying trivalent 1-complex of $U(l, m, n)$ is a bipartite graph with bi-partition induced by the clockwise cyclic order of colours of the incident faces (1, 2, 3 or 1, 3, 2).

The group of orientation- and face-colour-preserving hyperbolic isometries of the tessellation $U(l, m, n)$ is isomorphic to the well-known (hyperbolic) *triangle group* presented in the form

$$T(l, m, n) = \langle r, s, t \mid r^m = s^n = t^l = rst = 1 \rangle \tag{1}$$

where r, s, and t represent clockwise hyperbolic rotations about centres of three mutually adjacent $2l$-, $2m$-, and $2n$-gons of $U(l, m, n)$ by the angles of π/l, π/m, and π/n, respectively.

Any epimorphism $\varphi : T(l, m, n) \to H$ onto a finite group H with a torsion-free kernel N determines a finite, face-3-coloured quotient *hypermap* $\mathcal{M} = U(l, m, n)/N$ of type (l, m, n) in the compact, orientable surface $\mathcal{S} = \mathcal{H}/N$, with H acting on $\mathcal{M}$ as colour and orientation preserving automorphism group. Due to the regular action of H on vertices of $\mathcal{M}$ in the same bi-partition class, the hypermap $\mathcal{M}$ is called *regular*.

Hypermaps and regular hypermaps can, of course, be defined in a purely combinatorial way. We will not go into such details, however, since all finite, regular hypermaps on compact, orientable surfaces can be obtained by the above construction [7]. In the special case when $l = 2$ one usually considers a different cell-complex representation, obtained from the hypermap by contracting faces coloured 2 to single points and quadrangles coloured 1 to single edges. This results in a *regular embedding* of a graph, or, simply, a *regular map*. Regular action of H on vertices of one colour class of the original hypermap then transforms into a regular action on arcs of the embedded graph. For surveys on regular maps we recommend [12, 15].

The point of departure of our research is looking at the regular quotient hypermap $\mathcal{M} = U(l,m,n)/N$ as an object arising from a fundamental region F in $\mathcal{H}$ associated with the normal subgroup N by identifying sides of the boundary polygon of F according to a certain side-pairing. The interior of F may then be viewed as a region in which the restriction of the covering projection $U(l,m,n) \to \mathcal{M} = U(l,m,n)/N$ is injective. In this situation it is natural to speak about a certain 'radius of injectivity', introduced by means of either the covering projection and hyperbolic distance in F, or non-contractible closed curves in $\mathcal{M}$, or else combinatorics of words in $T(l,m,n)$ relative to the epimorphism φ. We focus on the third option, with mentioning the second in passing as well.

We are now in position to present our main concepts. In the triangle group $T(l,m,n)$ presented as in (1), for any $w \in T(l,m,n)$ such that $w \neq 1$ we let $\ell(w)$ denote the smallest length of a word in $\{r,r^{-1},s,s^{-1},t,t^{-1}\}$ that represents w in $T(l,m,n)$. We define the *injectivity radius* of the epimorphism $\varphi : T(l,m,n) \to H$ to be the largest k such that $\varphi(w) \neq 1$ for all non-identity $w \in T(l,m,n)$ such that $\ell(w) \leq k$.

The 'non-contractible curves' counterpart to this definition is as follows. Let K be the 1-skeleton of the hypermap $\mathcal{M} = U(l,m,n)/N$ and let $\mathcal{S}$ be the supporting surface of $\mathcal{M}$. The *planar width* of $\mathcal{M}$ is the least number of intersections $|\mathcal{C} \cap K|$ taken over all non-contractible closed curves $\mathcal{C}$ on $\mathcal{S}$.

Relations between the two parameters can be obtained by extending the analysis of [16]. Letting $\mu = \max\{l,m,n\}$, for any positive integer d the following holds:

If φ is an epimorphism from $T(l,m,n)$ onto a finite group with torsion-free kernel N and of injectivity radius at least $d\mu/2$, then the planar width of the hypermap $\mathcal{M} = U(l,m,n)/N$ is larger than d. Conversely, if the planar width of $\mathcal{M}$ is larger than d, then the injectivity radius of φ is at least d.

The aim of this paper is to acquaint the reader with the algebraic background developed recently in [8] and applied to constructions of relatively small finite groups onto which there is an epimorphism from a triangle group with a given injectivity radius. We will do so without going into numerous (and often non-trivial) technical details. In the course of explanation we will also review techniques used in earlier attempts [1, 4, 16].

The paper is organized as follows. In Section 2 we outline the strategy for constructions of epimorphic images of triangle groups by means of congruence subgroups. The strategy consists in choosing an appropriate faithful representation of a triangle group in a linear group over a polynomial ring, and then in selecting an appropriate ideal for factorization. The theory for the faithful representation part will be reviewed in Section 3. To have the injectivity radius and the order of the quotient group under control in this strategy, in Section 4 we develop a way to 'measure' ideals, leading to our main results regarding bounds on the order of finite groups admitting an epimorphism from a triangle group with a given injectivity radius. The final Section 5 is devoted to applications of the results to planar width of regular hypermaps.

2 EPIMORPHISMS OF LARGE INJECTIVITY RADIUS ONTO 'SMALL' FINITE GROUPS AND CONGRUENCE SUBGROUPS

The fact that for every hyperbolic triple (l,m,n) there exist torsion-free epimorphisms with arbitrarily large injectivity radius from $T(l,m,n)$ into finite groups is equivalent to residual finiteness of hyperbolic triangle groups, as was pointed out in [16]. The residual finiteness result itself follows from a general theorem of [9] on matrix groups, and also from the specific approach in [10] which we will present later. Nevertheless, explicit bounds on the smallest order of a finite group H for which there exists an epimorphism $T(l,m,n) \to H$ of injectivity radius at least δ appear not to have been considered until recently [16].

The counting argument of [11] related to the radii of certain subconfigurations in hyperbolic tessellations can be used to show that for every epimorphism of injectivity radius at least δ from a hyperbolic triangle group $T(l,m,n)$ onto a finite group H we have $|H| > c^{\delta}$ where c depends on l, m, n but not on δ. With regard to the upper bounds on $|H|$ this shows that the best one can hope for are estimates of the form $|H| < C^{\delta}$ where, again, C may depend on l, m, n but not on δ.

The main idea of constructing epimorphisms giving such an upper bound on $|H|$ has roots in [9] and consists in looking at *congruence subgroups*, that is, normal subgroups determined by certain congruences (ideals), and at the corresponding factor groups. To place this idea into a general setting, let $\mathbb{R}$ be a ring of algebraic integers over an algebraic number field and let G be a subgroup of the general linear group $GL(q, \mathbb{R})$ for some $q \geq 2$. A subgroup K of G is called *congruence subgroup* if there exists a non-zero ideal I of $\mathbb{R}$ such that the group $G \cap \ker(GL(q, \mathbb{R}) \rightarrow GL(q, \mathbb{R}/I))$ is contained in K. Note that such a K necessarily has a finite index in G.

Even at this level of generality it is not true that every finite hyperbolic regular hypermap can be obtained from a congruence subgroup for a fixed $\mathbb{R}$ and q. Namely [14], by non-trivial group theory, $GL(q, \mathbb{R}/I)$ is always an extension of a soluble finite group by a direct product of a finite number of groups of type $GL(r, p^{t})$ where t is bounded from above by a constant, and it is known that such a group cannot contain symmetric groups of arbitrarily large degree. In the category of maps, concrete examples of regular maps that do not arise from congruence subgroups are described in [5].

Nevertheless, we will see that the congruence subgroup approach indeed leads to bounds of type $|H| < C^{\delta}$ discussed above. The principle is best explained by using the language of algebras. Let A be a u-dimensional abelian $\mathbb{Z}$-algebra, i.e., an abelian ring with unity such that the additive group of A is a u-dimensional free $\mathbb{Z}$-module with bilinear multiplication. Let $B = \{\beta_1, \dots, \beta_u\}$ be an additive basis of A, which means that every element $\alpha \in A$ can be uniquely expressed in the form $\alpha = a_1\beta_1 + \cdots + a_u\beta_u$, where $a_i \in \mathbb{Z}$ for $1 \leq i \leq u$. The integer $\langle\alpha\rangle = \max_i |a_i|$ is the *integral norm* of α relative to the basis B. We extend the integral norm in the obvious way (keeping the notation) also to vectors and matrices over A. We may now formulate the result of [8] whose early version was first outlined in [16] and which appears to underpin all the existing work on injectivity radius [1, 4, 8, 16].

Theorem 1. *Let A be a u-dimensional abelian $\mathbb{Z}$-algebra. Let ϑ: $T(l, m, n) \rightarrow \mathrm{SL}(q, A)$ be a faithful representation of the triangle group $T(l, m, n) = \langle r, s, t | r^m = s^n = t^l = rst = 1\rangle$ and let $\Gamma = \{\vartheta(r)^{\pm 1}, \vartheta(s)^{\pm 1}, \vartheta(t)^{\pm 1}\}$. Further, let $\lambda = \max_{X \in \Gamma}\langle X\rangle$ where the norm is with respect to a fixed basis of A containing* 1 *and let $\kappa = \max\{\langle X\alpha\rangle / \langle\alpha\rangle;\ \alpha \in A^q \setminus \{0\},\ X \in \Gamma\}$. Assume that there is a positive integer δ and a prime p such that $\kappa^{\delta-1}\lambda + 1 < p < \kappa^{\delta}$. If ψ_p is the natural projection* $\mathrm{SL}(q, A) \rightarrow \mathrm{SL}(q, A/pA)$, *then the representation $\psi_p\vartheta$ has injectivity radius at least δ and* $|\mathrm{Im}(\psi_p\vartheta)| < C^{\delta}$ *where* $C = \kappa^{(q^2-1)u}$.

Motivation for this result goes back about a decade in connection with attempts to bound the number of vertices of a regular map of planar width larger than a preassigned integer d; we briefly review the results. In [13] the authors presented a construction of regular maps of hyperbolic type $(2, m, n)$ and arbitrary planar width, leading to no explicit upper bound on the number of vertices. With the help of faithful representations of triangle groups in orthogonal groups over rings of algebraic integers, an upper bound of the form $\tilde{C}(2, m, n)^d$ for the smallest number of vertices of a regular map of hyperbolic type $(2, m, n)$ with planar width larger than d was given in [16]. Exploring the same method in more detail, improvements resulting in smaller order of magnitude of the functions $\tilde{C}(2, m, n)$ and, in general, $\tilde{C}(l, m, n)$, were subsequently obtained for regular maps [4] and regular hypermaps [1]. The contribution of [1, 4] relied on exploring representations over factor rings of multivariate polynomials and a more accurate evaluation of the bounds at the expense of compactness of the resulting formulas. Very recently, a novel approach to deriving various types of estimates on $\tilde{C}(l, m, n)$ has been developed in [8], yielding asymptotically much better results. We will revisit these sources later in our article. At this point, note that while for the constant $c = c(l, m, n)$ appearing in the lower bound $|H| > c^{\delta}$ derived from Moran's work [11] we have $\sqrt{lmn} < c(l, m, n)$, one of the best results of [8] only gives $\log_2 \tilde{C}(l, m, n) < 64\ lmn \log_2(4\mu)$, where $\mu = \max\{l, m, n\}$. This motivates a further search for narrowing down the (still) huge gap between the existing lower and upper bounds.

3 FAITHFUL REPRESENTATIONS OF TRIANGLE GROUPS IN LINEAR GROUPS OVER POLYNOMIAL RINGS

Recall [7] that any hyperbolic triangle group $T(l, m, n)$ acts on the universal tessellation $U(l, m, n)$ as the group of orientation-preserving *isometries* of the hyperbolic plane, leaving $U(l, m, n)$ invariant and preserving face colours. This viewpoint leads to a useful matrix representation of $T(l, m, n)$. Let $\xi = 2\cos(\pi/l)$, $\eta = 2\cos(\pi/m)$, and $\zeta = 2\cos(\pi/n)$; these quantities are algebraic integers over $\mathbb{Z}$. Under a suitable coordinate system in the hyperbolic plane the generators r, s, and t of $T(l, m, n)$ in (1) can then be represented [10] by the 3×3 matrices R, S, and T, respectively, of the form

$$R = \begin{pmatrix} \eta^2 - 1 & 0 & \eta \\ \zeta + \xi\eta & 1 & \xi \\ -\eta & 0 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} -1 & -\zeta & 0 \\ \zeta & \zeta^2 - 1 & 0 \\ \eta & \xi + \eta\zeta & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & \zeta & \eta + \zeta\xi \\ 0 & -1 & -\xi \\ 0 & \xi & \xi^2 - 1 \end{pmatrix}. \tag{2}$$

The group $\langle R, S, T\rangle = \langle R, S\rangle$ is a subgroup of the orthogonal group $O(3, \mathbb{R})$ with respect to a suitable quadratic form [10]. As usual in representation theory, the hard part is to prove that the assignment $r \mapsto R$, $s \mapsto S$, and $t \mapsto T$ indeed extends to a *faithful* representation, that is, to an *injective* homomorphism, from $T(l, m, n)$ to $O(3, \mathbb{R})$. This was done in [10] by an implicit usage of properties of hyperbolic tessellations. Another two proofs of faithfulness of this representation, both invoking canonical bilinear forms of reflection groups, were given in [2] (with the original idea due to Tits [17]) and in [3].

As outlined in the general strategy, a natural way to arrive at finite groups admitting an epimorphism from a triangle group with a given injectivity radius is to regard the image of the above representation of $T(l, m, n)$ as a subgroup of $O(3, \mathbb{Z}[\xi, \eta, \zeta])$ and factorize the ring $\mathbb{Z}[\xi, \eta, \zeta]$ by a suitable ideal. This translates into looking for certain congruence subgroups of $\mathbb{Z}[\xi, \eta, \zeta]$ and was first considered in [16]. We defer the problem of choosing ideals to the next section and concentrate here on matrix groups (over various algebraic rings) that admit faithful representations of triangle groups.

Consider first the rings themselves. Let k be the least common multiple of l, m, n and let $k = l'l = m'm = n'n$. Also, let $\theta = 2\cos(\pi/k)$, let $f_\theta(x) \in \mathbb{Z}[x]$ be the minimal polynomial for θ, and let $P_j(x)$ be the j-th modified Tchebyshev polynomial. Then, the ring $\mathbb{Z}[\xi, \eta, \zeta]$ used in the representation above is naturally embedded in the ring $\mathbb{Z}[\theta] \cong \mathbb{Z}[x]/(f_\theta(x))$ and $\xi = P_{l'}(\theta)$, $\eta = P_{m'}(\theta)$, and $\zeta = P_{n'}(\theta)$.

In a first set of subsequent modifications considered in [1, 4], the ring $\mathbb{Z}[\theta]$ was replaced with $\mathbb{Z}[x, y, z]/J$ where the ideal $J = (f(x), g(y), h(z))$ was chosen so that the substitution $\xi \mapsto x + J$, $\eta \mapsto y + J$, and $\zeta \mapsto z + J$ in (2), gives a faithful representation of $T(l, m, n)$.

More substantial improvements in [8] have been based on representing ξ, η and ζ as sums of an element and its reciprocal, which in turn was motivated by spectra of R, S and T. We will explain the method on two types of rings: in $\mathbb{Z}[x]/(\Phi_{2k}(x))$ where k is as above and $\Phi_{2k}(x)$ is the $2k$-th cyclotomic polynomial, and in $\mathbb{Z}[x, y, z]/(f(x), g(y), h(z))$ where $f(x) = (x^{2l} - 1)/(x^2 - 1)$, $g(y) = (y^{2m} - 1)/(y^2 - 1)$ and $h(z) = (z^{2n} - 1)/(z^2 - 1)$.

From now on we will assume that R, S, and T are matrices as in (2), but with ξ, η and ζ taken from more general structures (rings or fields) that will be specified in the course of explanations. With this convention in mind one can show [8] that in the two types of rings introduced above we still have faithful representations of triangle groups. In both cases we assume that (l, m, n) is a hyperbolic triple.

Proposition 1. *Let $k = \text{l.c.m.}(l,m,n) = l'l = m'm = n'n$. Let $f(x) \in \mathbb{Z}[x]$ be a monic reciprocal polynomial of even degree. Let R, S, and T be matrices as in* (2) *defined over the ring $\mathbb{Q}[x]/(f(x))$, where $\xi = x^{l'} + x^{-l'} + (f(x))$, $\eta = x^{m'} + x^{-m'} + (f(x))$, and $\zeta = x^{n'} + x^{-n'} + (f(x))$. If the $2k$-th cyclotomic polynomial divides $f(x)$ and if $f(x)$ divides $(x^{2k}-1)/\text{l.c.m.}(x^{2l'}-1, x^{2m'}-1, x^{2n'}-1)$, then the assignment $r \mapsto R$, $s \mapsto S$ and $t \mapsto T$ extends to a faithful representation of the triangle group $T(l,m,n)$ in $SL(3, \mathbb{Q}[x]/(f(x)))$.*

Proposition 2. *Let $J = (f(x), g(y), h(z))$ be an ideal in $\mathbb{Q}[x,y,z]$ where $f(x) \in \mathbb{Z}[x]$, $g(y) \in \mathbb{Z}[y]$, and $h(z) \in \mathbb{Z}[z]$ are monic reciprocal polynomials of even degree. Let R, S, and T be matrices as in* (2) *defined over the ring $\mathbb{Q}[x,y,z]/J$, where $\xi = x + x^{-1} + J$, $\eta = y + y^{-1} + J$, and $\zeta = z + z^{-1} + J$. Assume that $\Phi_{2l}(x) | f(x)$ and $f(x) | (x^{2l}-1)/(x^2-1)$, $\Phi_{2m}(y) | g(y)$ and $g(y) | (y^{2m}-1)/(y^2-1)$, and $\Phi_{2n}(z) | h(z)$ and $h(z) | (z^{2n}-1)/(z^2-1)$. Then, the assignment $r \mapsto R$, $s \mapsto S$ and $t \mapsto T$ extends to a faithful representation of the triangle group $T(l,m,n)$ in $SL(3, \mathbb{Q}[x,y,z]/J)$.*

4 BOUNDING THE ORDERS OF FINITE TARGET GROUPS FOR EPIMORPHISMS OF LARGE INJECTIVITY RADIUS

As indicated in Section 2, upper bounds on the order $|H|$ of finite groups H for which there is an epimorphism $T(l,m,n) \to H$ of injectivity radius at least δ were initially derived from factor rings associated with minimal polynomials of algebraic integers of type $2\cos \pi/j$, with bases for the integral norm being formed by powers of such algebraic integers. The first such estimate from [16] was of the form $|H| < C^{\delta}$ where $\log_2(C) < 72(mn)^3$. The best construction improvement obtained by the same technique [1] give $|H| < C^{\delta}$ with $\log_2 C < 9(l^2 + m^2 + n^2)lmn$. For $l = 2$ the best result of the same type [4] is $|H| < C^{\delta}$ with $\log_2 C < 2(\phi(2m)^2 + \phi(2n)^2)\phi(2m)\phi(2n)$, where ϕ is the Euler function.

With the help of the two faithful representations of hyperbolic triangle groups introduced earlier, substantial improvement of these constructions have been obtained in [8] by applying Theorem 1 to the $\mathbb{Z}$-algebras used in Propositions 1 and 2. This requires establishing estimates on integral norms with respect to bases that are more sophisticated than the ones used previously. We now describe a basis that was successfully used in [8]. Consider a monic, reciprocal polynomial $f(x) = x^{2u} + c_1x^{2u-1} + \cdots + c_{u-1}x^{u+1} + c_ux^u + c_{u-1}x^{u-1} + \cdots + c_1x + 1 \in \mathbb{Z}[x]$ of even degree $2u$. Because f is reciprocal, elements of the form $x + x^{-1} + (f(x))$ are well defined in the ring $\mathbb{Z}[x]/(f(x))$. Define $\theta = x + x^{-1} + (f(x))$ and $\theta_i = x^i + x^{-i} + (f(x))$ for any $i \in \mathbb{Z}$; in particular, $\theta_0 = 2$ and $\theta_1 = \theta$. Then, the set $B = \{1, \theta_1, \theta_2, \ldots, \theta_{u-1}\}$ is a basis of the $\mathbb{Z}$-algebra $\mathbb{Z}[\theta]$. For the associated norm we will write $\langle f \rangle$ instead of $\langle f(x) \rangle = \max_i |c_i|$, and $\langle g \rangle$ instead of $\langle g(\theta) \rangle$ for elements $g(\theta) \in \mathbb{Z}[\theta]$.

Quite remarkably, the effect of the change of basis is enormous. The point is that the new basis allows for obtaining much better estimates on the parameters κ, λ, and C introduced in Theorem 1. Leaving numerous technical details aside (such as the fact that $\langle X\alpha \rangle \le \kappa \langle \alpha \rangle$ implies $\langle X^j\alpha \rangle \le \kappa^j \langle \alpha \rangle$ which is used throughout), application of the faithful representation in Proposition 1 in conjunction with Theorem 1 gives the following [8]:

Theorem 2. *Let (l,m,n) be a hyperbolic triple, let $k = \text{l.c.m.}(l,m,n) = l'l = m'm = n'n$, and let $\mu = \max\{l', m', n'\}$. Let $f(x)$ be the $2k$-th cyclotomic polynomial and let $\langle f \rangle$ be the largest absolute value of its coefficients. Then, for every positive integer δ there exists an epimorphism $\varphi : T(l,m,n) \to H$ onto a finite group H of injectivity radius at least δ such that $|H| \le C^{\delta}$ where $C \le (3 + \langle f \rangle)^{8\mu\phi(2k)}$.*

A look at the first few values might suggest the false impression that coefficients of the k-th cyclotomic polynomial are always small compared to its degree. However, in [18] it was proved that the natural logarithm of the norm of the k-th cyclotomic polynomial is larger than $\exp(\ln 2 \ln k / \ln \ln k)$ for infinitely many k. This fact has to be taken into account in asymptotic analysis of the bound from Theorem 2.

In a similar manner one can apply the faithful representation in Proposition 2 to obtain improvements. Since this is not as straightforward as in the previous case, we include a few more details. The polynomials $f(x) = (x^{2l} - 1)/(x^2 - 1) \in Z[x]$, $g(y) = (y^{2m} - 1)/(y^2 - 1) \in Z[y]$, and $h(z) = (z^{2n} - 1)/(z^2 - 1) \in Z[z]$ are monic, reciprocal, and of even degree; let $u_f = \deg(f)/2$, $u_g = \deg(g)/2$, $u_f = \deg(h)/2$, and let $u = u_f u_g u_h < lmn$. Take the ideal $J = (f(x), g(y), h(z)) \in \mathbb{Q}[x, y, z]$ and define $\xi = x + x^{-1} + J$, $\eta = y + y^{-1} + J$, and $\zeta = z + z^{-1} + J$. Further, let $\xi_i = x^i + x^{-i} + J$, $\eta_j = y^j + y^{-j} + J$, and $\zeta_k = z^k + z^{-k} + J$ for any integers i, j, k. Having now three independent variables, it is natural to take the basis B of the $\mathbb{Z}$-algebra $A = \mathbb{Z}[\xi, \eta, \zeta]$ to be formed of all products $\xi_i \eta_j \zeta_k$ where $0 \leq i < u_f$, $0 \leq j < u_g$, and $0 \leq k < u_h$; observe that the dimension of A is equal to u and replacing $\xi_0\, \eta_0\, \zeta_0$ with 1 we will have $1 \in B$. Again, after working out details regarding estimates on the parameters κ, λ, and C from Theorem 1, the counterpart of Theorem 2 reads as follows [8].

Theorem 3. *Let (l, m, n) be a hyperbolic triple. Then, for every positive integer δ there exists an epimorphism $\varphi : T(l, m, n) \to H$ onto a finite group H of injectivity radius at least δ such that $|H| \leq C^\delta$ where $C \leq 2^{32lmn}$.*

The exponent at C can be decreased further by observing that the calculations in [8] remain valid if, for $k \in \{l, m, n\}$, the polynomial $(x^{2k} - 1)/(x^2 - 1)$ is replaced with $x^k + 1$ or $(x^k + 1)/(x + 1)$, depending on whether k is even or odd. It can be shown that the dimension of A then decreases by a factor of 8, and hence $C \leq 2^{4lmn}$.

As regards pros and cons of the two approaches, Proposition 1 allows to work with algebras of relatively small dimension, particularly in the case when the greatest common divisor of l, m, n is relatively large compared to l, m, n. Also, working in the ring of algebraic integers $\mathbb{Z}[2\cos(\pi/k)]$ may be of advantage; for instance, its embeddability in a field which has been used in [8]. A disadvantage carried by Proposition 1 is the upper bound on κ which tends to be rather large. This drawback disappears in applications of Proposition 2 which allows κ to be constant, but on the other hand the dimension of the algebra (necessarily containing divisors of zero) then tends to be enormous if the greatest common divisor of l, m, n is relatively large compared to l, m, n.

Some of these drawbacks may be overcome by various refinements in calculations associated with bounding the parameters κ, λ, and C featuring in Theorem 1. Details [8] are quite involved and non-trivial in a number of places; they involve generalization of the concept of integral norm, and estimates of norms of matrices by a detailed investigation of the behaviour of matrix multiplication with respect to the new norm. We just list the following representative result [8] of the refined considerations.

Theorem 4. *Let (l, m, n) be a hyperbolic triple and let k be the least common multiple of l, m, n. Let $f(x)$ be the $2k$-th cyclotomic polynomial. Then, for every positive integer δ there exists an epimorphism $\varphi : T(l, m, n) \to H$ onto a finite group H of injectivity radius at least δ such that $|H| \leq D \cdot C^\delta$ where $D \leq (3 + \langle f \rangle)^{4k\phi(2k)}$ and $C \leq 2^{16\phi(2k)}$.*

We conclude this section with pointing out advantages of the algebraic background worked out in [8]. First, using variables of the form of a sum of an element and its reciprocal enabled to Tchebyshev's polynomials (that have a huge norm) aside and, instead, work with polynomials $(x^{2k} - 1)/(x^2 - 1)$ of norm 1. Second, the corresponding change of basis opened up room to working with powers of the generating matrices in a more direct way. Last, extending the concept of norm to generating sets allowed to use representations over complex numbers of comparatively small dimension.

As mentioned earlier, the (significant) improvements on the estimates on C and $\tilde{C}$ are exponential in lmn, while the lower bound extracted from [11] is polynomial in lmn. Possible paths to further improvements of lower bounds lead to the study of the shape of fundamental regions of normal, torsion-free, finite-index subgroups of triangle groups. Upper bounds could be refined by our methods applied to different bases or, possibly, with the help of the classification of 2-dimensional linear representations of triangle groups over finite fields [14]. Linear representations over u-dimensional algebras will, however, not help in removing the exponent u appearing in Theorem 1, because of Minkowski's theorem on lattice points in convex subsets of multidimensional spaces (see e.g. [6]).

5 APPLICATIONS TO PLANAR WIDTH OF REGULAR HYPERMAPS

In Section 2 we have indicated that research into injectivity radius of epimorphisms of triangle groups was actually motivated by questions about planar width of regular maps of type (m,n), which can be identified with regular hypermaps of type $(2,m,n)$. Accordingly, a pair (m,n) is hyperbolic if $1/m + 1/n < 1/2$. A standard surface representation of a regular map is obtained from the corresponding face-3-coloured hypermap by contracting faces coloured 2 to points and collapsing quadrangles coloured 1 to line segments. This, of course, changes the 1-skeleton of the map (compared to the 1-skeleton of the original hypermap). The corresponding triangle group $T(2,m,n)$ is usually presented as a two-generator group in the form $T(2,m,n) = \langle r,s|\ r^m = s^n = (rs)^2 = 1\rangle$, which requires a modification of definitions of injectivity radius and planar width when applied to a *map*. Therefore, in the context of maps, the map-injectivity radius of an epimorphism $\phi :\ T(2,m,n) \to H = \langle \rho,\sigma \,|\, \rho^m = \sigma^n = (\rho\sigma)^2 = \cdots = 1\rangle$ is defined with respect to the 'alphabet' $\{r, r^{-1}, s, s^{-1}\}$, and the planar width of a regular map is the smallest number of intersections of a non-contractible closed curve with the 1-skeleton of the *map*. In algebraic terms, the planar width of the map associated with an epimorphism $\varphi :\ T(2,m,n) \to H$ is the smallest positive integer d such that there exists a 'word' $w = (r^{i_1}s^{j_1})(r^{i_2}s^{j_2})\dots(r^{i_d}s^{j_d})$ such that $w \neq 1$ and $\varphi(w) = 1$.

Bounds on the map-injectivity radius of epimorphisms of $T(2,m,n)$ and on planar width of regular maps can therefore be obtained by the general methods outlined in the previous sections, with a number of shortcuts. Indeed, for $l = 2$, in every representation of $T(2,m,n)$ of the type (2), we can use $\xi = 0$ and, of course, ignore the matrix T and work just with R and S. Again, leaving details aside, one can prove the following result [8].

Theorem 5. *Let (m,n) be a hyperbolic pair and let k be the least common multiple of m,n. For any $\delta, d \geq 2$ there exists a representation of $T(2,m,n)$ of map-injectivity radius at least δ onto a group of order at most $D \cdot C^\delta$, where $C \leq 13^{4\phi(2M)}$, and a regular map of type (m,n) of planar width larger than d with automorphism group of order at most $D \cdot \tilde{C}^\delta$, where $\tilde{C} \leq (5mn)^{8\phi(2M)}$; in both cases D depends on m and n but not on δ.*

Further simplification can be made for concrete values of m,n. We illustrate this on the example $\{m,n\} = \{3,7\}$, important in the theory of maps; finite quotients of $T(2,3,7)$ are known under the name *Hurwitz groups* The best we can obtain by our methods (including refinements depending on the values of m,n) is the following, cf. [8].

Theorem 6. *For any $d, \delta \geq 2$ there exists a representation of $T(2,3,7)$ of map-injectivity radius at least δ into a finite group of order at most $5^{9\delta}$, and a regular map of type $(3,7)$ of planar width larger than d with automorphism group of order at most 21^{9d}.*

The constants 5^9 and 21^9 are much smaller than the values of 13^{48} and 105^{96} obtained by substituting $m = 3$ and $n = 7$ in the bounds of Theorems 5.

ACKNOWLEDGEMENT

The authors acknowledge partial support from the VEGA Grants No. 1/3020/06, 1/3022/06, 1/2004/05, and APVV Research Grants 20-000704, 0040-06, and LPP-0203-06. The second author would like to thank the Com2Mac Centre at Pohang University of Technology for warm hospitality during his stay which led to this paper.

REFERENCES

[1] M. Abas, Homomorphisms of triangle groups with large injectivity radius, Acta Math. Univ. Comenianae 72 (2003) 2, 253–259.

[2] K. S. Brown, "Buildings," Springer, 1989.

[3] J. Humphreys, "Reflection groups and Coxeter groups," Cambridge U. Press, 1990.

[4] M. Ipolyiová, Algebraic constructions of regular maps, PhD Dissertation, 2004.

[5] G. A. Jones, Triangular maps and non-congruence subgroups of the modular group, Bull. London Math. Soc. 11 (1979), 117–123.

[6] G. A. Jones and M. Jones, "Elementary Number Theory", Springer, 1998.

[7] G. A. Jones and D. Singerman, Belyĭ functions, hypermaps, and Galois groups, Bull. London Math. Soc. 28 (1996), 561–590.

[8] M. Mačaj, J. Širáň and M. Ipolyiová, Injectivity radius of representations of triangle groups and planar width of regular hypermaps, submitted for publication.

[9] A. Maľcev, On the faithful representation of infinite groups by matrices, Russian: Mat. Sbornik 8 (50) (1940) 405–422; English: AMS Transl. (2) 45 (1965), 1–18.

[10] J. Mennicke, Eine Bemerkung über Fuchssche Gruppen, Inv. Math. 2 (1967), 301–305.

[11] J. F. Moran, The growth rate and balance of homogeneous tilings in the hyperbolic plane, Discrete Math. 133 (1997) 1–3, 151–186.

[12] R. Nedela, Regular maps—combinatorial objects relating different fields of mathematics, J. Korean Math. Soc. 38 (2001) 5, 1069–1105.

[13] R. Nedela and M. Škoviera, Regular maps on surfaces with large planar width, European J. Combin. 22 (2001) 2, 243–262.

[14] Ch. Sah, Groups related to compact Riemann surfaces. Acta Math. 123 (1969), 13–42.

[15] J. Širáň, Regular maps on a given surface: a survey. Topics in discrete mathematics, 591–609, Springer, Berlin, 2006.

[16] J. Širáň, Triangle group representations and constructions of regular maps, Proc. London Math. Soc. (3) 82 (2001), 513–532.

[17] J. Tits, Groupes et géométries do Coxeter, unpublished manuscript, 1961.

[18] R. C. Vaughan, Bounds for the coefficients of cyclotomic polynomials, Michigan Math. J. 21 (1974), 289–295.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Genus parameters and sizings of groups

Thomas W. Tucker
Department of Mathematics, Colgate University, Hamilton, NY, U.S.A.

ABSTRACT: The various genus parameters for finite groups can be viewed in a broader context. A sizing is a function s from the set of all finite groups to the nonnegative integers satisfying $s(A) \leq s(B)$ whenever A is isomorphic to a subgroup of B. Numerous example and non-examples are given. Natural questions about a sizing s are its range (gaps), whether $s(Q) \leq s(A)$ when Q is a quotient group of A, whether s provides a certificate for isomorphism so that $s(A) = s(B)$ implies A is isomorphic to B. Given two sizings, the comparison set $C(s,t)$ is defined to be the set of all rational numbers $s(A)/t(A)$ where $t(A) \neq 0$. This provides a general setting for a variety of results like the $5/8$ theorem for commuting pairs or a similar $3/4$ theorem for proportion of involutions. It also provides a setting for asymptotic comparisons: define s and t to be asymptotic if both $C(s,t)$ and $C(t,s)$ are bounded. It is shown, for example, that all the genus parameters are asymptotic with each other for all groups of genus greater than one, but none are asymptotic to the order of a group.

1 INTRODUCTION

This paper is a sketch of some ideas I have been carrying around for the last few years and which I have discussed in a few seminars and conference talks in Christchurch (NZ) in 2000 and an AMS Special Session at Santa Barbara (USA) in 2005. Some sections here are just a definition and a few comments. Others are much more fully developed. There are many open questions and computations. Some are barely more than an exercise in an elementary group theory book; others are far more serious, even daunting. Once one starts looking at group theory through the glasses of sizings, one sees questions and conjectures sprouting everywhere. This viewpoint should provide plenty of work for anyone interested in group theory, from undergraduates to specialists. Participants at this conference asked for something they could reference, and that is why I have put these ideas on paper.

I wish to thank Marston Conder for helpful conversations.

Let **G** be the collection of all finite groups and let **N** denote the set of nonnegative integers. A function $s : \mathbf{G} \rightarrow \mathbf{N}$ is called a *sizing* if whenever the group A is isomorphic to a subgroup of B, then $s(A) \leq s(B)$.

Examples of sizings include:

1. The various genus parameters ([10]):
   - (a) $\gamma(A)$, the smallest g such that some Cayley graph for A can be embedded in the surface S_g of genus g
   - (b) $\sigma(A)$, the smallest g such that A acts (faithfully) as a group of homeomorphisms of S_g
   - (c) $\sigma^o(A)$, the smallest g such that A acts as a group of orientation-preserving homeomorphism of S_g
   - (d) $\tilde{\gamma}(A)$, the smallest number c such that a Cayley graph for A embeds in the nonorientable surface N_c with c crosscaps
   - (e) $\tilde{\sigma}(A)$, the smallest c such that A acts as a group of homeomorphism of N_c
2. $\beta(A)$, the least Betti number of any Cayley graph for A
3. $ord(A)$, the order of A

4. *exp*(A), the exponent of A
5. *#sub*(A), the number of subgroups of A
6. *#r*(A), the number of elements of order r
7. *com*(A), the order of the commutator of A
8. *#compair*(A), the number of ordered pairs of commuting elements
9. *#norpair*(A), the number of element-subgroup pairs (a, B) such that $aBa^{-1} = B$
10. *isomdim*(A), the least n such that A is isomorphic to an isometry group of euclidean space E^n, alternatively the smallest n such that A has a faithful representation in $GL(n)$ (see [2])
11. *perm*(A), the smallest n such that A has a faithful permutation representation on n symbols
12. Given any group property P inherited by subgroups (e.g abelian, solvable), the $0-1$ sizing defined by $P(A) = 0$ if A has property P and $P(A) = 1$ otherwise.

Most of these are sizings by definition. The parameters $\gamma, \tilde{\gamma}$, and β are sizings because of Babai's theorem [3] that given a subgroup B of the group A, any Cayley graph for A edge-contracts to a Cayley graph for B (and then use that edge-contraction cannot increase genus or Betti number).

There are also many natural parameters which are not sizings:

1. *rank*(A), the smallest size of a generating set for A
2. *abel*(A), the order of the abelianization A/A'
3. *series*(A), length of a composition series for A
4. *transperm*(A), the smallest n such that A acts faithfully and transitively on n symbols
5. *pres*(A), the length of the shortest presentation for A, measured by number of keystrokes in some standardized format

The simple observation that every group is a subgroup of the symmetric group S_n for some n explains why the first four parameters are not sizings (for the fourth, note that if A is abelian, *transperm*$(A) =$ *ord*(a)). For *pres*(A), consider presentations such as $A = \langle X, Y : X^2 = Y^{1000} = [Y, XYX] = 1\rangle$ with $B = \langle Y, XYX\rangle$. The sum of the lengths of the relators for A are $2 + 1000 + 8$. Letting $U = Y, V = XYX$, we get $B = \langle U, V : U^{1000} = V^{1000} = [U, V] = 1\rangle$ so the sum of the lengths for B is $1000 + 1000 + 4$, and it is not hard to show there can be no shorter presentation for $B \cong \mathbb{Z}_{1000} \times \mathbb{Z}_{1000}$.

2 GAPS AND POLES

A long standing problem for genus parameters is whether for every g there is a group of genus g. Call n a *gap* for the sizing s if there is no group A with $s(A) = n$, that is n is not in the range of s. At the other extreme, call n a *pole* for s if there are infinitely many groups A with $s(A) = n$.

For the genus parameters, it is known that 0 and 1 are the only poles for γ, σ, σ^o, because the Riemann-Hurwitz equation, and its generalization to embeddings of Cayley graphs [5], implies *ord*(A) is bounded above by $164(\gamma(A)-1)$, $84(\sigma^o(A)-1)$ and $168(\sigma(A)-1)$. May and Zimmerman [7] have shown that σ^o has no gaps, but it is not known whether there are any gaps for γ or σ. Conder and Tucker [4] have shown that the only possible gaps for σ occur when $g \equiv 8, 14 \bmod(18)$ and there is a prime p dividing $g - 1$ such that $p \equiv 5 \bmod (6)$ and the exponent of p in the factorization of $g - 1$ is odd.

We give two more elementary examples of gaps and poles.

Theorem 2.1. *For the sizing #2(A), the number of involutions in A, all even positive numbers are gaps and all odd numbers, together with 0, are poles.*

Proof. Clearly all odd order groups have no involutions, so 0 is a pole. If A has even order, by pairing an element with its inverse, we see that the number of nonidentity, noninvolutoary elements must be even, so the number of involutions must be odd. For every odd $n > 1$, the dihedral group D_n has n involutions and if m is odd, then $\#2(A \times \mathbb{Z}_m) = \#2(A)$, so all odd numbers $n > 1$ are poles. The groups $\mathbb{Z}_{2m}$ for m odd all have exactly one involution, so 1 is also a pole. □

If p is an odd prime, then $\#p(A)$ must be divisible by $p-1$ since the different subgroups of A of order p intersect only in the identity. Thus the only nongaps are for n divisible by $p-1$. Which multiples of $p-1$ are possible seems not to be known. Of course, all nongaps are poles (by taking products with groups whose order is not divisible by p).

Theorem 2.2. *For the sizing $\beta(A)$, the least Betti number of a Cayley graph for A, the only gaps are* 2 *and* $p+1$*, where* p *is a prime, and the only pole is* 1.

Proof. Let $C(A,X)$ be a Cayley graph for A of valence d; note that d is the number of involutions in X plus twice the number of non-involutions. Then the Betti number b of $C(A,X)$ is $E-V+1$, where $E = dV/2$ is the number of edges of $C(A,X)$ and $V = ord(A)$ is the number of vertices. Thus $b-1 = ord(A)(d/2-1)$, so $b-1$ is composite for $d > 4$. Moreover, if $d = 4$, then $b-1$ is composite unless $ord(A)$ is prime, in which case $A = \mathbb{Z}_p$ so $\beta(A) = 1$. Thus if $b-1 = p$, a prime, the only possibility is that $d = 3$ and $b-1 = ord(A)/2 = p$. But then $ord(A) = 2p$ and the only groups of order $2p$ are $\mathbb{Z}_{2p}$ or D_p, for which $\beta(A) = 1$. Thus $p+1$, for any prime p, is a gap for β. Also, if $\beta(A) = 2$, then $d = 3$ $ord(A) = 2$, but then $\beta(a) = 1$, so 2 is a gap as well.

Suppose instead that n is composite. We will show there is a group A with $\beta(A) - 1 = n$. First assume n is divisible by distinct odd primes. Then $r^2 \equiv 1 \bmod(n)$ has a solution other than $r = \pm 1$, so $A = \langle X, Y : X^2 = Y^n = 1, XYX = Y^r\rangle$, has $\beta(A) - 1 = 2n(3/2-1) = n$. If p is an odd prime and $n = p^r$, for $r > 1$, then $A = \mathbb{Z}_p \times \mathbb{Z}_{p^{r-1}}$ satisfies $\beta(A) - 1 = n(4/2-1) = n$. Finally, if $n > 2$ is even then $A = \mathbb{Z}_2 \times \mathbb{Z}_n$ satisfies $\beta(A) - 1 = 2n(3/2-1) = n$. Note that the trivial group has $\beta = 0$.

Finally, 1 is a pole since all cyclic groups have $\beta = 1$. Since $ord(A) \leq 2(\beta(A) - 1)$, when $\beta(A) > 1$, there can be only finitely many groups with $\beta = n$ for $n > 1$, so 1 is the only pole. □

We have not considered gaps and poles for other sizings, such as the examples given above. For some, such as *ord*, *exp* or *perm*, there are clearly no gaps and no poles. For others, such as *#sub* or *com*, the answers are not so obvious.

3 STRUCTURE OF THE COLLECTION OF ALL SIZINGS

The collection **S** of all sizings is clearly closed under addition and multiplication and hence forms a semi-ring. There is also an action on **S** by the set **ND** of nondecreasing functions $f : \mathbf{N} \to \mathbf{N}$ defined by $fs(A) = f(s(A))$. A natural question is whether **S** has some countable basis **B**. How one combines members of **B**, either simply by nonnegative integer linear combinations, or by multinomials, or by allowing orbits under the action of **ND**, would be open to interpretation. Note that if one allows orbits under **ND**, one cannot argue simply by cardinality, since **ND** is uncountable. To indicate the freedom one can have, if $f_n \in \mathbf{ND}$ is the characteristic function for the interval of integers $[n, \infty)$, then $\{f_n\}$ forms a basis for **ND** in the sense that every $f \in \mathbf{ND}$ can be written as an infinite linear combination $\Sigma a_n f_n$: note that the sum is finite for any given value of x since $f_n(x) = 0$ for all $n > x$.

4 CERTIFICATION

A sizing s is *certifying* if $s(A) = s(B)$ implies A and B are isomorphic, so that the values of s provide certificates for isomorphism class. Any sizing s without poles can be turned into a certifying sizing by spreading out each value in the range of s: if G_n is the set of groups A such that $s(A) = n$, define t inductively to be any one-to-one function from G_n to the closed interval of integers $\Sigma_{i<n}|G_i| + 1 \leq k \leq \Sigma_{i\leq n}|G_i|$. On the other hand, it would be interesting to have a certifying sizing whose values are related to some structural parameters on groups. For example,

$$s(A) = 2^{ord(A)}3^{com(A)}5^{\#sub(A)}7^{\beta(A)}11^{\sigma(A)}$$

is a sizing and $s(A) = s(B)$ would imply $ord(A) = ord(B), com(A) = com(B), \#sub(A) = \#sub(B), \beta(A) = \beta(B)$, and $\sigma(A) = \sigma(B)$.

5 COMPARISON AND ASYMPTOTICS

Given sizings s and t, define the *comparison set* to be the set of rational numbers $C(s,t) = \{s(A)/t(A) : t(A) \neq 0\}$. Define s and t to be *asymptotic* if both $C(s,t)$ and $C(t,s)$ are bounded. Given a subset $\mathbf{H} \subset \mathbf{G}$, we can define the *relative comparison set* $C_{\mathbf{H}}(s,t) = \{s(A)/t(A) : t(A) \neq 0, A \in \mathbf{H}\}$, and we can define s and t to be *asympotic* relative to $\mathbf{H}$ if both $C_{\mathbf{H}}(s,t)$ and $C_{\mathbf{H}}(t,s)$ are bounded.

Comparison sets provide a setting for some familiar exercises in elementary group theory:

Theorem 5.1. $C(\#compair(A), ord(A)^2) \subset (0, 5/8] \cup \{1\}$.

Proof. Assume A is not abelian. Then the center $Z(A)$ of A has index at least 4, since a cyclic extension of a central group is abelian. If $a \notin Z(A)$, then the centralizer $C(a)$ of a has index at least two, so a fails to commute with at least half the elements of A. Thus the number of noncommuting pairs is at least $(3/4)ord(A)(1/2)ord(A)$, so $\#compair(A)/ord(A)^2 \leq 5/8$. The value of 5/8 is achieved by the quaternions Q, since the center has index exactly 4 and every element not in the center has centralizer of index exactly 2. □

It is interesting to try to characterize the groups such that $\#compair(A)/ord(A)^2 = 5/8$. Clearly, $Q \times B$, where B is abelian, achieves the 5/8 bound (this includes all hamiltonian groups).

Theorem 5.2. *([9])* $C(\#2(A) + 1, ord(A)) \subset [0, 3/4] \cup \{1\}$.

Proof. (Marston Conder) Supppose $\#2(A) + 1 > (3/4)ord(A)$. We will show then that A is an elementary abelian 2-group. Let I be the set of involutions in A together with the identity and let $x \in I$. Since $|I| > (3/4)ord(A)$, we have $|xI \cap I| > (1/2)ord(A)$. Each element of $xI \cap I$ corresponds to an involution z such that $(xz)^2 = 1$, that is z is in the centralizer of x. We conclude that the centralizer of x has index less than two, so x is central. Thus $I \subset Z(A)$ so since $|I| > (3/4)ord(A)$, we have that A is abelian and all elements are involutions, except the identity. □

Theorem 5.3. $C(\#norpair(A), ord(A)\#sub(A))$ *is dense in* $[0, 1]$.

Proof. This is the main result of [8]. □

As an example of asymptotic sizings, we consider the various genus parameters. The following result appears in [6] and is alluded to in [11]. We include a sketch of the proof. First, define $\epsilon(\rho) = 1$ for $\rho = \gamma, \sigma, \sigma^o$ and $\epsilon(\rho) = 2$ for $\rho = \widetilde{\gamma}, \widetilde{\sigma}$.

Theorem 5.4. *Let ρ and τ be any of the genus parameters $\gamma, \sigma, \sigma^o, \tilde{\gamma}, \tilde{\sigma}$. Then there is a number $m(\rho, \tau)$, depending only on ρ and τ such that given any group A and any normal subgroup N:*

$$\rho(A/N) - \epsilon(\rho) \leq m(\rho, \tau)(\tau(A) - \epsilon(\tau))/ord(N).$$

Proof. We consider only the case $\rho = \sigma^o$ and $\tau = \gamma$; the other cases are handled in the same way. We want to find an m such that $\sigma^o(A/N) - 1 \leq m(\gamma(A) - 1)/|N|$. Suppose that $\gamma(A)$ is achieved by an embedding of the Cayley graph $C(A, X)$ of valence d in a surface of Euler characteristic $2 - 2\gamma(A)$. By standard counting arguments using Euler's formula and the fact that all faces have size 3 or more, we have

$$2 - 2\gamma(A) \leq |A|(1 - d/2 + d/3) = |A|(1 - d/6).$$

Since the image of X under the quotient map from A to A/N generates A/N, the quotient group A/N has a Cayley graph of valence d as well. That Cayley graph has a strongly symmetric embedding in some surface; the Euler characteristic of that surface is at least $|A/N|(1 - d/2)$ (assume there are no faces at all). Thus $2 - 2\sigma^o(A/N) \geq |A/N|(1 - d/2)$, and therefore

$$\sigma^o(A/N) - 1 \leq \frac{|A|(d-2)}{4|N|}.$$

First assume that $d > 6$. Rewriting the inequality for $\gamma(A)$, we have

$$|A| \leq (2\gamma(A) - 2)/(d/6 - 1) \leq 12(\gamma(A) - 1)/(d - 6),$$

Thus,

$$\sigma^o(A/N) - 1 \leq 3c(\gamma(A) - 1)/|N|,$$

where $c = (d-2)/(d-6)$. Since $d > 6$, we have $c \leq 5$, so $\sigma^o(A/N) - 1 \leq m(\gamma(A) - 1)/|N|$ with $m = 15$.

Assume now that $d \leq 6$. Then $\sigma^o(A/N) - 1 \leq |A|/|N|$. By the Hurwitz bound [5] for γ, $|A| \leq 168(\gamma(A) - 1)$, so $\sigma^o(A/N) - 1 \leq m(\gamma(A) - 1)/|N|$, where $m = 168$. Choosing the larger m from the two cases, we have the desired inequality. □

Applying this theorem for the case where N is the trivial group, we get that any two genus parameters ρ, τ are sympotitic relative to the set of groups satifying $\rho(A) > \epsilon(\rho)$ and $\tau(A) > \epsilon(\tau)$. It is not hard to show, using the same calculations, that one can also allow $\rho(A) = \beta(A)$, with $\epsilon = 1$, and hence all the genus parameters are asymptotic with β, over all groups of genus greater than 1.

The presence of the normal subgroup N is useful for another property of sizings. Call the sizing *s normal* if $s(Q) \leq S(A)$ for any quotient Q of A. Many sizings are obviously normal: $ord(A)$, $com(A)$,$\#sub(A)$, $\#r(A)$, $\#compair(A)$. Others are not: Marston Conder has an example with $perm(A) < perm(Q)$ with $perm(A) = 8$. By the Riemann-Hurwitz equation, $\sigma, \sigma^o, \widetilde{\sigma}$ are all normal and $\beta(A)$ is normal as well. It is still an open question whether γ or $\widetilde{\gamma}$ are normal. The case of Theorem 5.4 for $\rho = \tau = \gamma$ or $\rho = \tau = \widetilde{\gamma}$ sheds some light on the difficulty of the question.

It is worth noting that $ord(A)$ and $\beta(A)$ are not asymptotic, since $\beta(\mathbb{Z}_2^n) = 2^n(n/2 - 1)$.

6 SIZINGS FOR GRAPHS

One can also define sizings for graphs (and many other mathematical objects). Here there are choices for the partial ordering one chooses: graph minors, induced subgraphs. For example, $indep(G)$, the largest independent set in graph G, is a sizing for induced subgraph, but not minors, while the Betti number or genus of G are sizings for minors. In particular, the independence ratio, studied extensively by Alberston, Hutchinson and others, [1], is a form of comparison set for $indep(G)$ and $ord(G)$, the number of vertices in G. Sizings might form an interesting viewpoint for graph minors.

REFERENCES

[1] M.O. Alberston and J.P. Hutchinson, On the independence ratio of a graph, *J. Graph Theory* 2(1978), 1–8.

[2] M.O. Albertson and D. Boutin, Realizing finite groups in Euclidean space, *Journal of Algebra* 225(2000), 947–956.

[3] L. Babai, Some applications of graph contractions, *J. Graph Theory* 1(1977), 25–30.

[4] M.D.E. Conder and T.W. Tucker, unpublished.

[5] J.L. Gross and T.W. Tucker, *Topological Graph Theory*, Wiley-Interscience, New York 1987 (Dover paperback 2001).

[6] *Topics in Topological Graph Theory*, edited by J.L. Gross and T.W. Tucker, series editors R. Wilson and L Beinecke, Cambridge University Press, to appear.

[7] C.L. May and J. Zimmerman, There is a group of every strong symmetric genus, *Bull. Lon. Math. Soc.* 35(4) (2003), 433–439.

[8] G.J. Sherman, T.J. Tucker, M.E. Walker, How hamiltonian can a group be?, *Arch. Math. (Basel)* 57(1991), 1–5.

[9] C.T.C. Wall, On groups consisting mostly of involutions, *Proc. Camb. Phil. Soc.* 67(1970), 251–262.

[10] T.W. Tucker, Groups acting on surfaces and the genus of a group, *J. Comb. Th., Series B* 34 (1983), 82–98.

[11] T.W. Tucker, Symmetric embeddings of Cayley graphs in nonorientable surfaces, in *Graph Theory, Combinatorics and Applications: Proceedings on the Sixth International Conference on the Theory and Applications of Graphs*, edited by Alavi, Chartrand, Oellerman, Schwenk, Wiley-Interscience, New York 1991, pp. 1105–1120.

Applications of Group Theory to Combinatorics – Koolen, Kwak & Xu (eds)
© 2008 Taylor & Francis Group, London, ISBN 978-0-415-47184-8

Belyi functions: Examples, properties and applications

Alexander K. Zvonkin
LaBRI, Université Bordeaux I, France

ABSTRACT: Let X be a Riemann surface, and $f : X \to \overline{\mathbb{C}}$ a non-constant meromorphic function on X (here $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ is the complex Riemann sphere). The function f is called a *Belyi function*, and the pair (X, f), a *Belyi pair*, if f is unramified outside $\{0, 1, \infty\}$. The study of Belyi functions, otherwise called the theory of *dessins d'enfants*, provides a link between many important theories. First of all, it is related to Riemann surfaces, as follows from the definition. Then, to Galois theory since, according to the Belyi theorem, a Belyi function on X exists if and only if X is defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers. It is also related to combinatorics of maps, otherwise called embedded graphs, since $f^{-1}([0, 1])$ is a graph drawn on the two-dimensional manifold underlying X. Therefore, certain Galois invariants can be expressed in purely combinatorial terms. More generally, many properties of functions, surfaces, fields, and groups in question may be "read from" the corresponding pictures, or sometimes constructed in a "picture form". Group theory is related to all the above subjects and therefore plays a central role in this theory.

The theory of Belyi functions is very rich with beautiful examples. It is difficult to give a representative sample of them, but we will try to do it at least to some extent.

1 MAPS AND HYPERMAPS

Convention 1.1. We consider only connected graphs; loops and multiple edges are allowed. All maps in this paper will be oriented.

When we draw a graph on a piece of paper, we add to it an additional structure. Namely, we choose a particular cyclic order of the edges in the vicinity of each vertex. Also, the drawing itself subdivides the plane into a number of regions. The resulting object is a map; however, the theory of maps is more beautiful when we draw graphs not on the plane ("piece of paper") but on the sphere, the torus, or another compact two-manifold.

Definition 1.2 (Map). A *map* is a graph embedded in a compact oriented two-dimensional manifold in such a way that

- the edges do not intersect;
- the complement of the graph in the surface is a disjoint union of regions homeomorphic to open disks.

These regions are called *faces* of the map. The *genus* of the map is, by definition, the genus of the underlying surface.

We define the *degree of a vertex* as the number of incident edges (loops are counted twice), and the *degree of a face*, as the number of edges surrounding it ("inner edges" are counted twice).

Figures 1, 2, 3 will help to understand the above definitions.

Definition 1.3 (Hypermap). A *hypermap* is a bicolored map: its vertices are colored in black and white in such a way that the adjacent vertices have opposite colors.

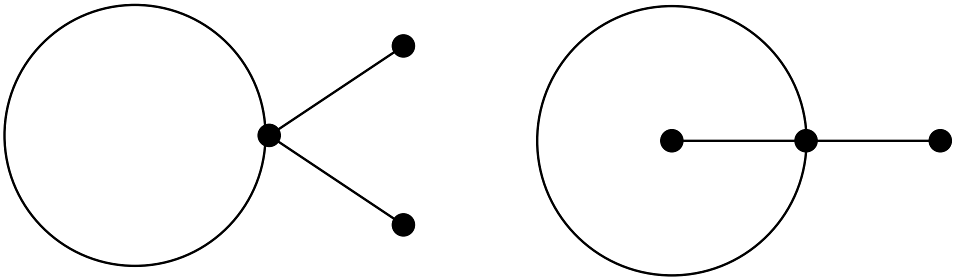


Figure 1. One graph but two different maps. The face degrees of the map on the left are 1 and 5, and for that on the right, 3 and 3. Note that a graph does not have faces at all: it has only vertices and edges.

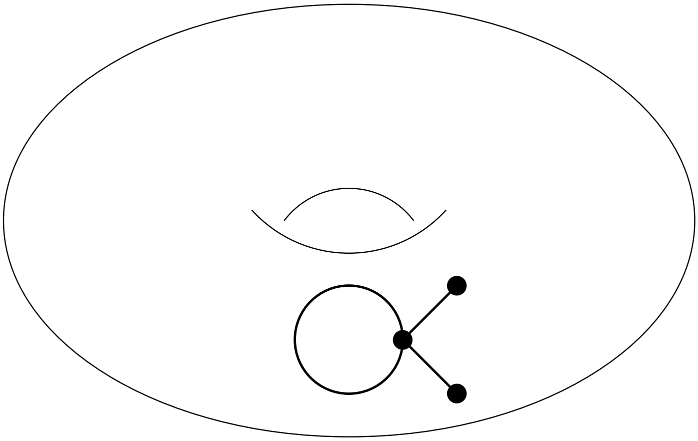


Figure 2. This is not a map: one of the “regions” obtained after cutting the surface along the edges of the graph is not homeomorphic to an open disk.

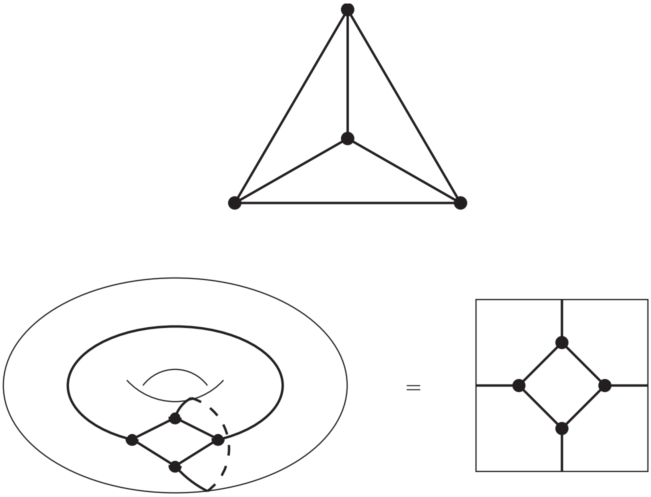


Figure 3. The graph K_4 gives rise to a map of genus 0 (tetrahedron) having 4 faces of degree 3, and to a map of genus 1 having 2 faces, of degree 8 and 4 respectively.

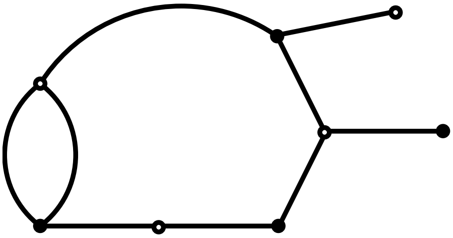


Figure 4. A hypermap.

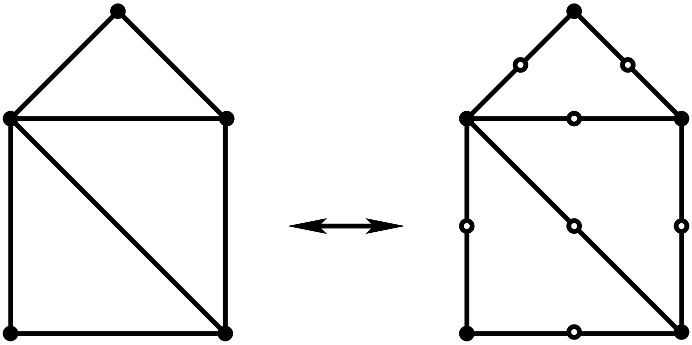


Figure 5. Maps may be considered as hypermaps whose white vertices are all of degree 2.

An example of a hypermap is given in Figure 4.

The above definition suggests that a hypermap is a particular case of a map. However, hypermaps were first invented as generalizations of maps [5]. Indeed, taking a map, we may insert a white vertex in the middle of every edge (see Figure 5), thus obtaining a particular case of a hypermap—such that all its white vertices are of degree 2.

Convention 1.4. Our convention will be as follows:

- we always work with hypermaps;
- if it so happens that all the white vertices of a given hypermap are of degree 2, we erase them in order to simplify the picture and draw the hypermap as a map—and quite often even call it a map;
- in order to be coherent with the previous definitions, the segments joining a black vertex with a white one are called not edges but *half-edges*; then, for example, the degree of a face is equal to the number of surrounding half-edges divided by 2; the term "edge" is reserved for maps.

For a hypermap H with n half-edges, the Euler characteristic is computed as follows:

$$\chi(H) = 2 - 2g = B + W + F - n$$

where B is the number of black vertices, W is the number of white ones, and F is the number of faces.

Encoding by permutations. Hypermaps admit an encoding by triples of permutations. In constructing this incoding, we twice use the fact that the surface on which the hypermap is drawn is oriented: first, a half-edge has a left bank and a right bank; second, the vicinity of every vertex has a positive and a negative orientation.

Let H be a hypermap with n half-edges. We label the half-edges by the labels from 1 to n, and place the label of a half-edge near its left bank when we go from its black end to the white one. Then we associate to H the following triple of permutations $(\sigma, \alpha, \varphi)$ on the set of n labels:

- a cycle of σ contains the labels of the half-edges incident to a black vertex, taken in the positive (i. e., counterclockwise) direction around this vertex; thus, there are as many cycles in σ as there are black vertices, and the degree of a vertex is equal to the length of the corresponding cycle;
- the cycles of α correspond, in the same way, to white vertices;
- a cycle of φ contains the labels placed inside a face; these labels are taken in the positive direction around the center of the face; thus, there are as many cycles in φ as there are faces, and the degree of a face is equal to the length of the corresponding cycle.

Example 1.5. For the hypermap of Figure 6, we obtain the following permutations:

$$\begin{aligned}\sigma &= (1,2,3)(4,5)(6)(7,8,9),\\ \alpha &= (1,4)(2,9,3)(5,6,7)(8),\\ \varphi &= (1,5,9)(2)(3,8,7,6,4).\end{aligned}$$

For the outer face, the first impression is that the corresponding cycle $(3,8,7,6,4)$ turns in the negative direction. In fact, we must look "from the opposite side of the sphere", or, otherwise, "from the inside of the outer face", and then the direction becomes positive.

Remark 1.6. The following very important observation is true for any hypermap (the proof is a simple exercise):

$$\sigma\alpha\varphi = 1.$$

Therefore, in order to encode a hypermap, we may take any two of the three permutations. The form we have chosen is, however, more symmetric.

The correspondence between hypermaps and triples of permutations also works in the opposite direction.

Proposition 1.7. *To any triple of permutations $(\sigma, \alpha, \varphi)$ such that*

- *the permutation group $G = \langle \sigma, \alpha, \varphi \rangle$ is transitive,*
- *$\sigma\alpha\varphi = 1$,*

there corresponds a hypermap.

The condition of transitivity ensures the connectivity of the corresponding graph.

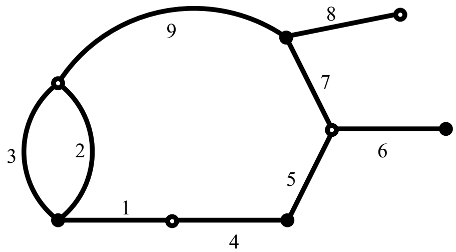


Figure 6. A labeling of the hypermap of Figure 4.

2 DIGRESSION: THE CARTOGRAPHIC GROUP

A fact which rarely attracts attention is that a simple picture drawn on a piece of paper, via the triple of permutations described above, generates a permutation group. We call this group $G = \langle \sigma, \alpha, \varphi \rangle$ the *cartographic group* corresponding to a (hyper)map. Of course, more often than not the group thus obtained is either S_n or A_n. But there exist also many other, more interesting examples. A very small sample is given in Figures 7, 8, 9.

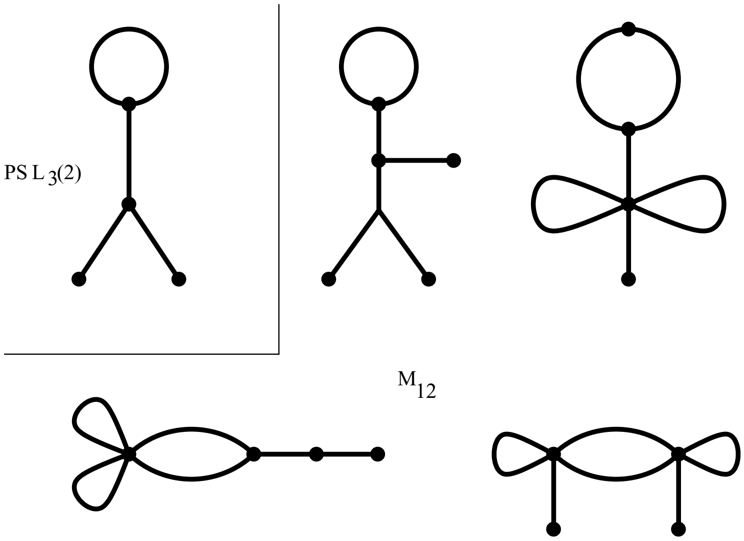


Figure 7. A map with 4 edges representing the group $PSL_3(2)$, and four maps with 6 edges representing the Mathieu group M_{12}. In total, there are 50 planar maps with 6 edges representing M_{12}.

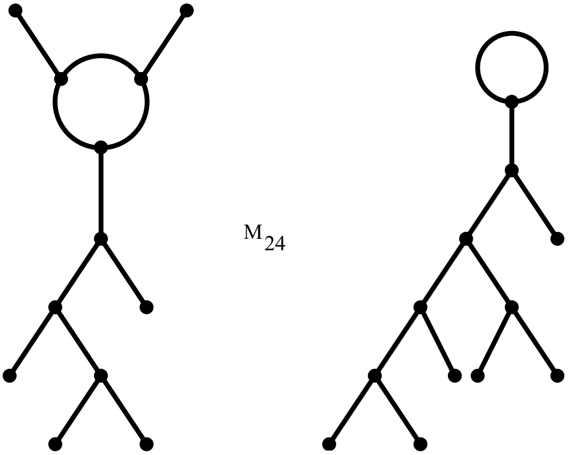


Figure 8. Two maps with 12 edges representing the Mathieu group M_{24}; the one on the right was found by N. Adrianov (private communication).

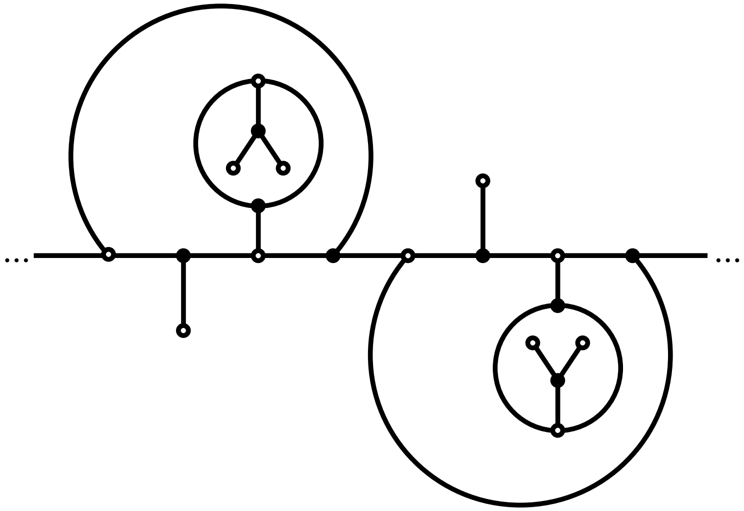


Figure 9. A hypermap with 24 half-edges representing M_{24} (this example is borrowed from [3]). The horizontal line is an equator on the sphere. All the 6 faces are of degree 4.

3 BELYI FUNCTIONS: PLANAR CASE

Definition 3.1 (Belyi function). Let H be a planar hypermap with n half-edges. A rational function f of degree n is a *Belyi function* corresponding to H if H may be embedded in the Riemann complex sphere $\overline{\mathbb{C}}$ in such a way that:

1. All black vertices of H are roots of the equation $f(x) = 0$, the multiplicity of each root being equal to the degree of the corresponding vertex.
2. All white vertices of H are roots of the equation $f(x) = 1$, the multiplicity of each root being equal to the degree of the corresponding vertex.
3. The hypermap itself is the preimage of the segment $[0, 1]$, that is, $H = f^{-1}([0, 1])$.
4. Inside each face of H there exists a (single) pole of f (or, if you like, a root of the equation $f(x) = \infty$), the multiplicity of the pole being equal to the degree of the face. We will call this pole the *center* of the face (of course, it is in no way its "geometric center").
5. Besides 0, 1, and ∞, there are no other critical values of f.

(A *critical point* of f is a root of its derivative (with a standard change of variables when it comes to infinity); a *critical value* of f is the value of f at its critical point.)

In fact, it is not difficult to see that *any* rational function which does not have critical values outside the set $\{0, 1, \infty\}$ is a Belyi function corresponding to a hypermap. (If there are three critical values but they are not equal to 0, 1 or ∞, we may apply a linear fractional transformation and place them to 0, 1, and ∞.) Therefore, we may take as a definition of a Belyi function the property of not having critical values outside the set $\{0, 1, \infty\}$.

The correspondence also works in the opposite direction.

Theorem 3.2. *For every hypermap H, there exists a corresponding Belyi function $f = f(x)$. This function is unique, up to a linear fractional transformation of the variable x.*

This theorem is a particular case of Riemann's existence theorem which we will formulate later.

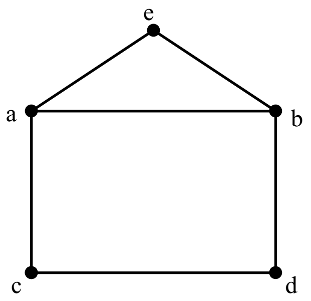


Figure 10. A “dessin d’enfant”.

An interesting and highly nontrivial question is, given a hypermap, how to compute the corresponding Belyi function. Let us illustrate some initial stages of such a computation. Suppose we have the “dessin d’enfant” shown in Figure 10.

According to the 1st condition of Definition 3.1, the points a, b, c, d, e must be the roots of the function f we are looking for, with multiplicities corresponding to the vertex degrees. Therefore, the numerator of f must have the form

$$(x-a)^3(x-b)^3(x-c)^2(x-d)^2(x-e)^2.$$

In fact, it is much more convenient to write this expression in the form

$$(x^2+px+q)^3(x^3+rx^2+sx+t)^2$$

since the parameters p, q, r, s, t belong to a smaller and simpler field than a, b, c, d, e (just imagine r, s, t being rational numbers while c, d, e being cubic irrationals).

Our map has 6 edges, which means that the hypermap in question has 6 white vertices, all of degree 2. Therefore, the numerator of the function $f-1$ is a product of 6 quadratic factors, or, better (as before), a square of a polynomial of degree 6.

Finally, the map has three faces, of degree 5, 4, and 3 respectively. Therefore, according to the 4th condition of Definition 3.1, the denominator of f factorizes as $(x-A)^5(x-B)^4(x-C)^3$.

As a result we have:

$$f(x) = K\frac{(x^2+px+q)^3(x^3+rx^2+sx+t)^2}{(x-A)^5(x-B)^4(x-C)^3},$$

and

$$f(x)-1 = K\frac{(x^6+mx^5+nx^4+ux^3+vx^2+wx+z)^2}{(x-A)^5(x-B)^4(x-C)^3}.$$

Taking the first expression, computing $f-1$ and equating the result to the second expression, we obtain a system of 12 algebraic equation in 15 unknowns $K, p, q, r, s, t, m, n, u, v, w, z, A, B, C$.

The three remaining degrees of freedom correspond to the possibility of making a linear fractional transformation of x. It allows us to choose certain parameters to our convenience. For example, traditionally the center of the outer face is placed to ∞, thus making the denominator of f equal to $(x-B)^4(x-C)^3$. We may also put, for example, $B=0$ (any other choice not equal to ∞ would also be possible), and to choose a value for one more parameter almost arbitrarily. However, one must be careful since certain choices of values for unknowns may turn out to be contradictory.

For example, if a map is centrally symmetric then the sum of the positions of black vertices is equal to the sum of the positions of white vertices; hence, we cannot take one sum equal to 0 and the other one equal to 1.

Galois action. Now it comes as no surprise that the coefficients of Belyi functions can always be made algebraic numbers. (Of course, we could have a weird idea to take $B = \pi$ instead of $B = 0$ and thus to spoil everything; but we will be wise.) This property of Belyi functions leads to the most interesting aspect of the theory of dessins d'enfants, namely, the action of the *absolute Galois group* $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ (the automorphism group of the field $\overline{\mathbb{Q}}$ of algebraic numbers) on the hypermaps. We act on the coefficients of a Belyi function, replacing them by their Galois conjugates. In this way we obtain another Belyi function which corresponds to another hypermap.

Unfortunately, we cannot develop this subject here since it needs a much longer exposition. Therefore, we limit ourselves with few remarks concerning some combinatorial invariants of the Galois action. The simplest and most obvious such invariant is the triple of cycle structures of the permutations σ, α, φ. Indeed, even from our brief discussion above it becomes clear that these cycle structures represent the only information we used while writing down the system of algebraic equations on the coefficients of the function. More advanced invariants are: the automorphism group of a hypermap; its cartographic group; the triple of conjugacy classes of σ, α, φ in the cartographic group (a very subtle case is represented, for example, by the Mathieu group M_{22} in which there exist two algebraically non-conjugate classes, $4A$ and $4B$ in the Atlas [4] notation, with cycle structure $4^4 2^2 1^2$; note that hypermaps with σ, α, φ all having the cycle structure $4^4 2^2 1^2$ are planar); and even some highly non-trivial information about the number field to which the coefficients belong can be found in the character table of the cartographic group.

A less advanced but more combinatorial in nature is such an invariant as the property of a map to be self-dual. It involves the operation of composition of which we will speak later. For other types of invariants, such as certain diophantine relations between vertex degrees, see [9].

Plane trees and Shabat polynomials. A particular case of a hypermap is a *bicolored plane tree*, that is, a planar hypermap with a single face, see Figure 11. If we put the single pole to infinity, the corresponding Belyi function becomes a polynomial. These polynomials are called *Shabat polynomials*.

Example 3.3. The two simplest trees are shown in Figure 12; their Shabat polynomials are:

- for the star-tree, $f(x) = x^n$;
- for the chain-tree, $f(x) = T_n(x)$, the Chebyshev polynomial (critical values, instead of being 0 and 1, are ± 1).

One more example is given in Figure 13. The corresponding Shabat polynomial is

$$f(x) = \frac{1}{729} \cdot (2x^2 - 3x + 9)^3 (x + 1),$$

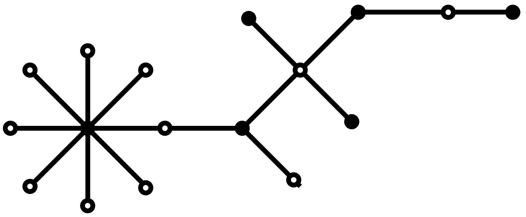


Figure 11. A plane tree.

while

$$f(x) - 1 = \frac{1}{729} \cdot x^3(8x^4 - 28x^3 + 126x^2 - 189x + 378)$$

(the vertex of degree 3 at the origin must be considered as white).

The whole construction leads to a very unusual property of plane trees:

Proposition 3.4. *Every plane tree has a canonical geometric form.*

Indeed, linear fractional transformations that don't move infinity are affine transformations. Therefore, the tree obtained via its Shabat polynomial can be rotated, translated, and undergo a homothetic transformation, but all these do not change its geometric form.

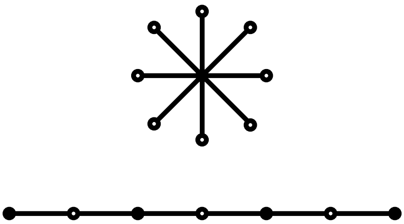


Figure 12. The star-tree and the chain-tree.

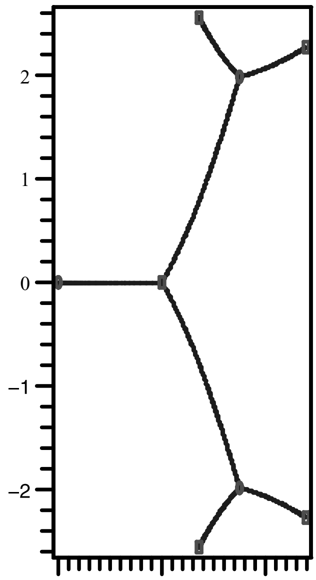


Figure 13. A plane tree obtained as a preimage of a segment via its Shabat polynomial (courtesy of J. Bétréma).

4 DAVENPORT–STOTHERS–ZANNIER BOUND: AN APPLICATION OF BELYI FUNCTIONS

Let $P, Q \in \mathbb{C}[x]$ be two coprime complex polynomials. The question we would like to discuss is, what is the smallest possible degree of $P^3 - Q^2$?

Denote $\deg P = 2n$, $\deg Q = 3n$, and let

$$P^3 - Q^2 = R.$$

In the paper [2] (1965), the authors have formulated two conjectures:

- $\deg R \geq n + 1$;
- this bound is sharp; that is, it is attained for infinitely many values of n (as we will see shortly, it is, in fact, attained for every n).

The first conjecture was proved by Davenport in the same year [6]. The second one remained open for 16 years and was finally proved by Stothers [15]; later on, it was reproved once again and generalized by Zannier [16]. It is this second, and apparently more difficult conjecture (the sharpness of the bound) that we will prove now.

Let us denote

$$f = \frac{P^3}{R}$$

and remark that

$$f - 1 = \frac{P^3 - R}{R} = \frac{Q^2}{R}.$$

The computational part of the proof is finished. Now we make the following

Assumption 4.1. Assume that f is a Belyi function.

What follows is just a translation of the initial problem data into combinatorial properties of the corresponding hypermap.

- The numerator of f is P^3, $\deg P = 2n$; this means that the hypermap in question has $2n$ vertices, all of them of degree 3.
- The numerator of $f - 1$ is Q^2, $\deg Q = 3n$; this means that the hypermap has $3n$ white vertices, all of them of degree 2. It is a map! Forget white vertices and half-edges, let us speak of edges.
- For the number of faces F, the Euler formula gives

$$2n - 3n + F = 2 \;\Rightarrow\; F = n + 2.$$

Put the center of one of the faces to ∞; then the $\deg R$ becomes equal to the sum of the degrees of the remaining $n + 1$ faces.

Summing up: in order to prove the statement, we must construct a planar map having $3n$ edges, $2n$ vertices of degree 3, and all its $n + 1$ “finite” faces of degree 1.

We would like to underline the fact that up to now we did nothing: we have only translated the initial problem into a combinatorial language. But now the problem becomes trivial: its solution is shown in Figure 14.

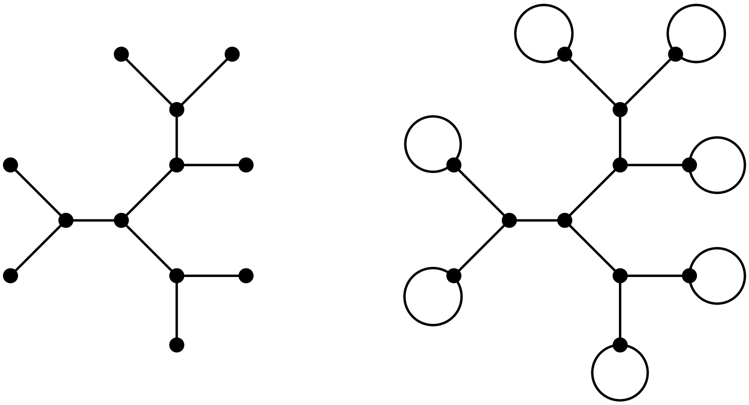


Figure 14. Draw a tree with all its internal vertices of degree 3 and attach a loop to each leaf.

5 COMPOSITION

Many operations with maps and hypermaps can be represented using a composition of functions:

$$h : X \xrightarrow{f} Y \xrightarrow{g} Z.$$

Here, at least in this section, X, Y, and Z all mean the complex sphere $\overline{\mathbb{C}}$ but we use different letters in order to clearly distinguish on which level our operations take place.

Dual map. Let f be a Belyi function for a map. How to find a Belyi function to its dual map? It is very simple: we need to exchange vertices with face centers while leaving the (invisible) white vertices at the same places. In the language of Belyi functions this just means exchanging critical values 0 and ∞ while leaving 1 unchanged. The function that makes this operation is $g_1(y) = 1/y$. Therefore, the Belyi function corresponding to the dual map is $h(x) = 1/f(x)$. The operation, of course, remains meaningful also for hypermaps.

Doubling edges. For a map, we would like to replace every edge by two parallel edges surrounding a face of degree 2. For a hypermap, a new face must surround each white vertex, and the degree of this face must be equal to the degree of the corresponding white vertex. The degrees of all black vertices become twice bigger than before; the degrees of all "old" faces are preserved. Note that even for a hypermap the result of this operation will be a map.

Using the same reasoning as before, we understand that we need a function $g(y)$ which would send 0 to 0 (doubling the multiplicity), ∞ to ∞, and 1 to ∞. And we easily find $g(y) = y^2/(y-1)$. However, there is a mistake here. The function g creates a new critical value: $g'(y) = y(2-y)/(y-1)^2$ has two roots 0 and 2, and $g(0) = 0$, which is OK, but $g(2) = 4$. The function $h = g \circ f$ thus constructed will have four critical values: $z = 0, 1, 4, \infty$. The mistake is very easy to correct: we must just take $g_2(y) = y^2/4(y-1)$.

A map together with its dual. We have a map, and we would like to draw it together with its dual in the same picture. Note that now the white vertices become "visible" since they all acquire degree 4. The function g we are looking for must send 1 to 1 doubling the multiplicity, and send both 0 and ∞ to 0. Such a function is $g_3(y) = 4y/(y+1)^2$.

Medial map. Taking a map, we transform all its (invisible) white vertices of degree 2 into black vertices of degree 4 by joining them successively by new edges inside each face. The face degrees remain the same while all black vertices are replaced by faces whose degrees are equal to degrees of the former vertices. The corresponding transformation is realized by $g_4(y) = -(y-1)^2/4y$.

Truncation. When applied to a polyhedron, this operation means "cutting vertices". For an arbitrary map, it means replacing each black vertex by a face of the same degree, and inserting a new black vertex of degree 3 inside each edge (thus, each edge gets two new vertices which are placed near both its ends).

It is important to understand that the functions g_1, g_2, g_3, g_4 constructed up to now are themselves Belyi functions. We leave it to the reader to draw the corresponding hypermaps. All the above operations can be understood in the following way: instead of drawing the segment $[0,1]$ on Y-sphere, we draw there a simple hypermap H, which is sent to the segment $[0,1]$ on the Z-sphere by the function g. Then, the hypermap on the X-sphere is obtained as $f^{-1}(H)$. A necessary condition for this operation to be successful is the following one: the critical values of f, that is, $0, 1, \infty \in Y$, must find themselves among the g-preimages of $0, 1, \infty \in Z$, that is, among vertices and face centers of H.

The case of the truncation is not an exception. In this case, the hypermap H on the Y-sphere looks as is shown in Figure 15. The corresponding Belyi function is $g_5(y) = (4y-1)^3/27y$. (Thus, the position of the black vertex is $y = 1/4$, and the position of the white vertex of degree 2 may be easily computed: it is the double root of $g_5(y) - 1$, which is $y = -1/8$.)

Remark 5.1. One can verify that $g_5 \circ g_4 = g_5 \circ g_2$. At first sight, this seems to be not very surprising since g_4 and g_2 are Belyi functions corresponding to the same map which is only placed in two different ways on the sphere. Hence, this fact represents an invariance of a function under certain linear fractional transformations. Yes, but the invariance of *which* function? It is, in fact, the composition which is invariant, and the map corresponding to it has a symmetry of order 3, but neither g_5 itself nor g_4 or g_2 are symmetric.

This is one of the examples of rational functions represented as a composition in a non-unique way. The problem was studied by Ritt in [13], [14] but completely solved (in [13]) only for polynomials. Essentially, only the polynomials x^n and $T_n(x)$ of Example 3.3 with n non prime allow a non-uniqueness. For rational functions in general, as Ritt wrote, "there is a much greater variety of possibilities".

Edge subdivision. In order to subdivide every edge of a map in n parts (that is, insert in it $n-1$ new vertices) we must apply the Chebyshev polynomial $T_n(y)$ (see Example 3.3) normalized in such a way as to have critical values 0 and 1 instead of ± 1, namely, $g_6(y) = (T_n(y)+1)/2$. Don't think that the parts in which an edge is subdivided are equal.

Rotational symmetry. The other "simplest" polynomial of Example 3.3 is commonly used in another way. Suppose we have a hypermap on the X-sphere which is invariant under rotation through the angles $k(2\pi/n)$, $k = 0, \ldots, n-1$ around one of its elements (i. e., a vertex or a face center). Note that this rotation center cannot be alone since a rotation of the sphere is always around an axis that passes through two antipodal points. Then, putting one of these points to 0 and the other one to ∞, and applying $f(x) = x^n$ we obtain a *reduced*, or a *quotiened* hypermap on the Y-sphere. After this operation, the degrees of the elements placed at 0 and ∞ become divided by n while all other elements of the initial hypermap are subdivided in blocs of size n (orbits of the rotation) and

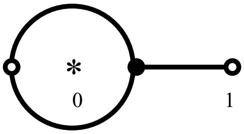


Figure 15. If we replace the segment [0, 1] by this hypermap, its preimage will give us a truncated map.

each bloc becomes represented by a single element of the reduced hypermap. Now we can apply a Belyi function $g(y)$ corresponding to this reduced hypermap.

A Belyi function of a cube. We are now able to attack a more complicated task and compute a Belyi function for the map of the cube. Let us place the center of a face at 0, and the center of the opposite face, at ∞. Then, applying the function x^4 we get the map shown in Figure 16. We recognize in it a truncation of a very simple map consisting of a unique edge $[0, \infty]$. Incidentally, the Belyi function of this latter map is g_3. Summing up, we obtain a Belyi function of the cube as a composition $f_{\text{cube}}(x) = g_5 \circ g_3 \circ x^4$. The result of the computation gives

$$f_{\text{cube}}(x) = -\frac{1}{108} \cdot \frac{(x^8 - 14x^4 + 1)^3}{x^4(x^4+1)^4}.$$

This function, as well as Belyi functions for the other Platonic maps were found by Felix Klein in 1875, see [8]. In [10], we have computed Belyi functions for all the Archimedean maps. The paper is a long series of exercises in composition, with two relatively more difficult computations for chiral maps, and with a very difficult one for the only non vertex-transitive Archimedean map.

Not everything is that simple. Let us consider a family of maps with 6 edges, with vertex degrees $6, 3, 2, 1$, and with face degrees also $6, 3, 2, 1$. The first, and rather challenging question is to find them all and to say how many of them there are. I never met a single person (including myself) who would find a correct answer within 3 days.

In a paper format, I cannot keep the answer secret for 3 days, so here it is: there are 18 maps with this set of vertex and face degrees. (Try to find them now!) For 6 of them the cartographic group is A_{12}; for other 8, it is M_{12}; and for remaining 4 maps we get an imprimitive group. This is why the family of 18 splits into three Galois orbits, of size 6, 8, and 4, respectively. One of the maps with an imprimitive cartographic group is shown in Figure 17 on the left.

According to a famous theorem due to Ritt, a ramified covering with an imprimitive monodromy group is a composition of two (or more) coverings. (Ritt [13] formulated this theorem only for polynomials but it remains true also in a more general setting.) In our case, this means that the Belyi function h of the map on the left in Figure 17 is a composition: $h = g \circ f$. Does it jump to the eye when you look at the picture? I bet it doesn't.

But watch out! In this case the function f itself is not a Belyi function. Indeed, it has not 3 but 4 critical values. However, it turns out that these 4 critical values are two (black) vertices and two

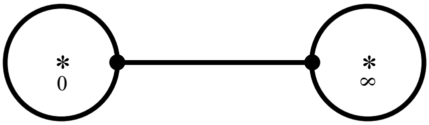


Figure 16. A cube quotiened by a rotational symmetry of order 4.

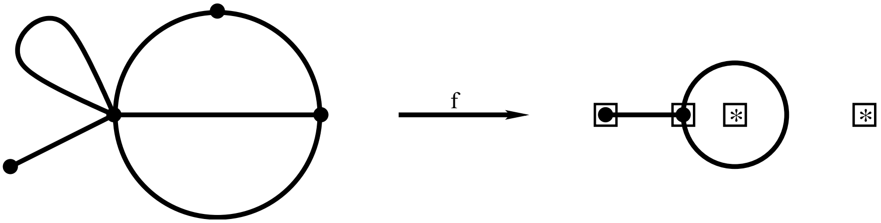


Figure 17. A decomposable map, and how it covers another map. Little squares show critical values of f.

face centers of a simpler map which is obtained via a Belyi function g. (In Figure 17, critical values of f are marked by little squares.) Hence, g sends all the four critical values of f to 0 and to ∞, and also creates a new critical value 1. This is why the composition $h = g \circ f$ is a Belyi function.

We do not present the results of the computations. Don't forget that this Galois orbit contains 4 elements; therefore, the coefficients of our rational function are themselves expressions involving roots of an equation of degree 4.

6 BELYI FUNCTIONS AND JULIA SETS

Definition 6.1 (Dynamical Belyi function). A Belyi function $f : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ is called *dynamical* if it sends $\{0, 1, \infty\}$ to $\{0, 1, \infty\}$ (any of the 27 possible combinations is allowed).

Remark 6.2. We know that

$$f^{-1}(\{0, 1, \infty\}) = \{\text{black vertices, white vertices, and face centers}\}.$$

Hence, a Belyi function f is dynamical if and only if the corresponding hypermap is positioned on the complex sphere in such a way that the three points 0, 1, and ∞ are "occupied" by black or white vertices or face centers (any combination is possible). If this is not the case then we can achieve this by using a linear fractional transformation which permits to put any three points of our choice to any three positions.

The reason of imposing this conditions is that a composition $h = g \circ f$ of two dynamical Belyi functions f and g is once again a dynamical Belyi function. Therefore, it is possible to iterate a dynamical Belyi functions

$$f^n = f \circ f \circ \cdots \circ f \quad (n \text{ times})$$

and get as a result a Belyi function.

Definition 6.3 (Fatou and Julia sets). For a sequence of iterations f^n the *Fatou set* is an open set $F \subseteq \overline{\mathbb{C}}$ such that for any $x \in F$ there exists a neighborhood U of x on which the iterations f^n form a "normal family": for any sequence $n_1, n_2, \ldots$ and for any compact $K \subset U$ there exists a subsequence for which the iterations converge uniformly on K. The *Julia set* is the complement to the Fatou set: $J = \overline{\mathbb{C}} \setminus F$.

Informally speaking, the Fatou set is the set of the regular behavior of the iterations, and the Julia set is the set of their irregular behavior.

We all saw beautiful pictures of fractal Julia sets. Less attractive visually but interesting from the theoretical point of view is the case of the so called "complete chaos".

Definition 6.4 (Complete chaos). The dynamical system f^n, $n \geq 1$, is completely chaotic if its Julia set coincides with the whole sphere: $J = \overline{\mathbb{C}}$.

The following famous theorem due to D. Sullivan (1985), see [16], gives a criterion for a complex dynamical system to be completely chaotic.

Theorem 6.5. *If all critical points of f eventually (i. e., after some number of iterations) become periodic but are not themselves periodic then $J = \overline{\mathbb{C}}$.*

For Belyi functions, critical points are under control; namely, they are black and white vertices and face centers, though not all of them but only those of degree > 1. Sullivan himself gave the following example:

$$f(x) = \left(\frac{x-2}{x}\right)^2.$$

Incidentally, this is a Belyi function corresponding to the hypermap shown in Figure 18.

Let us read the trajectories of critical points without using the formula but only looking at the picture. There are only two critical points: the point 2 (a vertex of degree 2), and the point 0 (the center of the face of degree 2). The point 2, being a black vertex, by definition goes to 0. The point 0, being a face center, goes—also by definition—to ∞. The point ∞, being a white vertex, goes to 1. Finally, the point 1, being a white vertex, also goes to 1. Summing up, we obtain

$$2 \mapsto 0 \mapsto \infty \mapsto 1 \mapsto 1.$$

Thus 1 is a periodic point, and both critical points 2 and 0 go to 1 after some number of iterations. What is important is the fact that the point 1 itself is not critical: while being a vertex it is a vertex of degree 1. Hence, the requirement of the theorem is satisfied: no critical points are themselves periodic.

We would like to propose here one more example to Sullivan's theorem, see Figure 19. Our example is somewhat less explicit since we are unable to give an explicit expression of the rational function in question. Nevertheless, we may affirm that the conditions of the theorem are satisfied and that therefore this is a case of complete chaos.

Indeed, after the first application of the Belyi function all critical points go to 0, 1, and ∞. As before, we can easily follow the subsequent applications of this function to these three points; they give

$$1 \mapsto \infty \mapsto 0 \mapsto 0.$$

Thus, all critical points of this function after several iterations go to 0 which is a periodic point. However, this point, being a vertex of degree 1, is not itself critical. Qed.

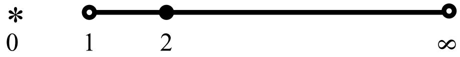


Figure 18. The hypermap corresponding to Sullivan's example.

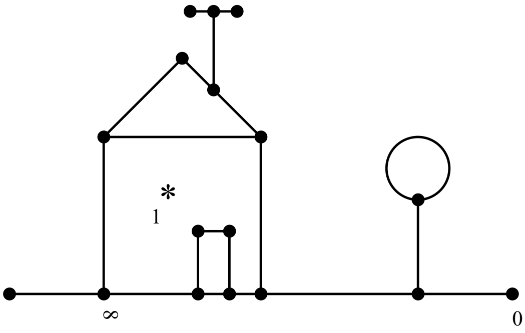


Figure 19. Iterations of the Belyi function corresponding to this "dessin d'enfant" create a dynamical system with a complete chaos.

We see that any hypermap having an element (a vertex or a face) of degree 1 permits to construct a similar example, quite often even several examples. In principle, it should be possible to study the behavior of the corresponding dynamical systems in a purely combinatorial and group-theoretic way, though there remain many obstacles to overcome. And, sure enough, such a study must be extended from Belyi functions to *postcritically finite* complex dynamical systems (see [11]) which are also *rigid* and therefore defined over $\overline{\mathbb{Q}}$.

7 NON-PLANAR CASE

We remind to the reader that for every genus $g \geq 1$ there are infinitely many non-isomorphic Riemann surfaces (all of them are homeomorphic to each other as topological surfaces). Therefore, for a bigger genus we must speak not about a Belyi function but about a *Belyi pair*.

Definition 7.1 (Belyi pair). A pair (X,f), where X is a Riemann surface and $f : X \to \overline{\mathbb{C}}$ is a meromorphic function on X, is called a *Belyi pair* if f is unramified outside the set $\{0, 1, \infty\} \subset \overline{\mathbb{C}}$.

In the same way as in the planar case, the preimage $f^{-1}([0, 1])$ is a hypermap embedded (in a very specific way) in the surface X. The preimages of 0 are its black vertices, the preimages of 1, white vertices, and the preimages of ∞ are the "face centers" (exactly one of them inside each face). Also as before, the multiplicities of these preimages correspond to the degrees of vertices or faces.

In the opposite direction, for any hypermap (of any genus) there exists a corresponding Belyi pair. Please, note: the hypermap specifies not only a Belyi function; it also specifies a Riemann surface on which this function is defined. But it is better to formulate a more general theorem.

There are two ways of representing Riemann surfaces. We may represent them as complex algebraic curves, i. e., sets of solutions of algebraic equations (one equation with two unknowns, or two equations with three unknowns, etc.). Or, otherwise, we may represent them as ramified coverings of the complex Riemann sphere $\overline{\mathbb{C}}$. In order to specify a ramified covering of degree n we must specify two sequences:

- a sequence of k ramification points $y_1, y_2, \ldots, y_k \in \overline{\mathbb{C}}$ (without any constraint imposed on them);
- a sequence of k permutations $g_1, g_2, \ldots, g_k \in \mathrm{S}_n$ which act transitively on n points and such that $g_1 g_2 \ldots g_k = 1$.

The permutations represent the *monodromy*: g_i shows how the preimage x goes from a sheet of the covering to another one when its image $y = f(x)$ makes a turn around y_i.

Theorem 7.2 (Riemann's existence theorem). *For any two sequences $y_1, y_2, \ldots, y_k \in \overline{\mathbb{C}}$ and $g_1, g_2, \ldots, g_k \in \mathrm{S}_n$ satisfying the above conditions, there exists a Riemann surface X and a meromorphic function $f : X \to \overline{\mathbb{C}}$ such that $y_1, y_2, \ldots, y_k$ are the ramification points (or, in another terminology, the critical values) of f, and $g_1, g_2, \ldots, g_k$ are the corresponding monodromy permutations. Such a Riemann surface is unique up to an automorphism.*

The surface X also does not change if we apply an automorphism of $\overline{\mathbb{C}}$, that is, a linear fractional transformation. Doing that, we can put once and for all the three last critical values y_{k-2}, y_{k-1}, y_k to the fixed positions 0, 1, and ∞. The covering now depends discretely on k permutations $g_1, g_2, \ldots, g_k$ (in fact, on $k - 1$ permutations since g_k can be computed out of $g_1, g_2, \ldots, g_{k-1}$), and it depends continuously on $k - 3$ complex parameters $y_1, y_2, \ldots, y_{k-3}$. Thus, the following question comes naturally:

Question 7.3. What happens when $k = 3$?

First, the case $k = 3$ corresponds to hypermaps, where $g_1 = \sigma$, $g_2 = \alpha$, $g_3 = \varphi$. Second, the covering becomes *rigid*: it does not have any continuous parameters and can change only discretely.

Is it possible to represent an arbitrary Riemann surface as a covering with only three ramification points? The answer is no, but the class of representable surfaces is the most interesting one. Namely, are representable in this way the surfaces *defined over* $\overline{\mathbb{Q}}$. The following theorem was proved by G. Belyi in 1979 [1]. Grothendieck [7] wrote about it: "I do not believe that a mathematical fact has ever struck me quite so strongly as this one, nor had a comparable psychological impact".

Theorem 7.4 (Belyi theorem). *A meromorphic function $f : X \to \overline{\mathbb{C}}$ unramified outside $\{0, 1, \infty\}$ exist if and only if the Riemann surface X is defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers. This means that X can be realized as an algebraic curve with all the equations having algebraic numbers as their coefficients. In this case, the function f is also defined over $\overline{\mathbb{Q}}$. This means that it can be realized as a rational function in variables defining X, with its coefficients being algebraic numbers.*

Thus, the absolute Galois group also acts on hypermaps of higher genera via its simultaneous action on X and f.

As for the computational aspect, the situation is hopeless. Generally, not only are we unable to solve the corresponding algebraic equations, most often we don't know how to write them down explicitly. We can only guarantee that such equations exist.

However, some very special cases can be solved. A beautiful example is given in the next section.

8 FERMAT CURVE

Consider the curve

$$F = \{(x:y:z) \mid x^n + y^n = z^n\} \subset \mathbb{C}\mathrm{P}^2$$

and its projection on the first coordinate given by

$$f : \mathbb{C}\mathrm{P}^2 \to \overline{\mathbb{C}} = \mathbb{C}\mathrm{P} : (x:y:z) \mapsto (x:z).$$

The function f is not defined for the points $x = z = 0$, $y \neq 0$, but, fortunately, these points do not belong to F. The point $\infty \in \overline{\mathbb{C}}$ is represented by $(x:0) \in \mathbb{C}\mathrm{P}$. Above this point, the equation $x^n + y^n = 0$ has n distinct solutions $(x:\zeta x)$ where ζ takes n values of $\sqrt[n]{-1}$.

Having stated that, we may now consider only the affine part of F, that is,

$$F^\circ = \{(x,y) \mid x^n + y^n = 1\} \subset \mathbb{C}^2$$

and its projection on the first coordinate given by

$$f : \mathbb{C}^2 \to \mathbb{C} : (x,y) \mapsto x.$$

For a fixed value of x, the equation $y^n = 1 - x^n$ considered as an equation on y, usually has n distinct solutions. The exceptions are the nth roots of unity: when $x = \sqrt[n]{1}$ the number of solutions for y is reduced to one. Therefore, f has n critical values, namely, the nth roots of unity. (As we have said before, ∞ is not a critical value of f since there are n distinct points of the curve F over ∞.)

Now, applying the function $g(x) = x^n$ we push all these critical values to 1, and create two new critical values: 0 and ∞. Therefore, the composition

$$h : F \xrightarrow{f} \overline{\mathbb{C}} \xrightarrow{g} \overline{\mathbb{C}} : (x,y) \mapsto x \mapsto x^n$$

is a Belyi function on F. Since $\deg f = n$ and $\deg g = n$, the degree of their composition $h = g \circ f$ is $\deg h = n^2$.

In this case, it is more interesting to consider not the preimage of the segment $[0, 1]$ but the preimage of the whole real line. More exactly, we mark the points 0, 1, and ∞ on $\overline{\mathbb{C}}$ by $\bullet$, $\circ$, and $*$, and join them by the segments $[0, 1]$, $[1, \infty]$, and $[\infty, 0]$. In this way we get a triangulation of the sphere, two triangular faces being the upper and the lower half-planes. Now, simple reasoning leads to the following results:

- The graph embedded in F has $3n$ vertices: n vertices of the type $\bullet$, n vertices of the type $\circ$, and n vertices of the type $*$.
- The degree of each vertex is $2n$; therefore, it is joined to every vertex of two other types. Hence, the graph on F is $K_{n,n,n}$, the complete tripartite graph.
- Except 0, 1, and ∞ (which are critical values of h), all other points of $\overline{\mathbb{C}}$ are "repeated" n^2 times on F. Therefore, the map on F has $3n^2$ edges and $2n^2$ faces.
- The genus of F can now be easily computed:

$$2 - 2g = 3n - 3n^2 + 2n^2 \;\Rightarrow\; g = \frac{(n-1)(n-2)}{2}.$$

- All faces of the map on F are triangles; therefore, this is an embedding of the least genus of the graph $K_{n,n,n}$.

The fact that the least possible genus of an embedding of the graph $K_{n,n,n}$ is equal to $(n - 1)(n - 2)/2$, was established by White in 1969 [17] and by Ringel and Youngs in 1970 [12]. They would have been very much amazed had they known that their work was related to the Fermat equation.

If, according to previous conventions, we consider the preimage of the segment $[0, 1]$, we obtain a hypermap which is a regular embedding of the complete bipartite graph $K_{n,n}$. The embeddings of complete bipartite graphs are thoroughly studied by Gareth Jones. The construction using the Fermat curve also belongs to him.

A more general construction. The above example is a very particular case of the following more general scheme. Let f and g be two planar Belyi functions. Here the word "planar" means that they are rational functions of one complex variable, and the hypermaps corresponding to them are planar. Let $\deg f = m$, $\deg g = n$. Consider the algebraic curve

$$X = \{(x, y) \mid f(x) = g(y)\}.$$

Then the function on X given by $h(x, y) = f(x)$ (or, equivalently, $h(x, y) = g(y)$ since $f(x) = g(y)$ on X) is a Belyi function.

Indeed, if $z \neq 0, 1, \infty$ then the equation $f(x) = z$ has m distinct solutions and the equation $g(y) = z$ has n distinct solutions; therefore, the curve X contains mn distinct points (x, y) for which $f(x) = g(y) = z$. Only for $z = 0, 1, \infty$ the number of solutions may become smaller. For the Fermat curve, $f(x) = x^n$ and $g(y) = 1 - y^n$.

What is even more interesting, the hypermap on X corresponding to the Belyi function h can be constructed combinatorially, using only the information about two planar hypermaps corresponding to f and g.

However, this direction is not yet properly explored.

Conclusion. We must finish this, already long but inevitably too short, exposition of Belyi functions, dessins d'enfants, and related topics. We would like to conclude it by the following remark: such a visibly simple object as a triple of permutations $(\sigma, \alpha, \varphi)$ acting transitively and satisfying the condition $\sigma\alpha\varphi = 1$ (or, if you prefer, just a pair of permutations (σ, α) acting transitively) leads to a great variety of interesting mathematical structures, namely:

- maps or hypermaps—with all their innumerable combinatorial properties extensively studied by many researchers;
- cartographic groups—with a possibility of a pictorial representation of groups, and with groups themselves being Galois invariants and character tables being a useful tool for enumeration and other things;
- Riemann surfaces—with the underlying notion of complex structure, with their representation as algebraic curves, etc.;
- number fields (finite extensions of $\mathbb{Q}$)—with the corresponding Galois groups and other properties.

Sure enough, all these structures are interrelated, and this is the most attractive quality of the subject. I often recall the phrase once told by Littlewood about Ramanujan, that every positive integer was one of his personal friends. I would say that working with dessins d'enfants leads to a sort of an intimate acquaintance with many maps, while other branches of map theory often tend to consider maps in huge herds whose members lack any individuality.

Acknowledgments. I was happy to plunge once again into the stimulating atmosphere of Com^{2}MaC during the conference "Applications of Group Theory to Combinatorics" (July 2007). I am grateful to the center director Professor Jin Ho Kwak and to all the conference organizers who gave me this opportunity to meet old friends and colleagues and to acquire new ones.

REFERENCES

[1] Belyi G.V. On Galois extensions of a maximal cyclotomic field.—*Mathematics USSR Izvestija*, vol. **14** (1980), no. 2, 247–256. (Original in Russian: *Izvestiya Akademii Nauk SSSR*, vol. **14** (1979), no. 2, 269–276.)

[2] Birch B.J., Chowla S., Hall M., Jr., Schinzel A. On the difference $x^3 - y^2$.—*Norske Vid. Selsk. Forh. (Trondheim)*, 1965, vol. **38**, 65–69.

[3] Conder M. The symmetric genus of the Mathieu groups.—*Bull. of the London Math. Soc.*, 1991, vol. **23**, no. 5, 445–453.

[4] Conway J.H., Curtis R.T., Norton S.P., Parker R.A., Wilson R.A. (With computational assistance from J.G. Thackray.) Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups.—Clarendon Press, Oxford, 1985, xxxiv+252 pp. (Reprinted in 2005 with corrections.)

[5] Cori R. Un code pour les graphes planaires et ses applications.—Astérisque, vol. **27**, 1975.

[6] Davenport H. On $f^3(t) - g^2(t)$.—*Norske Vid. Selsk. Forh. (Trondheim)*, 1965, vol. **38**, 86–87.

[7] Grothendieck A. Esquisse d'un programme (1984).—In: L. Schneps, P. Lochak, eds. "Geometric Galois Action. Vol. 1: Around Grothendieck's *Esquisse d'un Programme", London Math. Soc.* Lecture Notes Series, vol. **242**, Cambridge Univ. Press, 1997, 5–48. (English translation: "Scketch of a programme", the same volume, p. 243–284.)

[8] Klein F. Vorlesungen über das Ikosaeder und die Aflösung der Gleichungen vom fünften Grade.—Leipzig, 1884. Reprinted by Dover Publ.: **Klein F.** The Icosahedron and the Solution of Equations of the Fifth Degree, 1956.

[9] Lando S.K., Zvonkin A.K. Graphs on Surfaces and Their Applications.—Springer-Verlag, 2004.

[10] Magot N., Zvonkin A. Belyi functions for Archimedean solids.—*Discrete Math.*, 2000, vol. **217**, 249–271.

[11] Pilgrim K.M. Combinations of Complex Dynamical Systems.—Springer-Verlag, 2003 (Lecture Notes in Math., vol. **1827**).

[12] Ringel G., Youngs J.W.T. Das Geschlecht des symmetrischen vollständingen dreifärbbaren Graphen.—*Comm. Math. Helv.*, 1970, vol. **45**, 152–158.

[13] Ritt J.F. Prime and composite polynomials.—*Trans. Amer. Math. Soc.*, 1922, vol. **23**, no. 1, 51–66. (Errata: 1922, vol. **23**, no. 4, p. 431.)

[14] Ritt J.F. Permutable rational functions.—*Trans. Amer. Math. Soc.*, 1923, vol. **25**, no. 3, 399–448. (Errata: 1924, vol. **26**, no. 4, p. 494.)

[15] Stothers W.W. Polynomial identities and Hauptmoduln.—*Quart. J. Math. Oxford, ser. 2*, 1981, vol. **32**, no. 127, 349–370.

[16] Sullivan D. Quasiconformal homeomorphisms and dynamics. I: Solution of the Fatou–Julia problem on wandering domains.—*Ann. Math.*, 1985, vol. **122**, 401–418.

[17] White A.T. The genus of the complete tripartite graph $K_{mn,n,n}$.—*J. Combinat. Theory*, 1969, vol. **7**, 283–285.

[18] Zannier U. On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's Existence Theorem.—*Acta Arithmetica*, 1995, vol. **71**, no. 2, 107–137.

Author index

Applications of Group Theory to Combinatorics contains 11 survey papers from international experts in combinatorics, group theory and combinatorial topology. The contributions cover topics from quite a diverse spectrum, such as design theory, Belyi functions, group theory, transitive graphs, regular maps, and Hurwitz problems, and present the state-of-the-art in these areas.

Applications of Group Theory to Combinatorics will be useful in the study of graphs, maps and polytopes having maximal symmetry, and is aimed at researchers in the areas of group theory and combinatorics, graduate students in mathematics, and other specialists who use group theory and combinatorics.

Jack Koolen teaches at the Department of Mathematics at Pohang University of Science and Technology, Korea. His main research interests include the interaction of geometry, linear algebra and combinatorics, on which topics he published 60 papers.

Jin Ho Kwak is Professor at the Department of Mathematics at Pohang University of Science and Technology, Korea, where he is director of the Combinatorial and Computational Mathematics Center (Com^{2}MaC). He works on combinatorics and topology, mainly on covering enumeration related to Hurwitz problems and regular maps on surfaces, and published more than 100 papers in these areas.

Ming-Yao Xu is Professor at the Department of Mathematics at Peking University, China. The focus in his research is on finite group theory and algebraic graph theory, in particular on finite p-groups and the interaction of groups and graphs. Ming-Yao Xu published over 80 papers on these topics.

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
Schipholweg 107C
2316 XC Leiden, NL
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

ISBN 0415471842
9 780415 471848

an **informa** business