Séminaire Lotharingien de Combinatoire **56** (2006), Article B56a

CHARACTER THEORY OF SYMMETRIC GROUPS, ANALYSIS OF LONG RELATORS, AND RANDOM WALKS

THOMAS W. MÜLLER

Abstract. We survey a number of powerful recent results concerning diophantine and asymptotic properties of (ordinary) characters of symmetric groups. Apart from their intrinsic interest, these results are motivated by a connection with subgroup growth theory and the theory of random walks. As applications, we present an estimate for the subgroup growth of an arbitrary Fuchsian group, as well as a finiteness result for the number of Fuchsian presentations of such a group, the latter result solving a long-standing problem of Roger Lyndon's. We also sketch the proof of a well-known conjecture of Roichman's concerning the mixing time of random walks on finite symmetric groups, and of a result describing the parity of the subgroup numbers for a substantial class of one-relator groups.

Introduction

As is well known, representation theory has a number of applications in Probability Theory and in Statistics; examples include, for instance, estimates for the mixing time of random walks on finite groups and homogeneous spaces, analysis of partially ranked data, and the modelling of card shuffling. The monograph by Diaconis [11] covers these and other applications of a similar flavour.

What is needed for these applications is simply the ordinary character theory (over $\mathbb{C}$) of finite groups built up by Frobenius, Burnside, Schur and others since the late 1890s; and the version of ordinary representation theory of finite symmetric groups developed by Young and others since the late 1920s.

It would seem that, by now, the ordinary representation theory of finite symmetric groups is rather well understood. Nevertheless, recent years have seen a number of exciting developments and breakthroughs at the bottom of which lie distinct advances in our understanding of the characteristic zero representation theory of symmetric groups. Here, we shall concentrate on a number of powerful results concerning diophantine and asymptotic properties of characters of symmetric groups, recently obtained in a series of papers by the author in collaboration with J.-C. Schlage–Puchta; cf. [33], [34], [38], and [40]. Apart from their considerable intrinsic interest, these investigations are motivated by connections with the subgroup arithmetic of certain large groups (large in the sense of Pride [45]) and with the theory of random walks; it is this interplay between an improved and refined character theory of S_n (and, more generally, monomial groups) on the one hand, and the analysis of long relators and random walks on the other, which forms the main theme of the present paper.

The main new results concerning the asymptotics of character values and multiplicities established in [38] can be summarized as follows.

Theorem A. *Let $\varepsilon > 0$ and a positive integer q be given, suppose that n is sufficiently large, and let χ be an irreducible character of S_n.*

(1) *We have $|\chi(\mathbf{c})| \leq \big(\chi(1)\big)^{1-\delta}$ with*

$$\delta = \left(\big(1 - 1/(\log n)\big)^{-1} \frac{12 \log n}{\log(n/f)} + 18\right)^{-1},$$

where $\mathbf{c}$ is any conjugacy class of S_n with f fixed points.

(2) *We have*

$$\sum_{\substack{\pi \in S_n\\ \pi^q = 1}} |\chi(\pi)| \leq \big(\chi(1)\big)^{\frac{1}{q}+\varepsilon} \sum_{\substack{\pi \in S_n\\ \pi^q = 1}} 1.$$

(3) *Let $m_\chi^{(q)}$ be the multiplicity of χ in the q-th root number function of S_n. Then*

$$m_\chi^{(q)} \leq \big(\chi(1)\big)^{1-2/q+\varepsilon}.$$

All these bounds are essentially best possible. We remark that, in characteristic zero, estimates for character values and multiplicities are among the least understood topics in the representation theory of symmetric groups. In recent times, additional interest in this circle of problems was sparked by the theory of random walks on finite groups. In this context, the first part of Theorem A enables us to prove the following.

Theorem B. *Let $\mathbf{c}$ be a non-trivial conjugacy class in S_n. Denote by $t_{\mathrm{comb}}(\mathbf{c})$ the least even integer such that $t_c(\mathbf{c})$ elements chosen at random from $\mathbf{c}$ have, with probability $\geq 1 - \frac{1}{n}$, no common fixed point, and let $t_{\mathrm{stat}}(\mathbf{c})$ be the mixing time for the random walk generated by $\mathbf{c}$ (see the beginning of Section 5 for notions left undefined here). Then, for $n \geq 4000$, we have*

$$t_{\mathrm{comb}}(\mathbf{c}) \leq t_{\mathrm{stat}}(\mathbf{c}) \leq 10 t_{\mathrm{comb}}(\mathbf{c}).$$

Theorem B establishes in full generality a conjecture of Roichman; cf. [47, Conj. 6.6]. For special choices of $\mathbf{c}$, Roichman's conjecture had already been known to hold: Diaconis and Shahshahani [12] established it for transpositions, Roichman [47] generalized their result to conjugacy classes having at least cn fixed points, where c is some positive constant, and Fomin and Lulov [13] established a character bound implying Theorem C for conjugacy classes having only cycles of the same length. On the other hand, parts (2) and (3) of Theorem A allow us to derive an asymptotic estimate for the subgroup growth of Fuchsian groups; that is, groups Γ of the form

$$\Gamma = \Big\langle x_1, \ldots, x_r, y_1, \ldots, y_s, u_1, v_1, \ldots, u_t, v_t \;\Big|\; x_1^{a_1} = \cdots = x_r^{a_r} = x_1 \cdots x_r y_1^{e_1} \cdots y_s^{e_s} [u_1, v_1] \cdots [u_t, v_t] = 1 \Big\rangle \quad (1)$$

with integers $r, s, t \geq 0$ and $e_1, \ldots, e_s \geq 2$, and $a_1, \ldots, a_r \in \mathbb{N} \cup \{\infty\}$. ($\Gamma$ is a Fuchsian group in the most general sense met in the literature; cf., for instance, [25, Prop. 5.3] or [26, Sec: II.7]).

Theorem C. *Let Γ be a Fuchsian group such that*

$$\alpha(\Gamma) := \sum_i \Big(1 - \frac{1}{a_i}\Big) + \sum_j \frac{2}{e_j} + 2(t-1) > 0,$$

and let

$$\mu(\Gamma) = \sum_i \Big(1 - \frac{1}{a_i}\Big) + s + 2(t-1)$$

be the hyperbolic measure of Γ. Then the number $s_n(\Gamma)$ of index n subgroups in Γ satisfies an asymptotic expansion

$$s_n(\Gamma) \approx \delta L_\Gamma (n!)^{\mu(\Gamma)} \Phi_\Gamma(n) \Big\{ 1 + \sum_{\nu=1}^{\infty} a_\nu(\Gamma) n^{-\nu/m_\Gamma} \Big\}, \quad (n \to \infty).$$

Here,

$$\begin{aligned}
\delta &= \begin{cases} 2, & \forall i : a_i \text{ finite and odd}, \forall j : e_j \text{ even} \\ 1, & \text{otherwise}, \end{cases} \\
L_\Gamma &= (2\pi)^{-1/2 - \sum_i (1-1/a_i)} (a_1 \cdots a_r)^{-1/2} \exp\Bigg(- \sum_{\substack{i \\ 2 | a_i}} \frac{1}{2a_i} \Bigg), \\
\Phi_\Gamma(n) &= n^{3/2 - \sum_i (1-1/a_i)} \exp\Bigg(\sum_{i=1}^{r} \sum_{\substack{t | a_i \\ t < a_i}} \frac{n^{t/a_i}}{t} \Bigg), \\
m_\Gamma &= [a_1, a_2, \dots, a_r],
\end{aligned}$$

and the $a_\nu(\Gamma)$ are explicitly computable constants depending only on Γ.

Theorem C has a number of noteworthy consequences for the classification of Fuchsian groups; in particular it leads to the solution of a long standing problem, apparently first raised in an important special case by Hurwitz, and later brought to the forefront in its general form by Roger Lyndon during a meeting at IAS Princeton in 1968:

> *Can a (non-degenerate) Fuchsian group have infinitely many Fuchsian presentations* (*i.e., presentations of the form* (1) *above*)*?*

While it is not hard to give examples of Fuchsian groups of positive hyperbolic measure allowing for more than one presentation of the form (1), we are able to show that such a group has at most *finitely many* such presentations; cf. [38, Theorem 7] and Theorem 7 in Section 3 below.

A rather different note is struck by the earlier paper [34]; here, we are concerned with certain diophantine properties of character values and multiplicities, which appear to be both new and of independent interest. To be more specific, denote by φ the bijection between the self-conjugate partitions of n and the partitions of n into distinct odd parts, mapping a self-conjugate partition λ onto the partition given by the symmetric main hooks of λ. Moreover, denote by $\mathbf{c}_\lambda$ the conjugacy class of S_n whose cycle structure is given by the partition $\lambda \vdash n$, and by χ_λ the irreducible character of S_n corresponding to the Specht module S^λ. Finally, call an irreducible character χ of S_n *symmetric*, if $\chi = \epsilon_n \chi$, where $\epsilon_n = \chi_{(1^n)}$ is the sign character. (This is equivalent to demanding that the partition associated with χ be self-conjugate). Then the first part of [34] establishes the following.

Theorem D. (a) *Let λ_1 and λ_2 be partitions of n with λ_1 self-conjugate. Then $\chi_{\lambda_1}(\mathbf{c}_{\lambda_2})$ is odd if, and only if, $\lambda_2 = \varphi(\lambda_1)$.*

(b) *Let χ and χ' be irreducible characters of S_n. If both χ and χ' are symmetric, then the multiplicity $\langle \chi^2 | \chi' \rangle$ of χ' in χ^2 is odd if, and only if, $\chi = \chi'$.*

After introducing a certain rather substantial class $\mathcal{W}$ of relators, including in particular all surface relators

$$\prod_{1 \leq j \leq g} [x_{2j-1}, x_{2j}] \quad \text{and} \quad \prod_{1 \leq j \leq h} x_j^2,$$

the second part of [34], building on Theorem D as well as detailed information concerning the representation numbers of binary quadratic forms, establishes the following surprising and beautiful result.

Theorem E. *If w is in $\mathcal{W}$ and involves at least 3 generators, then the number of index n subgroups in the one-relator group defined by w is odd if, and only if, $n = k^2$ or $n = 2k^2$ for some $k \geq 1$.*

Our treatment here will cover Theorems A–E in some detail. This leaves out the asymptotic decomposition of the conjugacy representation and the estimate derived from it for the subgroup growth of a large class of groups, including in particular all one-relator groups with defining relation belonging to class $\mathcal{W}$, and all Fuchsian groups, as well as many other groups dominated by a long relation. These results, beginning with their actual statement, are rather technical, and seem altogether unsuitable for the purposes of a survey; for this topic, the reader is referred to the original paper [40].

Our article is organized as follows. In Section 1, we give a brief introduction to the subgroup growth theory of large groups. The purpose of this section is to provide the reader with some background for the analysis of long relators, which will form one of the main topics. In Section 2, we explain our character-theoretic approach to the subgroup growth of surface groups, originally developed in [33]. This is a first example to show how the solution of a problem in the ordinary representation theory of finite symmetric groups (here the asymptotic approximation of the sum $\sum_{\lambda \vdash n} \chi_\lambda(1)^{-s}$ for fixed real $s > 0$) leads to a result concerning the subgroup growth associated with a certain type of long relator. Proposition 4, which provides an asymptotic expansion for the number of index n subgroups in a large surface group, is essentially superseded by our corresponding result for Fuchsian groups (Theorem C), which will be presented, together with related results (including its representation-theoretic background) in Section 3. However, the main new idea how to apply character theory in the context of long relations occurs here for the first time and in a particularly transparent form, so that I thought it worthwhile to discuss this special case first.

Section 4 introduces the class of relators $\mathcal{W}$, and sketches a proof of Theorem E modulo Theorem D, while Section 5 discusses and sketches the proof of Theorem B.

The paper presents a somewhat extended version of a series of lectures given at the 56th Séminaire Lotharingien de Combinatoire, held 9–12 April 2006 in Ellwangen, Germany. It is my pleasure to thank Christian Krattenthaler and Volker Strehl for the invitation to give these lectures, and for inviting this report.

1. Counting subgroups of finite index in large groups

For a finitely generated group Γ, denote by $s_n(\Gamma)$ the number of index n subgroups of Γ. Subgroup growth theory, a thriving chapter in asymptotic group theory developed over the last 20 years by Grunewald, Lubotzky, Mann, Segal, and others including the present author, deals with number-theoretic properties of the sequence $\big\{s_n(\Gamma)\big\}_{n\geq 1}$ or related subgroup counting functions and their connection with the algebraic structure of the underlying group Γ. Here, we shall be concerned exclusively with *large* groups: a group is termed large (in the sense of Pride [45]), if it contains a subgroup of finite index which projects homomorphically onto a non-abelian free group. Clearly, for such a group, $s_n(\Gamma)$ grows at least as fast as the subgroup numbers of a free group of rank 2, but it is by no means true that $s_n(\Gamma)$ necessarily has *smooth* growth; in particular there need not exist an asymptotic formula for this function.[1]

As a first example, let us consider Marshall Hall's recurrence relation

$$s_n(F_r) = n(n!)^{r-1} - \sum_{\nu=1}^{n-1} \big((n-\nu)!\big)^{r-1} s_\nu(F_r) \tag{2}$$

for the subgroup numbers of a free group $G = F_r$ of rank r; cf. [15]. It is immediate from this relation that, for $r \geq 1$ and $n \geq 2$,

$$s_n(F_r) \equiv s_{n-1}(F_r) \bmod 2,$$

hence *the subgroup numbers of a non-trivial finitely generated free group are all odd.* With very little work (and almost no thought) one also extracts from (2) an asymptotic formula for the subgroup numbers of a non-abelian free group. Indeed, observe from (2) that

$$s_n(F_r) \leq n(n!)^{r-1}, \quad n \geq 1. \tag{3}$$

Assuming $r \geq 2$, and dividing (2) throughout by $n(n!)^{r-1}$, we then see that

$$\frac{s_n(F_r)}{n(n!)^{r-1}} = 1 - \epsilon(n, r),$$

[1] Cf. [37, Section 7] for an example in this direction.

where

$$\begin{aligned}\epsilon(n,r) &:= \sum_{\nu=1}^{n-1} \big((n-\nu)!\big)^{r-1}\, s_\nu(F_r) \,/\, \big(n(n!)^{r-1}\big)\\ &\leq \sum_{\nu=1}^{n-1} \frac{\nu}{n}\binom{n}{\nu}^{-(r-1)}\\ &\leq n^{-r} + \frac{n-1}{n^r} + \sum_{\nu=2}^{n-2}\binom{n}{\nu}^{-(r-1)}\\ &= n^{-r} + \frac{n-1}{n^r} + \mathcal{O}_r\big(n^{-2r+3}\big)\\ &= \mathcal{O}_r\big(n^{-1}\big),\end{aligned}$$

so

$$s_n(F_r) \sim n(n!)^{r-1} \quad (n \to \infty), \quad r \geq 2.$$

This is [41, Theorem 3]. Note that $1-r = \chi(F_r)$ is the Euler characteristic of the free group of rank r, so that the exponent of $n!$ in the last formula can be re-expressed as $-\chi(F_r)$. Non-abelian free groups and, more generally, finitely generated virtually free groups, i.e., fundamental groups $\Gamma = \pi_1(G(-),Y)$ of finite graphs of finite groups (in the sense of Bass and Serre), with $\chi(\Gamma) < 0$, are prototypes of large groups in the sense of Pride, and are typical examples of groups with fast subgroup growth. A prominent example of a virtually free group is the classical modular group

$$\Gamma = \mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3.$$

Here the corresponding results concerning parity and asymptotics are already quite non-trivial.

Proposition 1 [Stothers [51], 1977]. *Let $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ be the modular group. Then*

$$s_n(\Gamma) \equiv 1 \bmod 2 \iff n = 2^\alpha - 3 \text{ or } n = 2(2^\alpha - 3) \text{ for some } \alpha \geq 1.$$

Proposition 2 [Newman [41], 1976]. *For $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$,*

$$s_n(\Gamma) \sim (12\pi e^{1/2})^{-1/2}\, n^{n/6} \exp\Big(-\frac{n}{6} + n^{1/2} + n^{1/3} + \frac{1}{2}\log n\Big).$$

Note that, apart from correction terms coming from the torsion in the group, the right-hand side of the last formula looks like $(n!)^{-\chi(\Gamma)}$, where $\chi(\Gamma) = -\frac{1}{6}$ is the Euler characteristic (in the sense of Wall) of the modular group; cf. [6, Chapter IX]. This behaviour appears to be typical of large virtually free groups of smooth growth; cf. also Theorem 2 below, which provides further evidence in this direction.

We mention in passing that the kernel of the Cartesian map

$$\Gamma = \mathrm{PSL}_2(\mathbb{Z}) \to C_2 \times C_3 \cong C_6$$

is free of rank 2 (Nielsen [42], see also Lyndon [24]); hence, descending an index 6 along a cyclic group, we have managed to completely destroy the rather complex pattern exhibited by Stothers' result above. This indicates that, unlike growth, divisibility properties of subgroup counting functions tend to be severely distorted when deforming the underlying group over a commensurability class.

Here are two more recent results concerning free products.

Theorem 1 [Müller [31], 2003]. *Let $q \geq 3$ be an integer. Then q is a Fermat prime if, and only if,*

$$s_n(C_2 * C_q) \equiv 1 \bmod 2 \Longleftrightarrow n = \frac{2(q-1)^\alpha - q}{q-2}$$

$$\text{or } n = 2\left(\frac{2(q-1)^\alpha - q}{q-2}\right) \text{ for some } \alpha \geq 1.$$

Theorem 2 [Müller [27], 1996]. *Let $\Gamma = G_1 * \cdots * G_s * F_r$ be a free product with finite groups G_i, $m_i = |G_i|$, and suppose that $\chi(\Gamma) < 0$. Then*

$$s_n(\Gamma) \sim L_\Gamma\, \Phi_\Gamma(n) \quad (n \to \infty),$$

where

$$L_\Gamma := (2\pi)^{\frac{r-1}{2}}\, (m_1 \cdots m_s)^{-1/2} \exp\left(- \sum_{\substack{i \\ 2 | m_i}} \frac{\big(s_{G_i}(m_i/2)\big)^2}{2m_i} \right)$$

and

$$\Phi_\Gamma(n) := n^{-\chi(\Gamma)n} \exp\left(\chi(\Gamma)n + \sum_{i=1}^{s} \sum_{\substack{d_i | m_i \\ d_i < m_i}} \frac{s_{G_i}(d_i)}{d_i}\, n^{d_i/m_i} + \frac{r+1}{2} \log n \right).$$

As is well known, Fermat primes, that is, prime numbers of the form $2^{2^\lambda}+1$ with $\lambda \geq 0$, satisfy (or can even be characterized by) a number of curious regularity conditions; for instance, according to Gauß,[2] a regular p-gon ($p > 2$ a prime) can be constructed by compass and ruler if, and only if, p is a Fermat prime. Theorem 1 provides a new such characterization, within the set of integers ≥ 3, through the arithmetic of the associated (standard) Hecke group $\mathfrak{H}(q) \cong C_2 * C_q$, while at the same time representing the maximal generalization of Stothers' result (Proposition 1) for Hecke groups. Much more is known concerning divisibility properties of subgroup counting functions, but results tend to get quite technical; cf. [7], [30], [31], [32], and [36].

The second result gives an estimate for the subgroup growth of free products Γ of the form

$$\Gamma = G_1 * \cdots * G_s * F_r \quad (m_i = |G_i| < \infty,\, \chi(\Gamma) < 0) \tag{4}$$

in terms of the local data m_i and $s_{G_i}(d_i)$ for $d_i \mid m_i$. In fact, a full asymptotic expansion is known for $s_\Gamma(n)$ in this case, of which $L_\Gamma \Phi_\Gamma(n)$ is the main term; cf. [27, Theorem 1].

It appears that for virtually free groups Γ of more complicated structure (for instance, amalgamated products or HNN extensions) global invariants like $\chi(\Gamma)$ do not suffice to control the asymptotics of $s_n(\Gamma)$ (although they might still suffice to determine the growth type), and it is unclear, whether this function still exhibits smooth growth in

[2] Disquisitiones arithmeticae [14], §366.

such cases. In some mysterious way, the character theory of the finite stabilizers seems to come into the picture, but the situation is essentially not understood. However, there are other large groups, for instance one-relator groups, or Fuchsian groups.[3] What can we say about their subgroup growth? We shall come back to this question (which leads into our first main theme) shortly; but first let me explain how finite symmetric groups and, more generally, full monomial groups (i.e. groups of the form $H \wr S_n$ with a finite group H) enter our picture in an essential way.

For groups of super-exponential subgroup growth, no direct approach is known to the problem of counting finite index subgroups. Instead, one uses the transformation formula

$$\sum_{n\geq 0} \frac{|\operatorname{Hom}(\Gamma, S_n)|}{n!}\, z^n = \exp\left(\sum_{n\geq 1} \frac{s_n(\Gamma)}{n}\, z^n\right) \tag{5}$$

or, more generally, the equation

$$\sum_{n\geq 0} \frac{|\operatorname{Hom}(\Gamma, H\wr S_n)|}{n!}\, z^n = \exp\left(\sum_{n\geq 1} \frac{|H|^{n-1}s_n(\Gamma, H)}{n}\, z^n\right), \tag{6}$$

where

$$s_n(\Gamma, H) := \sum_{(\Gamma:\Delta)=n} |\operatorname{Hom}(\Delta, H)| \quad (H \text{ a finite group}).$$

We briefly sketch the proof of (5):[4] classify the Γ-actions on the standard n-set

$$[n] := \{1, 2, \dots, n\}$$

by the orbit ω_0 of the point 1. This orbit ω_0 may have any size k between 1 and n, and the Γ-action on ω_0 is transitive, while the action of Γ on $[n] \setminus \omega_0$ is arbitrary. Moreover, the transitive actions of Γ on $[n]$, modulo the (free) action of the stabilizer $\operatorname{stab}_\Gamma(1)$, are in one-to-one correspondence with the subgroups of index n in Γ. There are $\binom{n-1}{k-1}$ ways of choosing the elements of ω_0; and, on each such k-set, Γ has $(k-1)!s_k(\Gamma)$ transitive actions, hence

$$|\operatorname{Hom}(\Gamma, S_n)| = \sum_{1\leq k\leq n} \binom{n-1}{k-1}(k-1)!s_k(\Gamma)|\operatorname{Hom}(\Gamma, S_{n-k})|, \tag{7}$$

from which (5) follows. Note also that Marshall Hall's relation (2) is a special case of (7).

For a large group Γ, a function like $|\operatorname{Hom}(\Gamma, S_n)|$ tends to be more approachable than $s_n(\Gamma)$ itself, and there is machinery in place (see, for instance, Bender [4] and Wright [53], [54]) to transfer, say, asymptotic information from one side of the relations (5), (6) to the other. Henceforth, for the purposes of this survey, the problem of analyzing $s_n(\Gamma)$, the number of index n subgroups in Γ, will be identified with that of investigating the function $|\operatorname{Hom}(\Gamma, S_n)|$. No further mention will be made here of the more complicated case of monomial representations, apart from remarking that Formula (6), or rather the techniques underlying its proof, play a key role in the solution of the Poincaré-Klein

[3] By a result of Baumslag and Pride, a one-relator group having 3 or more generators is large; cf. [5]. The situation for Fuchsian groups is more involved, compare Theorem 4 in Section 3.

[4] Cf. [29] for the proof of (6), which is considerably more demanding.

Problem, one of the most important long-standing problems in pure mathematics; cf. [35] and [39].

Let us quickly come back to Theorem 2. For Γ as in (4), the function $|\operatorname{Hom}(\Gamma, S_n)|$ decomposes as

$$|\operatorname{Hom}(\Gamma, S_n)| = (n!)^r \prod_{i=1}^{s} |\operatorname{Hom}(G_i, S_n)|.$$

Thus, if we want to understand the asymptotics of $s_n(\Gamma)$ in this case, we have to investigate the function $|\operatorname{Hom}(G, S_n)|$, the number of G-actions on an n-set for large n, where G is an arbitrary *finite* group. In this situation, the transformation formula (5) yields

$$\sum_{n=0}^{\infty} \frac{|\operatorname{Hom}(G, S_n)|}{n!}\, z^n = \exp\left(\sum_{d|m} \frac{s_d(G)}{d}\, z^d\right), \quad m = |G|.$$

Hence, what we need is an asymptotic estimate for the Laurent coefficients of an entire function of the form $\exp(P(z))$, where $P(z)$ is a polynomial with real coefficients. What makes this problem hard is the (necessary) requirement that our estimates be completely explicit in the input data (the degree and coefficients of $P(z)$). Indeed, interpreted in this way, this problem is not well-posed, since the family of functions

$$\left\{e^{P(z)} :\ P(z) \in \mathbb{R}[z]\right\}$$

turns out to be too large to admit of a uniform asymptotics for its coefficients. Consequently, we have to study this question under suitable restrictions on the polynomial $P(z)$. In [28], among other things, the following is proved.

Theorem 3 [Müller [28], 1997]. *Let $P(z) = \sum_{\mu=1}^{m} c_\mu z^\mu$ be a polynomial of degree $m \geq 1$ with real coefficients c_μ. Set $\exp(P(z)) = \sum_{n=0}^{\infty} \alpha_n z^n$, and assume that* (i) *$\alpha_n > 0$ for sufficiently large n, and that* (ii) *$c_\mu = 0$ for $m/2 < \mu < m$. Then we have the asymptotic formula*

$$\alpha_n \sim \frac{K}{\sqrt{2\pi n}} \left(\frac{n}{mc_m}\right)^{-n/m} \exp\left(P\left(\left(\frac{n}{mc_m}\right)^{1/m}\right)\right), \tag{8}$$

where

$$K = K(P) = \begin{cases} m^{-1/2}, & m \text{ odd} \\ m^{-1/2} \exp\left(-\frac{c_{m/2}^2}{8c_m}\right), & m \text{ even} \end{cases}.$$

Theorem 3, in conjunction with [53, Theorem 3] or Bender's method [4], suffices in order to establish Theorem 2. Under more stringent conditions, we also obtain in [28] a full asymptotic expansion for α_n refining (8). The latter (much harder) result in turn leads to the improvement of Theorem 2 mentioned above. Thus, we see that Theorem 2 and its refinement are in fact complex analytic results.

2. Subgroup growth of surface groups

For elements x, y in a group Γ, we denote by

$$[x, y] = x^{-1}y^{-1}xy$$

the commutator of x and y. Let Γ be the fundamental group of a closed 2-manifold, that is, Γ equals

$$\Gamma_g^+ = \Big\langle x_1, y_1, \ldots, x_g, y_g \mid [x_1, y_1] \cdots [x_g, y_g] = 1 \Big\rangle$$

or

$$\Gamma_h^- = \Big\langle x_1, \ldots, x_h \mid x_1^2 \cdots x_h^2 = 1 \Big\rangle,$$

depending on whether or not the underlying manifold is orientable. These groups are large if, and only if, they have at least three generators, i.e.,

$$\Gamma_g^+ \text{ large} \Longleftrightarrow g \geq 2, \quad \Gamma_h^- \text{ large} \Longleftrightarrow h \geq 3.$$

The exceptional cases

$$\Gamma_1^+ \cong \mathbb{Z}^2,\ \Gamma_1^- \cong C_2,\ \Gamma_2^- \cong \mathbb{Z} \underset{2\mathbb{Z}}{*} \mathbb{Z}$$

are well understood; it is known that[5]

$$s_n(\Gamma_2^-) = s_n(\Gamma_1^+) = \sigma_1(n) := \sum_{d \mid n} d,$$

and, by a result of Gronwall,[6] $\sigma_1(n)$ has maximal order $e^\gamma n \log\log n$, where γ is Euler's (or Mascheroni's) constant, so the growth is indeed slow in these cases.

If we want to estimate the asymptotics of, say $s_n(\Gamma_g^+)$ for $g \geq 2$, we have to control the function

$$|\operatorname{Hom}(\Gamma_g^+, S_n)| = \Big|\Big\{(x_1, y_1, \ldots, x_g, y_g) \in S_n^{2g} :\ [x_1, y_1] \cdots [x_g, y_g] = 1\Big\}\Big|,$$

or, on a slightly more general level, the function

$$N_g^+(G, z) := \Big|\Big\{(x_1, y_1, \ldots, x_g, y_g) \in G^{2g} :\ [x_1, y_1] \cdots [x_g, y_g] = z\Big\}\Big|,$$

where G is a finite group, and $z \in G$. As a first step, consider the function

$$N_1^+(G, z) =: N^G(z) = \big|\big\{(x, y) \in G \times G :\ [x, y] = z\big\}\big|.$$

As is well known, the number of solutions of the equation $x \cdot y = z$ with x and y restricted to given (not necessarily distinct) conjugacy classes of G can be expressed in character-theoretic terms as follows:

$$\big|\big\{(x, y) \in G \times G :\ x \cdot y = z,\ x \in \mathbf{c}_1,\ y \in \mathbf{c}_2\big\}\big| = \frac{|\mathbf{c}_1| \cdot |\mathbf{c}_2|}{|G|} \sum_\chi \frac{\chi(\mathbf{c}_1)\chi(\mathbf{c}_2)\chi(z^{-1})}{\chi(1)}, \quad (9)$$

where χ runs through the ordinary irreducible characters of G; cf., for instance, [9, Proposition 9.33] or [20, Theorem 6.3.1]. Since $[x, y] = x^{-1} \cdot x^y$, where $x^y = y^{-1}xy$, we can obtain the solutions of the equation $[x, y] = z$ with x in a given conjugacy class $\mathbf{c}$ by first solving the equation $\bar{x} \cdot \bar{x}' = z$ with $\bar{x} \in \mathbf{c}^{-1}$ and $\bar{x}' \in \mathbf{c}$, and then choosing $y \in G$ in

$$|C_G(x)| = |G|/|\mathbf{c}|$$

[5] Cf., for instance, [33, Section 4.2].

[6] Trans. Amer. Math. Soc. 14 (1913), see also [16, Theorem 323].

ways to write a given $\bar{x}'$ as $\bar{x}' = x^y$ with $x = \bar{x}^{-1}$. Applying (9) and noting that $|\mathbf{c}| = |\mathbf{c}^{-1}|$, we see that

$$\begin{aligned}\left|\left\{(x,y) \in G \times G :\, [x,y] = z,\, x \in \mathbf{c}\right\}\right| &= \left|\left\{(\bar{x},\bar{x}') \in G \times G :\, \bar{x}\cdot\bar{x}' = z, \bar{x} \in \mathbf{c}^{-1}, \bar{x}' \in \mathbf{c}\right\}\right| \\ &\qquad \times |C_G(x)| \\ &= \frac{|G|}{|\mathbf{c}|}\,\frac{|\mathbf{c}|^2}{|G|}\sum_\chi \chi(\mathbf{c}^{-1})\chi(\mathbf{c})\chi(z^{-1})/\chi(1) \\ &= |\mathbf{c}|\sum_\chi \chi(\mathbf{c}^{-1})\chi(\mathbf{c})\chi(z^{-1})/\chi(1).\end{aligned}$$

Summing over the conjugacy classes gives

$$N^G(z) = \sum_{\mathbf{c}} |\mathbf{c}| \sum_\chi \chi(\mathbf{c}^{-1})\chi(\mathbf{c})\chi(z^{-1})/\chi(1).$$

Interchanging summations, and using the fact that characters are class functions plus their orthogonality, we find that

$$\begin{aligned}N^G(z) &= \sum_\chi \frac{\chi(z^{-1})}{\chi(1)} \sum_{\mathbf{c}} |\mathbf{c}|\,\chi(\mathbf{c}^{-1})\,\chi(\mathbf{c}) \\ &= \sum_\chi \frac{\chi(z^{-1})}{\chi(1)} \sum_{x\in G} \chi(x^{-1})\chi(x) \\ &= \sum_\chi \frac{\chi(z^{-1})}{\chi(1)}\,|G|\,\langle \chi \mid \chi\rangle \\ &= |G|\sum_\chi \chi(z^{-1})/\chi(1).\end{aligned}$$

Conjugating the resulting equation

$$N^G(z) = |G|\sum_\chi \chi(z^{-1})/\chi(1)$$

yields the formula

$$N^G(z) = |G|\sum_\chi \chi(z)/\chi(1). \tag{10}$$

We can now establish the character formula

$$N_g^+(G,z) = |G|^{2g-1}\sum_\chi \chi(z)/(\chi(1))^{2g-1} \tag{11}$$

by induction on g. If $g = 1$, then (11) holds in virtue of (10). Suppose that (11) holds for some $g \geq 1$. Then

$$\begin{aligned} N_{g+1}^+(G,z) &= \sum_{x\in G} N_g^+(G,x)\, N^G(x^{-1}z) \\ &= |G|^{2g} \sum_{x\in G} \Big[\sum_\chi \chi(x)/(\chi(1))^{2g-1}\Big]\Big[\sum_\chi \chi(x^{-1}z)/\chi(1)\Big] \\ &= |G|^{2g} \sum_{\chi_1,\chi_2} (\chi_1(1))^{-(2g-1)}(\chi_2(1))^{-1} \sum_{x\in G} \chi_1(x)\chi_2(x^{-1}z) \\ &= |G|^{2g+1} \sum_\chi \chi(z)/(\chi(1))^{2g+1}. \end{aligned}$$

In the last step, we have used the generalized orthogonality relation

$$\sum_{x\in G} \chi_1(x)\chi_2((ax)^{-1}) = |G|\, \chi_1(a^{-1})\, \langle \chi_1 \mid \chi_2\rangle/\chi_1(1)$$

with $a = z^{-1}$ (cf. [8, Formula 31.16]) together with orthogonality of characters. In a similar way, one shows that

$$\begin{aligned} N_h^-(G,z) &:= \Big|\Big\{(x_1,\dots,x_h) \in G^h :\, x_1^2\cdots x_h^2 = z\Big\}\Big| \\ &= |G|^{h-1} \sum_\chi c_\chi^h(G)\chi(z)/(\chi(1))^{h-1}, \end{aligned} \tag{12}$$

where the $c_\chi(G)$ are given by the expansion

$$R^G(z) := \Big|\Big\{x \in G :\, x^2 = z\Big\}\Big| = \sum_\chi c_\chi(G)\chi(z), \quad z \in G. \tag{13}$$

In general, R^G need not be a proper character; it is a virtual character of G, and the (integral) coefficients $c_\chi(G)$ in the Fourier decomposition (13) satisfy $|c_\chi(G)| \leq 1$ and are non-zero if, and only if, the corresponding character χ is real-valued. It is known that R^{S_n} is in fact the *model character* of S_n, that is,

$$R^{S_n}(z) = \sum_{\lambda\vdash n} \chi_\lambda(z), \quad z \in S_n. \tag{14}$$

The higher root number functions of S_n have more recently also been shown to be proper characters; cf. Scharf [49]. An alternative proof of Scharf's result using symmetric function theory is outlined in the solution to [50, Exercise 7.69 c]. A good account of all the facts on root number functions mentioned is found in [20, Chapter 6.2].

Setting $G = S_n$ and $z = 1$ in (11) and (12), and using (14), we obtain the equation

$$|\operatorname{Hom}(\Gamma_d, S_n)| = (n!)^{d-1}\Phi_{d-2}(n), \quad d \geq 1, \tag{15}$$

which summarizes the essence of our discussion so far. Here, Γ_d is a surface group (orientable or not) of rank d,[7] and, for fixed real s,

$$\Phi_s(n) := \sum_{\lambda \vdash n} \big(\chi_\lambda(1)\big)^{-s}.$$

It is clear from Equation (15), that information on the asymptotics of $s_n(\Gamma_d)$ with $d \geq 3$ will flow from a sufficiently precise estimate of the character sum $\Phi_s(n)$ for $s > 0$ as $n \to \infty$. Such an estimate is given by our next result.

Proposition 3 [Müller/Puchta [33], Theorem 1]. *For fixed $s > 0$, we have the asymptotic expansion*

$$\Phi_s(n) \approx 2 \sum_{\rho \geq 0} \mathcal{A}_\rho(s)\, n^{-\rho} \quad (n \to \infty).$$

Here, the coefficients $\mathcal{A}_\rho(s)$ are given by

$$\mathcal{A}_\rho(s) = \sum_{r \geq 0} \sum_{\mu \vdash r} H[\mu]^s \sum_{(\kappa_\nu)} \prod_{\nu \in N(\mu,r)} \left[\binom{s+\kappa_\nu-1}{\kappa_\nu}(2r-\nu)^{\kappa_\nu}\right], \quad \rho \geq 0,$$

where $H[\mu]$ is the hook product of μ,

$$N(\mu,r) := [2r] - \left\{ j + \sum_{i=0}^{j-1} m_{r-i}(\mu) :\ 1 \leq j \leq r \right\},$$

with $m_j(\mu)$ the multiplicity of j in the partition μ of r, and $\sum_{(\kappa_\nu)}$ denoting the sum over the family of discrete variables

$$\Big\{\kappa_\nu : \nu \in N(\mu,r)\Big\}$$

satisfying $\kappa_\nu \geq 0$ for $\nu \in N(\mu,r)$ and $\sum_\nu \kappa_\nu = \rho - rs$.

Observing that, for $1 \leq \rho < s$ and every $r \geq 0$, the summation over the κ_ν in the definition of the $\mathcal{A}_\rho(s)$ is empty, while $\mathcal{A}_0(s) = 1$, we obtain the following estimate, which will be used in Section 5.

Corollary 1. *For fixed $s > 0$, we have*

$$\Phi_s(n) = 2 + \mathcal{O}(n^{-s}), \quad n \to \infty.$$

Combining Proposition 3 with Bender's method [4] finally yields the following.

Proposition 4 [Müller/Puchta [33], Theorem 2]. *For $d \geq 3$, the function $s_n(\Gamma_d)$ satisfies the asymptotic expansion*

$$s_n(\Gamma_d) \approx 2n(n!)^{d-2} \left\{ 1 + \sum_{\nu \geq 1} \mathcal{C}_\nu(d) n^{-\nu} \right\} \quad (n \to \infty),$$

[7]The *rank* of a finitely generated group is, by definition, the minimal number of generators for this group.

where, for $\nu \geq 1$,

$$\mathcal{C}_\nu(d) = \sum_{k=1}^{\lfloor \frac{\nu}{d-2} \rfloor} \sum_{\eta_1+\cdots+\eta_{k-1}+\eta+\rho+k(d-2)=\nu} \mathfrak{c}_k(d)\, k^\eta \binom{\eta+\rho-1}{\eta} \mathcal{A}_\rho(d-2) \times \prod_{i=1}^{k-1} \left[i^{\eta_i} \binom{d+\eta_i-3}{\eta_i} \right],$$

and

$$\mathfrak{c}_k(d) = \left\langle \left(\sum_{n\geq 0} (n!)^{d-2}\, \Phi_{d-2}(n)\, z^n \right)^{-1} \,\middle|\, z^k \right\rangle.$$

3. Subgroup growth of Fuchsian groups

By a Fuchsian group we shall mean a group Γ having a presentation of the form[8]

$$\Gamma = \Big\langle x_1, \ldots, x_r, y_1, \ldots, y_s, u_1, v_1, \ldots, u_t, v_t \,\Big|\, x_1 \cdots x_r\, y_1^{e_1} \cdots y_s^{e_s}\, [u_1, v_1] \cdots [u_t, v_t] = x_1^{a_1} = x_2^{a_2} = \cdots = x_r^{a_r} = 1 \Big\rangle, \quad (16)$$

where r, s, t are non-negative integers, $e_1, \ldots, e_s$ are integers ≥ 2, and $a_1, \ldots, a_r \in \mathbb{N} \cup \{\infty\}$. If, for instance, $r = s = 0$, then $\Gamma = \Gamma_t^+$, while for $r = t = 0$ and $e_1 = \cdots = e_s = 2$ we have $\Gamma = \Gamma_s^-$. Another prominent class of examples are the (orientation preserving) hyperbolic triangle groups

$$\Delta(p, q, r) = \Big\langle x, y, z \,\Big|\, x^p = y^q = z^r = xyz = 1 \Big\rangle$$

with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

Here, $r = 3$, $s = t = 0$, $a_1 = p$, $a_2 = q$, and $a_3 = r$. For a Fuchsian group as in (16), we define the *hyperbolic measure* $\mu(\Gamma)$ of Γ via

$$\mu(\Gamma) := \sum_i \left(1 - \frac{1}{a_i}\right) + s + 2(t-1).$$

It can be shown that the hyperbolic measure is in fact an invariant of Γ, that is, independent of the Fuchsian presentation chosen for Γ, and one would expect $\mu(\Gamma)$ to play a role similiar to that played by the rational Euler characteristic $\chi(\Gamma)$ in the case of virtually free groups. We shall also need another invariant, first introduced in [38],

[8] Γ is a Fuchsian group in the most general sense met in the literature; cf., for instance, [25, Prop. 5.3] or [26, Sec. II.7].

which yields a rough measure for the size of the Fuchsian group Γ:

$$\begin{aligned}\alpha(\Gamma) &:= \sum_i \Big(1 - \frac{1}{a_i}\Big) \,+\, \sum_j \frac{2}{e_j} \,+\, 2(t-1)\\ &= \mu(\Gamma) \,-\, \sum_j \Big(1 - \frac{2}{e_j}\Big).\end{aligned}$$

Finally, we set $m_\Gamma := [a_1, a_2, \dots, a_r]$. The main result of this section provides an asymptotic estimate for the subgroup growth of large Fuchsian groups.

Theorem 4 [Müller/Schlage–Puchta [38, Theorem 3], 2002]. *Let Γ be as in* (16), *and suppose that $\alpha(\Gamma) > 0$. Then the number of index n subgroups in Γ satisfies an asymptotic expansion*

$$s_n(\Gamma) \approx \delta \hat{L}_\Gamma (n!)^{\mu(\Gamma)} \hat{\Phi}_\Gamma(n) \Big\{ 1 + \sum_{\nu \geq 1} a_\nu(\Gamma) n^{-\nu/m_\Gamma} \Big\}, \quad n \to \infty. \tag{17}$$

Here,

$$\delta = \begin{cases} 2, & \forall i : a_i \textit{ finite and odd}, \forall j : e_j \textit{ even}\\ 1, & \textit{otherwise}, \end{cases}$$

$$\hat{L}_\Gamma = (2\pi)^{-1/2 - \sum_i (1 - 1/a_i)} \Big(\prod_{a_i \neq \infty} a_i \Big)^{-1/2} \exp\Big(- \sum_{2 \mid a_i} \frac{1}{2a_i} \Big),$$

$$\hat{\Phi}_\Gamma(n) = n^{3/2 - \sum_i (1 - 1/a_i)} \exp\Bigg(\sum_i \sum_{\substack{d \mid a_i\\ d < a_i}} \frac{n^{d/a_i}}{d} \Bigg),$$

and the $a_\nu(\Gamma)$ are explicitly computable constants depending only on Γ.[9]

As in the case of Proposition 4, the proof of Theorem 4 begins by establishing a character formula for the function $|\operatorname{Hom}(\Gamma, S_n)|$ counting the permutation representations of Γ of degree n. (We remark in passing that, from a more philosophical point of view, this approach by means of a character formula for $|\operatorname{Hom}(\Gamma, S_n)|$ may be seen as a non-abelian and discrete analogue of the circle method, with the linear characters corresponding to the major arcs.)

Proposition 5 [38, Formula (38)]. *For Γ as in* (16), *we have*

$$|\operatorname{Hom}(\Gamma, S_n)| = (n!)^{s+2t-1} \prod_{i=1}^r |\operatorname{Hom}(C_{a_i}, S_n)| \sum_{\lambda \vdash n} \frac{\prod_{i=1}^r \alpha_{\chi_\lambda}^{(a_i)} \prod_{j=1}^s m_{\chi_\lambda}^{(e_j)}}{(\chi_\lambda(1))^{r+s+2t-2}}, \tag{18}$$

where, for $q \in \mathbb{N} \cup \{\infty\}$ and an irreducible character χ,

$$\alpha_\chi^{(q)} = \frac{1}{|\operatorname{Hom}(C_q, S_n)|} \sum_{\pi^q = 1} \chi(\pi),$$

[9]See [38, Sec. 5.2] for details concerning the computation of the coefficients $a_\nu(\Gamma)$.

and $m_\chi^{(q)} = \langle R_q^{S_n} \,|\, \chi \rangle$ *is the Fourier coefficient of* χ *in the expansion of the* q*-th root number function*

$$R_q^{S_n}(\pi) = \big|\{\sigma \in S_n : \sigma^q = \pi\}\big|$$

of S_n.

Proof. Let w be a segment of

$$R = x_1 x_2 \cdots x_r y_1^{e_1} y_2^{e_2} \cdots y_s^{e_s} [u_1, v_1][u_2, v_2] \cdots [u_t, v_t],$$

where powers $y_j^{e_j}$ and commutators $[u_k, v_k]$ are treated as single letters, and denote by $L(w)$ the formation length of w; that is, the number of letters (in the sense explained) comprising w. Given such a segment w and $\pi \in S_n$, define $N_w(\pi)$ to be the number of solutions of the equation $w = \pi$, subject to the conditions $x_i^{a_i} = 1$ for those i for which x_i occurs in w. Observing that $N_w(\pi)$ is a class function, define coefficients $\beta_\chi^{(w)}$ via the Fourier expansion

$$N_w(\pi) = (n!)^{-1} \prod_{x_i \in w} |\operatorname{Hom}(C_{a_i}, S_n)| \sum_{\chi \in \operatorname{Irr}(S_n)} \beta_\chi^{(w)} \chi(\pi).$$

We claim that

$$\beta_\chi^{(w)} = (n!)^{|\{j:\, y_j \in w\}| + 2|\{k:\, u_k \in w\}|} \prod_{x_i \in w} \alpha_\chi^{(a_i)} \prod_{y_j \in w} m_\chi^{(e_j)} \big/ \big(\chi(1)\big)^{\ell(w)-1}, \tag{19}$$

where $\ell(w)$ is the number of different generators x_i, y_j, u_k, v_k occurring in w. The proof of (19) is by induction on $L(w)$. If $L(w) = 1$, then (i) $w = x_1$ (subject to the condition $x_1^{a_1} = 1$), or (ii) $w = y_1^{e_1}$, or (iii) $w = [u_1, v_1]$, depending on whether $r > 0$, $r = 0$ and $s > 0$, or $r = s = 0$ and $t > 0$. In cases (ii) and (iii), we have $N_w = R_{e_1}^{S_n}$ or $N_w = N^{S_n}$, respectively, hence $\beta_\chi^{(y_1^{e_1})} = n!\, m_\chi^{(e_1)}$ respectively $\beta_\chi^{([u_1,v_1])} = (n!)^2/\chi(1)$ by the definition of the multiplicity $m_\chi^{(e_1)}$ respectively Formula (10), as predicted by (19). In case (i),

$$N_{x_1}(\pi) = \begin{cases} 1, & \pi^{a_1} = 1 \\ 0, & \pi^{a_1} \neq 1, \end{cases}$$

and Equation (19) requires us to verify the identity

$$\frac{1}{n!} \sum_\chi \sum_{\sigma^{a_1} = 1} \chi(\sigma)\, \chi(\pi) = \begin{cases} 1, & \pi^{a_1} = 1 \\ 0, & \pi^{a_1} \neq 1, \end{cases} \tag{20}$$

which however follows directly from the orthogonality relation[10]

$$\sum_\chi \chi(\mathbf{c}_1)\, \overline{\chi(\mathbf{c}_2)} = \frac{|G|}{|\mathbf{c}_1|}\, \delta_{\mathbf{c}_1, \mathbf{c}_2}. \tag{21}$$

Similarly, the induction step breaks into three cases, according to which type of letter x_i, $y_j^{e_j}$, or $[u_k, v_k]$ is adjoined. We shall give the argument in the case where the new

[10] Cf. [8, Formula (31.19)].

letter is x_i for some $2 \le i \le r$, the other two cases being similar but slightly easier. For $w' = wx_i$, we have

$$\begin{aligned}
N_{w'}(\pi) &= \sum_{\sigma\in S_n} N_w(\sigma) \times \begin{cases} 1, & (\sigma^{-1}\pi)^{a_i} = 1 \\ 0, & (\sigma^{-1}\pi)^{a_i} \neq 1, \end{cases} \\
&= \frac{1}{n!} \sum_{\sigma} N_w(\sigma) \sum_{\chi} \sum_{\tau^{a_i}=1} \chi(\tau)\, \chi(\sigma^{-1}\pi) \\
&= \frac{1}{n!} \sum_{\sigma} |\operatorname{Hom}(C_{a_i}, S_n)|\, N_w(\sigma) \sum_{\chi} \alpha_\chi^{(a_i)}\, \chi(\sigma^{-1}\pi) \\
&= \frac{\prod_{\nu=1}^{i} |\operatorname{Hom}(C_{a_\nu}, S_n)|}{(n!)^2} \sum_{\sigma} \sum_{\chi_1} \sum_{\chi_2} \alpha_{\chi_1}^{(a_i)}\, \beta_{\chi_2}^{(w)}\, \chi_1(\sigma^{-1}\pi)\, \chi_2(\sigma) \\
&= \frac{\prod_{\nu=1}^{i} |\operatorname{Hom}(C_{a_\nu}, S_n)|}{n!} \sum_{\chi_1} \sum_{\chi_2} \alpha_{\chi_1}^{(a_i)}\, \beta_{\chi_2}^{(w)}\, \frac{\chi_1(\pi)}{\chi_1(1)}\, \delta_{\chi_1,\chi_2} \\
&= \frac{\prod_{\nu=1}^{i} |\operatorname{Hom}(C_{a_\nu}, S_n)|}{n!} \sum_{\chi} \frac{\alpha_\chi^{(a_i)}\, \beta_\chi^{(w)}}{\chi(1)}\, \chi(\pi);
\end{aligned}$$

that is,

$$\beta_\chi^{(w')} = \frac{\alpha_\chi^{(a_i)}}{\chi(1)}\, \beta_\chi^{(w)} = \frac{\prod_{\nu=1}^{i} \alpha_\chi^{(a_\nu)}}{(\chi(1))^{i-1}},$$

in accordance with (19). Here, we have used (20) in step 2, the orthogonality relation[11]

$$\sum_{x_1\in G} \chi_1(x_2x_1)\, \overline{\chi_2(x_1)} = \frac{|G|\, \chi_1(x_2)}{\chi_1(1)}\, \delta_{x_1,x_2} \tag{22}$$

in step 5, and the inductive hypothesis in the concluding computation of $\beta_\chi^{(w')}$.

With (19) in hand, Equation (18) now follows by setting $w = R$ and $\pi = 1$. □

It is clear from Formula (18) that, in order to obtain asymptotic information concerning the function $|\operatorname{Hom}(\Gamma, S_n)|$ for a Fuchsian group Γ, we need an estimate for sums of the form

$$\sum_{\substack{\pi\in S_n \\ \pi^q=1}} \chi(\pi)$$

as well as a good upper bound on the multiplicities $m_\chi^{(q)}$ of root number functions. Our main new results in this direction are as follows.

Theorem 5 [Müller/Schlage–Puchta [38, Propositions 1 and 2(i)], 2002]. *Let $\varepsilon > 0$ and a positive integer q be given, and let χ be an irreducible character of S_n. Then, for sufficiently large n,*

[11]Cf. [8, Formula (31.16)].

(i)

$$\sum_{\substack{\pi\in S_n\\ \pi^q=1}} |\chi(\pi)| \;\leq\; \big(\chi(1)\big)^{\frac{1}{q}+\varepsilon} \sum_{\substack{\pi\in S_n\\ \pi^q=1}} 1,$$

(ii)

$$m_\chi^{(q)} \leq \big(\chi(1)\big)^{1-2/q+\varepsilon}.$$

It can be shown that both bounds given in Theorem 5 are in fact best possible. Applying Theorem 5 together with a number of auxiliary results, we obtain an asymptotic expansion for $|\operatorname{Hom}(\Gamma, S_n)|$ in the case where $\alpha(\Gamma) > 0$, that is, when Γ is large, and Theorem 4 follows from this expansion via Bender's method [4].

Theorem 4 has a number of noteworthy consequences for the classification of Fuchsian groups; in particular, it leads to the solution of a long standing problem, apparently first raised in an important special case by Hurwitz, and later brought to the forefront in its general form by Roger Lyndon during a meeting at IAS Princeton in 1968:

Can a (non-degenerate) Fuchsian group have infinitely many Fuchsian presentations?

Indeed, it is not hard to give examples of Fuchsian groups of positive hyperbolic measure allowing for more than one presentation of the form (16).

Call two finitely generated groups Γ and Δ *equivalent*, denoted $\Gamma \sim \Delta$, if

$$s_n(\Gamma) = \big(1 + o(1)\big)\, s_n(\Delta), \quad n \to \infty.$$

In [27, Theorem 3] a characterization in terms of structural invariants is given for the equivalence relation $\sim$ on the class of groups Γ of the form (4), and it is shown that each $\sim$-class decomposes into finitely many isomorphism classes. Our next result is concerned with the corresponding problem for Fuchsian groups. Denote by $\mathcal{F}$ the class of all groups Γ having a presentation of the form (16) with $\alpha(\Gamma) > 0$, and by $\cong$ isomorphy of groups.

Theorem 6 [Müller/Schlage–Puchta [38, Theorem 6(ii) and Corollary 2], 2002].

(i) *Let*

$$\Gamma = \Big\langle x_1, \ldots, x_r, y_1, \ldots, y_s, u_1, v_1, \ldots, u_t, v_t \;\Big|\; x_1 \cdots x_r\, y_1^{e_1} \cdots y_s^{e_s}\, [u_1, v_1] \cdots [u_t, v_t] = x_1^{a_1} = \cdots = x_r^{a_r} = 1 \Big\rangle$$

and

$$\Delta = \Big\langle x_1, \ldots, x_{r'}, y_1, \ldots, y_{s'}, u_1, v_1, \ldots, u_{t'}, v_{t'} \;\Big|\; x_1 \cdots x_{r'}\, y_1^{e'_1} \cdots y_{s'}^{e'_{s'}}\, [u_1, v_1] \cdots [u_{t'}, v_{t'}] = x_1^{a'_1} = \cdots = x_{r'}^{a'_{r'}} = 1 \Big\rangle$$

be Fuchsian groups such that $\alpha(\Gamma), \alpha(\Delta) > 0$. *Then we have* $\Gamma \sim \Delta$ *if, and only if,*

(a) *the multisets* $\{a_i : 1 \leq i \leq r\}$ *and* $\{a'_i : 1 \leq i \leq r'\}$ *coincide,*
(b) $\mu(\Gamma) = \mu(\Delta)$,
(c) $\delta = \delta'$.

(ii) *Let* Γ *be a Fuchsian group as in* (16) *with* $\alpha(\Gamma) > 0$. *Then the set*

$$\{\Delta \in \mathcal{F} : \Delta \sim \Gamma\}/\cong$$

is finite if, and only if, one of the following holds:

(a) $s = t = 0$,
(b) $s = 1$, $t = 0$, $\sum_i \left(1 - \frac{1}{a_i}\right) < 2$,
(c) $s = 2t = 2$, $r = 1$.

(iii) *Let* Γ *be as in* (ii). *Then the set*

$$\big\{\Delta \in \mathcal{F} : \Delta \sim \Gamma\big\}/\cong$$

is infinite, while the set

$$\big\{\Delta \in \mathcal{F} : s_n(\Delta) = \big(1 + \mathcal{O}(n^{-2\mu(\Gamma)})\big)\, s_n(\Gamma)\big\}/\cong$$

is finite if, and only if, the following three conditions are satisfied:

(a) $s + 2t + \sum_i \left(1 - \frac{1}{a_i}\right) \geq 3$,
(b) a_i *is odd for* $1 \leq i \leq r$,
(c) $e_j = 2$ *for* $1 \leq j \leq s$ *with at most one exception, and for the exceptional index* j_0 *(if it occurs), we have* $e_{j_0} = 2^{p-1}$ *for some prime* p.

It follows in particular from Theorem 6 that, unlike the situation for free products (4), the asymptotic class of the function $s_n(\Gamma)$ does not in general determine Γ up to finitely many isomorphism types. On the other hand, part (iii) of that theorem indicates that a finiteness result may perhaps be obtained by increasing the precision with which we measure the asymptotic behaviour of $s_n(\Gamma)$. It is therefore natural to ask, what happens if we take into account the full precision of (17) in Theorem 4. More specifically, consider three refinements of the equivalence relation $\sim$: (i) the relation $\approx$ of *strong equivalence* defined via

$$\Gamma \approx \Delta :\Longleftrightarrow s_n(\Gamma) = s_n(\Delta)\big(1 + \mathcal{O}(n^{-A})\big) \text{ for every } A > 0,$$

(ii) isomorphy, and (iii) equality of the system of parameters

$$(r, s, t; a_1, a_2, \ldots, a_r, e_1, e_2, \ldots, e_s)$$

in the Fuchsian presentation (16), denoted $\Gamma = \Delta$.[12] Clearly,

$$\Gamma = \Delta \implies \Gamma \cong \Delta \implies \Gamma \approx \Delta \implies \Gamma \sim \Delta.$$

It can be shown that all these implications are in fact strict. With this notation, we now have the following important result, which in particular settles Lyndon's problem mentioned above.

Theorem 7 [Müller/Schlage–Puchta [38, Theorem 7], 2002]. *Each* $\approx$*-equivalence class of* $\mathcal{FP}$ *decomposes into finitely many classes with respect to the relation* $=$; *that is, each*

[12]Strictly speaking, all these equivalence relations are now defined on the set $\mathcal{FP}$ of Fuchsian presentations (in the sense of (16)) with $\alpha > 0$.

group $\Gamma \in \mathcal{F}$ has only finitely many presentations of the form (16), *and is $\approx$-equivalent to at most finitely many non-isomorphic $\mathcal{F}$-groups.*

4. Parity patterns in one-relator groups

4.1. **The result.** We shall work over the alphabet

$$\mathcal{A} = \Big\{x_1, x_2, \dots, x_1^{-1}, x_2^{-1}, \dots\Big\}.$$

Define a class of words $\mathcal{W}$ over $\mathcal{A}$ by the following rules.

(i) $x_j^2, [x_j, x_k] \in \mathcal{W}$ for $j, k \geq 1$ and $j \neq k$.
(ii) If $w_1, w_2 \in \mathcal{W}$ have no generator in common, then $w_1 w_2 \in \mathcal{W}$.
(iii) If $v \in \mathcal{W}$, and x_j is a generator not occurring in v, then $[v, x_j] \in \mathcal{W}$.
(iv) $\mathcal{W}$ is the smallest set of words over $\mathcal{A}$ satisfying (i), (ii), and (iii).

Clearly, all surface group relators

$$\prod_{j=1}^{g} [x_{2j-1}, x_{2j}] \quad \text{and} \quad \prod_{j=1}^{h} x_j^2, \quad g, h \geq 1$$

are contained in $\mathcal{W}$, as is for instance the word $w = [x_1^2 x_2^2, x_3]$. For a word $w = w(x_1, \dots, x_d)$ over $\mathcal{A}$ involving the generators $x_1, \dots, x_d$, define the one-relator group Γ_w *associated with* w via

$$\Gamma_w = \Big\langle x_1, \dots, x_d \,\Big|\, w(x_1, \dots, x_d) = 1 \Big\rangle.$$

Then we have the following surprising result.

Theorem 8 [Müller/Puchta [34, Theorem 1], 2003]. *If w is in $\mathcal{W}$ and involves at least three generators, then $s_n(\Gamma_w)$ is odd if, and only if, $n = k^2$ or $n = 2k^2$ for some $k \geq 1$; in particular, all groups Γ_w with $w \in \mathcal{W}$ involving three or more generators share the same parity pattern, and $s_n(\Gamma_w)$ is multiplicative modulo* 2.

It appears likely that Theorem 8 is best possible in the sense that if, for some word w over $\mathcal{A}$ the function $s_n(\Gamma_w)$ displays the parity pattern described in Theorem 8, then in fact $w \in \mathcal{W}$.

4.2. **Some background: A recurrence relation modulo 2, Euler's pentagonal theorem, and the parity of the partition function.** The key to Theorem 8 lies in a remarkable recurrence relation for the mod 2 behaviour of $s_n(\Gamma_w)$ with $w \in \mathcal{W}$.

Proposition 6 [Müller/Puchta [34, Theorem 3], 2003]. *Let $w \in \mathcal{W}$ be a word involving three or more generators. Then, modulo* 2,

$$s_n(\Gamma_w) \equiv \sum_{\substack{k \geq 1 \\ k(k+1) < 2n}} s_{n - \frac{1}{2}k(k+1)}(\Gamma_w) \, + \, \delta(n), \quad n \geq 1, \tag{23}$$

where

$$\delta(n) = \begin{cases} 1, & n \textit{ odd and triangular} \\ 0, & \textit{otherwise.} \end{cases}$$

The background of Proposition 6 is representation-theoretic, and will be discussed below. Here, let me digress for a moment, and explain why, with Proposition 6 in hand, Theorem 8 nevertheless almost would have remained undiscovered.

Looking at Equation (23), which descends in triangular numbers, one cannot help but feel reminded of Euler's pentagonal theorem

$$\prod_{n\geq 1}(1-q^n) = 1 + \sum_{k\geq 1}(-1)^k q^{\frac{1}{2}k(3k-1)}(1+q^k) = \sum_{k=-\infty}^{\infty}(-1)^k q^{\frac{1}{2}k(3k-1)},$$

which yields the recurrence relation

$$p(n) = \sum_{k\geq 1}(-1)^{k+1}\Big\{p\Big(n-\frac{1}{2}k(3k-1)\Big) + p\Big(n-\frac{1}{2}k(3k+1)\Big)\Big\}, \quad n \geq 1$$

for the partition function $p(n)$, with the convention that $p(n) = 0$ for $n < 0$; cf. [1, Chapter 1.3]. However, while $p(n)$ is known to satisfy a number of congruences (for instance modulo 5, 7, and 11) when n is in certain arithmetic progressions[13], there do not seem to be any such congruences modulo 2 and 3. In fact, the parity of $p(n)$ appears to be quite random, and, on the basis of extensive numerical evidence, it is believed that the partition function is 'about equally often' even and odd; that is, that

$$\sum_{\substack{n\leq x\\ p(n)\equiv 0\,(2)}} 1 \;\sim\; \frac{x}{2} \quad (x\to\infty);$$

cf. [46]. Subbarao [52] has conjectured that, for any arithmetic progression $r\ (\mathrm{mod}\ t)$, there are infinitely many integers $m \equiv r\,(t)$ for which $p(m)$ is odd, and also infinitely many integers $n \equiv r\,(t)$ for which $p(n)$ is even. Partial results in this direction have been obtained by Ono [44]. Recently, Nicolas, Ruzsa, and Sárközy [43] have shown that, for all r and t,

$$x^{-\frac{1}{2}} \sum_{\substack{n\leq x\\ n\equiv r\,(t)\\ p(n)\equiv 0\,(2)}} 1 \;\to\; \infty \quad \text{as } x\to\infty.$$

In an appendix to the latter paper, Serre shows that the same type of result holds in fact for the coefficients of arbitrary modular forms. Against this background, Theorem 8 appears highly surprising. Once conjectured however, it can be established by induction on n, using the recurrence relation (23) together with classical results of Gauß and Legendre concerning the representation numbers of binary quadratic forms; cf. [14, § 205], [23], [10, Chapter VI.8], and [17, Satz 89].

[13]Cf. [21] for a comprehensive account up to 1970 concerning divisibility properties of $p(n)$. Some exciting recent developments in this area are described in [2] and [3].

4.3. **Some representation theory.** The proof of Proposition 6 depends on certain parity properties of character values and multiplicities for symmetric groups, which appear to be both new and of independent interest. Given a word $w = w(x_1, \ldots, x_d)$ over the alphabet $\mathcal{A}$ involving the generators $x_1, \ldots, x_d$, and an irreducible character χ of S_n, define complex numbers $\alpha_\chi(w)$ by means of the Fourier expansion

$$\begin{aligned} N_w(\sigma) &= \Big|\Big\{(\sigma_1, \ldots, \sigma_d) \in S_n^d :\, w(\sigma_1, \ldots, \sigma_d) = \sigma\Big\}\Big| \\ &= (n!)^{d-1} \sum_\chi \alpha_\chi(w)\chi(\sigma), \quad \sigma \in S_n, \end{aligned}$$

where the sum is taken over the set $\mathrm{Irr}(S_n)$ of all irreducible characters χ of S_n. Note that $N_w(\sigma)$ is a class function, thus the coefficients $\alpha_\chi(w)$ are well defined. Applying standard results from the representation theory of symmetric groups, it is not difficult to establish the following information concerning the $\alpha_\chi(w)$, leading to the explicit computation of these coefficients for each word $w \in \mathcal{W}$ and all $\chi \in \mathrm{Irr}(S_n)$.

Lemma 1 [34, Lemma 1]. *Let w_1, w_2, v be words over $\mathcal{A}$, and let χ be an irreducible character of S_n.*

(i) *We have $\alpha_\chi(x_j^2) = 1$ and $\alpha_\chi([x_j, x_k]) = \frac{1}{\chi(1)}$ for all $j, k \geq 1$ and $j \neq k$.*
(ii) *If w_1 and w_2 have no generator in common, then*

$$\alpha_\chi(w_1 w_2) = \frac{\alpha_\chi(w_1)\, \alpha_\chi(w_2)}{\chi(1)}.$$

(iii) *If x_j does not occur among the generators of v, then*

$$\alpha_\chi([v, x_j]) = \frac{1}{\chi(1)} \sum_{\chi' \in \mathrm{Irr}(S_n)} \alpha_{\chi'}(v)\, \langle \chi^2 \mid \chi' \rangle.$$

Indeed, (i) simply restates the fact that the square root function is the model character of S_n, as well as Equation (10), the character formula for the function N^G; and parts (ii) and (iii) also follow by arguments much in the spirit of Section 2.

Denote by φ the bijection between the self-conjugate partitions of n and the partitions of n into distinct odd parts, mapping a self-conjugate partition λ onto the partition given by the symmetric main hooks of λ. For example,

$$\varphi(6, 5, 4, 3, 2, 1) = (11, 7, 3).$$

Furthermore, denote by $\mathbf{c}_\lambda$ the conjugacy class of S_n whose cycle structure is given by the partition $\lambda \vdash n$, and by χ_λ the irreducible character of S_n corresponding to the Specht module S^λ. Then an inductive argument based on the Murnaghan-Nakayama rule enables one to prove the following result.[14]

Lemma 2 [34, Lemma 2]. *Let λ_1 and λ_2 be partitions of n, with λ_1 self-conjugate. Then $\chi_{\lambda_1}(\mathbf{c}_{\lambda_2})$ is odd if, and only if, $\lambda_2 = \varphi(\lambda_1)$.*

[14]Note that the Murnaghan-Nakayama rule implies in particular that characters of S_n are integer-valued. A more elementary argument uses the fact that, for all $\sigma \in S_n$ and exponents a coprime to the order of σ, the permutations σ and σ^a are conjugate.

Call an irreducible character χ of S_n *symmetric*, if $\chi = \epsilon_n\chi$, where $\epsilon_n = \chi_{(1^n)}$ is the sign character; this is equivalent to demanding that the partition associated with χ be self-conjugate. Lemma 2 thus describes the parity of any symmetric character of S_n. A rather subtle argument in the GF(2)-algebra

$$\mathfrak{A} = \mathrm{GF}(2)[\mathrm{Irr}(S_n)]$$

generated by the irreducible characters of S_n, building heavily on Lemma 2, now establishes the following.

Lemma 3 [34, Lemma 3]. *Let χ and χ' be irreducible characters of S_n.*

(i) *If χ is symmetric, then $\langle \chi^{2^k} | \chi' \rangle = \langle \chi^{2^k} | \epsilon_n\chi' \rangle$ for all k.*
(ii) *If both χ and χ' are symmetric, then $\langle \chi^2 | \chi' \rangle$ is odd if, and only if, $\chi = \chi'$.*

Call an irreducible character χ of S_n a 2-*core* character, if $n!/\chi(1)$ is odd. Note that, since the dimension of an ordinary irreducible representation of a finite group G always divides the order of $G/\mathrm{centre}(G)$, this concept is well defined for arbitrary finite groups; cf. [19] or [18, Chapter V, Satz 17.10]. For $G = S_n$, the hook formula shows that an irreducible character χ_λ is 2-core if, and only if, all hook lengths of the associated partition λ are odd. The last condition is easily seen to be equivalent to requiring that λ is of the form $\triangle = (k, k-1, \dots, 1)$ for some $k \geq 1$. It follows that S_n has a 2-core character if, and only if, $n = \frac{1}{2}k(k+1)$ is a triangular number, in which case $\chi_\triangle$ is the unique 2-core character; in particular, the 2-core character is symmetric. With these preliminaries, we are now in a position to establish the following result (a special case of [34, Lemma 4]), which is the decisive tool in proving Proposition 6.

Lemma 4. *Let $w \in \mathcal{W}$ be a word involving d generators, and let χ be an irreducible character of S_n.*

(i) *If $d \geq 2$, then $(n!)^{d-2}\chi(1)\alpha_\chi(w)$ is an integer.*
(ii) *If $d \geq 3$ and χ is not 2-core, then $(n!)^{d-2}\chi(1)\alpha_\chi(w)$ is even.*
(iii) *If $d \geq 2$ and χ is 2-core, then $(n!)^{d-2}\chi(1)\alpha_\chi(w)$ is odd.*

Proof. Using Lemma 1, we see by induction on d that $(\chi(1))^{d-1}\alpha_\chi(w)$ is integral for $d \geq 1$, each irreducible character χ, and every word $w \in \mathcal{W}$, which implies (i). Moreover, if χ is not 2-core, then $n!/\chi(1)$ is even, hence, for $d \geq 3$,

$$(n!)^{d-2}\chi(1)\alpha_\chi(w) = \left(\frac{n!}{\chi(1)}\right)^{d-2} \big(\chi(1)\big)^{d-1}\alpha_\chi(w)$$

is even, whence (ii). Now suppose that $\chi = \chi_\triangle$ is 2-core. We want to show that in this case $(\chi_\triangle(1))^{d-1}\alpha_{\chi_\triangle}(w)$ is odd. This is done by induction on the formation length of words in $\mathcal{W}$. By Lemma 1 (i), our claim holds for $w = x_j^2$ and $w = [x_j, x_k]$. Assume that our claim is true for words $w_1, w_2 \in \mathcal{W}$ having no generator in common, let d_i be the number of generators involved in w_i, and consider the word $w = w_1w_2$. Then w involves $d = d_1 + d_2$ generators, and by part (ii) of Lemma 1,

$$\big(\chi_\triangle(1)\big)^{d-1}\alpha_{\chi_\triangle}(w) = \big(\chi_\triangle(1)\big)^{d_1-1}\alpha_{\chi_\triangle}(w_1) \cdot \big(\chi_\triangle(1)\big)^{d_2-1}\alpha_{\chi_\triangle}(w_2),$$

which is odd, since by assumption both factors $(\chi_\triangle(1))^{d_i-1}\alpha_{\chi_\triangle}(w_i)$ are odd. Thus, it remains to show that our claim holds for $w = [v, x_j]$, provided it is true for $v \in \mathcal{W}$, and x_j does not occur in v. By Lemma 1 (iii),

$$\big(\chi_\triangle(1)\big)^{d-1}\alpha_{\chi_\triangle}(w) = \big(\chi_\triangle(1)\big)^{d-2}\sum_{\chi'}\alpha_{\chi'}(v)\big\langle\chi_\triangle^2\,\big|\,\chi'\big\rangle.$$

Now we distinguish the cases $d \geq 3$ and $d = 2$. If $d \geq 3$ and χ' is not 2-core, then $(\chi'(1))^{d-2}\alpha_{\chi'}(v)$ is integral, and $\chi_\triangle(1)$ is divisible by a higher power of 2 than $\chi'(1)$. Hence, the terms in the last sum not coming from the 2-core character $\chi_\triangle$ sum to an even integer, and we have

$$\big(\chi_\triangle(1)\big)^{d-1}\alpha_{\chi_\triangle}(w) \equiv \big(\chi_\triangle(1)\big)^{d-2}\alpha_{\chi_\triangle}(v)\big\langle\chi_\triangle^2\,\big|\,\chi_\triangle\big\rangle \bmod 2.$$

By assumption, $(\chi_\triangle(1))^{d-2}\alpha_{\chi_\triangle}(v)$ is odd, as is the multiplicity $\big\langle\chi_\triangle^2\big|\chi_\triangle\big\rangle$ by Lemma 3 (ii). Hence, $(\chi_\triangle(1))^{d-1}\alpha_{\chi_\triangle}(w)$ is odd, and the induction on formation length is complete in this case. It remains to deal with the case where $d = 2$. Then $w = \big[x_j^2, x_k\big]$ for some $j \neq k$, and, by Lemma 1 parts (i) and (iii),

$$\chi_\triangle(1)\alpha_{\chi_\triangle}(w) = \sum_{\chi'}\big\langle\chi_\triangle^2\,\big|\,\chi'\big\rangle.$$

By Lemma 3 (i) for $k = 1$, the right-hand side is congruent modulo 2 to

$$\sum_{\substack{\lambda\vdash n\\ \lambda=\lambda'}}\big\langle\chi_\triangle^2\,\big|\chi_\lambda\big\rangle,$$

which is odd by part (ii) of this lemma. □

With Lemma 4 in hand, we can now establish Proposition 6. Let $w \in \mathcal{W}$ be a word involving $d \geq 3$ generators. By the transformation formula (7), the subgroup numbers $s_n(\Gamma_w)$ are related to the sequence $h_n(\Gamma_w) := |\operatorname{Hom}(\Gamma_w, S_n)|/n!$ via the equation

$$nh_n(\Gamma_w) = \sum_{\nu=0}^{n-1} s_{n-\nu}(\Gamma_w)h_\nu(\Gamma_w), \quad n \geq 1.$$

Moreover, since homomorphisms of Γ_w to S_n can be identified with solutions of the equation $w(x_1, \ldots, x_d) = 1$ in S_n, we have

$$h_n(\Gamma_w) = (n!)^{-1}N_w(1) = (n!)^{d-2}\sum_\chi \alpha_\chi(w)\chi(1).$$

From Lemma 4 we know that $h_n(\Gamma_w)$ is odd if, and only if, n is a triangular number. Hence, for $n \geq 1$, we find that, modulo 2,

$$\begin{aligned} s_n(\Gamma_w) &= nh_n(\Gamma_w) - \sum_{\nu=1}^{n-1} s_{n-\nu}(\Gamma_w)h_\nu(\Gamma_w)\\ &\equiv \sum_{\substack{k\geq 1\\ k(k+1)<2n}} s_{n-\frac{1}{2}k(k+1)}(\Gamma_w) \,+\, \delta(n), \end{aligned}$$

the correction term $\delta(n)$ coming from the term $nh_n(\Gamma_w)$.

5. Random Walks on symmetric groups

5.1. **Roichman's conjectures.** Let $\mathbf{E} = E_1, E_2, E_3, \dots$ be a Markov chain on a metric space X; i.e., the probability of a sample sequence $\big(E_{j_0}, E_{j_1}, \dots, E_{j_n}\big)$ is given by

$$p\big\{\big(E_{j_0}, E_{j_1}, \dots, E_{j_n}\big)\big\} = a_{j_0} p_{j_0,j_1} p_{j_1,j_2} \cdots p_{j_{n-2},j_{n-1}} p_{j_{n-1},j_n},$$

where $p_{j,k}$ is the probability for the transition from E_j to E_k, a_k is the probability of the state E_k at time 0, and the initial probability distribution $\{a_k\}$ as well as the conditional probabilities $p_{j,k}$ are fixed throughout the whole process. The random walk on X determined by $\mathbf{E}$ is by definition the collection of all infinite paths on X with probability distribution induced by $\mathbf{E}$. If X is finite, and the initial probability distribution $\{a_k\}$ is given in advance, then $\mathbf{E}$ is determined by its transition matrix $P = (p_{j,k})$. In what follows, we will be interested in the case when X is a finite symmetric group given with the discrete metric. In this case, paths are simply infinite sequences $\{x_k\}_{k\geq 0}$ of states (that is, elements of S_n). Let $X = S_n$, and let $1 \neq \mathbf{c} \subseteq S_n$ be a non-trivial conjugacy class. The random walk $w_{\mathbf{c}}$ *generated by* $\mathbf{c}$ has initial state $x_0 = \mathrm{id}$ and the transition matrix $P_{\mathbf{c}} = \big(p^{\mathbf{c}}_{\sigma,\pi}\big)_{\sigma,\pi\in S_n}$, where

$$p^{\mathbf{c}}_{\sigma,\pi} := \begin{cases} \frac{1}{|\mathbf{c}|}, & \pi\sigma^{-1} \in \mathbf{c} \\ 0, & \text{otherwise.} \end{cases}$$

More explicitly, the statement concerning the initial state of $w_{\mathbf{c}}$ means that the initial probability distribution p_{initial} is concentrated in the identity; that is,

$$p_{\text{initial}}\{\pi\} = \begin{cases} 1, & \pi = \mathrm{id} \\ 0, & \text{otherwise} \end{cases}.$$

Given a norm $\|\cdot\|$ on the complex algebra $\mathbb{C}^{S_n}$ and a real number $\varepsilon > 0$, we say that the random walk $w_{\mathbf{c}}$ has reached *ε-equidistribution with respect to $\|\cdot\|$ in step k*, if

$$\left\| p\{x_k = \cdot\} - \frac{2}{n!}\mathbf{1}_{A_n} \right\|^2 \leq \varepsilon \cdot \left\| \frac{2}{n!}\mathbf{1}_{A_n} \right\|^2. \tag{24}$$

Here, $\mathbf{1}_S$ denotes the characteristic function for the subset S of the sample space X. We define the *statistical mixing time* $t_{\text{stat}}(\mathbf{c})$ of $w_{\mathbf{c}}$ as the least even integer k for which $w_{\mathbf{c}}$ has reached $\frac{1}{n}$-equidistribution with respect to the ℓ^2-norm; that is, the norm on $\mathbb{C}^{S_n}$ given by

$$\|f\|_2^2 = \langle f | f \rangle = \frac{1}{n!}\sum_{\sigma\in S_n} |f(\sigma)|^2, \quad f \in \mathbb{C}^{S_n}.$$

The appearance of $\mathbf{1}_{A_n}$ in (24) instead of the expected $\mathbf{1}_{S_n}$ is just a technical detail allowing us to avoid certain parity problems in the symmetric group S_n. For the same reason, step numbers are here restricted to even numbers. Computing the ℓ^2-norm of $\frac{2}{n!}\mathbf{1}_{A_n}$, $t_{\text{stat}}(\mathbf{c})$ is seen to be the least even integer k such that

$$\left\| p\{x_k = \cdot\} - \frac{2}{n!}\mathbf{1}_{A_n} \right\|_2^2 \leq \frac{2}{n(n!)^2}.$$

A lower bound for $t_{\text{stat}}(\mathbf{c})$ is given by the *combinatorial mixing time* $t_{\text{comb}}(\mathbf{c})$ of $\mathbf{c}$; that is, the least even integer k, such that any k elements of $\mathbf{c}$ have no common fixed point with probability at least $1-\frac{1}{n}$. A heuristic reason for the name "combinatorial mixing time" is the fact that, after $t_{\mathrm{comb}}(\mathbf{c})$ steps, almost certainly every element of the set $\{1,2,\dots,n\}$ has been moved by the conjugacy class $\mathbf{c}$. In [47], Roichman conjectures that, for every non-trivial conjugacy class $\mathbf{c}\subseteq A_n$,

$$t_{\mathrm{stat}}(\mathbf{c}) \ll t_{\mathrm{comb}}(\mathbf{c}). \tag{25}$$

His main result [47, Theorem 6.1] establishes this conjecture for classes $\mathbf{c}$ with cn fixed points, where c is some positive constant; this in turn generalizes an earlier result of Diaconis and Shahshahani [12] for transpositions. Following Roichman's paper, Fomin and Lulov [13] provide a character bound implying Conjecture (25) for conjugacy classes having only cycles of the same length. In [38], among other things, Roichman's conjecture is established in full generality.

Theorem 9 [Müller/Schlage–Puchta [38, Theorem 2], 2002]. *For $n\geq 4000$ and each non-trivial conjugacy class $\mathbf{c}\subseteq S_n$, we have*

$$t_{\mathrm{comb}}(\mathbf{c}) \leq t_{\mathrm{stat}}(\mathbf{c}) \leq 10\, t_{\mathrm{comb}}(\mathbf{c}).$$

In [47], Roichman suggests an approach to the general conjecture (25) via a certain estimate for character values of symmetric groups. More specifically, he conjectures that, for every $\varepsilon>0$, n sufficiently large, each conjugacy class $\mathbf{c}\subseteq S_n$, and every partition $\lambda\vdash n$,

$$|\chi_\lambda(\mathbf{c})| \leq \chi_\lambda(1)\bigg(\max\bigg\{\frac{\lambda_1}{n},\frac{\|\lambda\|}{n},\frac{1}{e}\bigg\}\bigg)^{(1-\varepsilon)n\log\frac{n}{n-\mathrm{supp}(\mathbf{c})+1}}, \tag{26}$$

which would imply (25).

5.2. **A remark concerning the estimate (26).** As it stands, estimate (26) is not correct. This can be seen, for instance, as follows. For $\mathbf{c}$ fixed-point free, λ such that $\max\{\lambda_1,\|\lambda\|\}\leq\frac{n}{e}$, and $\varepsilon=\frac{1}{2}$, Inequality (26) simplifies to

$$|\chi_\lambda(\mathbf{c})| \leq \chi_\lambda(1)\, e^{-(n\log n)/2}. \tag{27}$$

The right-hand side of (27) is bounded above by $\sqrt{n!}\, n^{-n/2}<1$; that is, for $\mathbf{c}$ and λ as above, and n sufficiently large, it would follow that $\chi_\lambda(\mathbf{c})=0$. Since the irreducible characters $\{\chi_\lambda\}_{\lambda\vdash n}$ form a basis for the space of class functions on S_n, this would imply that, for n sufficiently large, the set of characters

$$\Big\{\chi_\lambda : \lambda\vdash n,\ \max\{\lambda_1,\|\lambda\|\}>n/e\Big\} \tag{28}$$

would have to generate the space of class functions on the union of fixed-point free conjugacy classes of S_n. Comparing the size of the set (28) with the dimension of the last space, we find that, for large n,

$$2\sum_{0\leq\nu\leq n-n/e} p(\nu)\ \geq\ p(n)-p(n-1), \tag{29}$$

where $p(n)$ is the number of partitions of n. The right-hand side of (29) can be estimated via the first term in Rademacher's series expansion for $p(n)$ (see, for example, [1, Theorem 5.1]) to give

$$p(n) - p(n-1) \sim \frac{\pi e^{\pi\sqrt{\frac{2n}{3}}}}{12\sqrt{2}\, n^{3/2}} \quad (n \to \infty).$$

Bounding the left-hand side of (29) by means of the estimate[15]

$$p(n) < \frac{\pi}{\sqrt{6n}}\, e^{\pi\sqrt{\frac{2n}{3}}},$$

we obtain

$$2 \sum_{0 \le \nu \le n-n/e} p(\nu) \le 2np(n - \lfloor n/e \rfloor) \le A\sqrt{n}\, e^{\pi\sqrt{2(1-1/e)n/3}},$$

where A is some positive constant. From these two estimates it is clear that inequality (29) is violated for large n.

5.3. **Proof of Theorem 9 (Sketch).** Despite the failure of his conjecture concerning character values, the basic idea behind Roichman's suggested approach to (25) turns out to be correct. As a substitute for (26), we prove the following.

Theorem 10 [Müller/Schlage–Puchta [38, Theorem 1], 2002]. *For sufficiently large n, every non-trivial conjugacy class $\mathbf{c} \subseteq S_n$, and each partition $\lambda \vdash n$, we have*

$$|\chi_\lambda(\mathbf{c})| \le \big(\chi_\lambda(1)\big)^{1 - \frac{1-1/\log n}{6t_{\mathrm{comb}}(\mathbf{c})}},$$

and, for $1 \le s_1(\mathbf{c}) \le n-2$ (here, $s_1(\mathbf{c})$ is the number of 1-cycles of $\mathbf{c}$),

$$\left| t_{\mathrm{comb}}(\mathbf{c}) - \frac{2\log n}{\log\big(n/s_1(\mathbf{c})\big)} \right| \le 3,$$

whereas $t_{\mathrm{comb}}(\mathbf{c}) = 2$ for $s_1(\mathbf{c}) = 0$.

The proof of Theorem 10 is essentially probabilistic, making use of the following two auxiliary results.

Lemma 5. *Let $\mathbf{c} \subseteq S_n$ be a non-trivial conjugacy class, and let π be the element visited by the random walk $w_{\mathbf{c}}$ after $3t_{\mathrm{comb}}(\mathbf{c})$ steps. Then, for each $k \ge 1$, the probability that π has more than k fixed points is bounded above by*

$$\max\left\{ \frac{2^k}{(k-1)!}, \frac{2^{n/2}}{(\lfloor n/2 \rfloor - 1)!} \right\}.$$

Lemma 6. *Let $\mathbf{c}_1, \mathbf{c}_2 \subseteq S_n$ be non-trivial conjugacy classes with f_1 respectively f_2 fixed points. For $i = 1, 2$, let $x_i \in \mathbf{c}_i$ be chosen at random. Then the probability that x_1 and x_2 have ℓ common fixed points, is at most*

$$\binom{n}{\ell} \left(\frac{f_1 f_2}{n^2} \right)^{\ell}.$$

[15] Cf., for instance, [22, Satz 7.6].

Moreover, the probability for x_1x_2 *to have* k *cycles on* $\operatorname{supp}(x_1) \cup \operatorname{supp}(x_2)$ *is bounded above by*

$$(\log n)^{k-1}/(k-1)!.$$

We give a rough indication how Theorem 9 can be derived from the first part of Theorem 10; the second part then allows us to obtain completely explicit lower and upper bounds for $t_{\mathrm{stat}}(\mathbf{c})$ in terms of the number of fixed points of $\mathbf{c}$, while also transforming the first part of Theorem 10 into a more explicit form.

First, we note that the probability distribution $p\{x_k = \cdot\}$ in step k of the random walk $w_{\mathbf{c}}$ is given by the k-fold convolution of the function $\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}$ with itself, where, for two functions $f, g : S_n \to \mathbb{C}$, the convolution $f * g : S_n \to \mathbb{C}$ is defined as[16]

$$(f*g)(\pi) = \sum_{\sigma\in S_n} f(\sigma)g(\pi\sigma^{-1}).$$

Indeed,

$$\begin{aligned} p\{x_k = \pi\} &= \sum_{\sigma\in S_n} p\big\{x_{k-1} = \pi\sigma^{-1}\big\}\, p^{\mathbf{c}}_{\pi\sigma^{-1},\pi} \\ &= \frac{1}{|\mathbf{c}|}\sum_{\sigma\in\mathbf{c}} p\big\{x_{k-1} = \pi\sigma^{-1}\big\} \\ &= \left[\left(\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}\right) * p\big\{x_{k-1} = \cdot\big\}\right](\pi), \end{aligned}$$

and since

$$p\{x_1 = \pi\} = p^{\mathbf{c}}_{\mathrm{id},\pi} = \left(\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}\right)(\pi),$$

our claim that

$$p\{x_k = \cdot\} = \left(\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}\right)^{*k}$$

follows by induction on k. Next, we need a result relating the statistical mixing time of the random walk $w_{\mathbf{c}}$ to the character theory of the underlying finite group S_n. This is the following.

Lemma 7. *Let* $\mathbf{c} \subseteq S_n$ *be a conjugacy class,* k *a positive integer. Then*

$$(n!)^2 \left\| \left(\frac{1}{|\mathbf{c}|}\,\mathbf{1}_{\mathbf{c}}\right)^{*k} - \frac{2}{n!}\,\mathbf{1}_{A_n}\right\|_2^2 = \sum_{\substack{\chi\\ \chi(1)\neq 1}} \frac{|\chi(\mathbf{c})|^{2k}}{(\chi(1))^{2k-2}}. \tag{30}$$

Proof. For a class function $f : S_n \to \mathbb{C}$ and an irreducible character χ of S_n, define the Fourier coefficient $\alpha_\chi(f)$ via

$$f(\sigma) = \sum_{\chi} \alpha_\chi(f)\,\chi(\sigma), \quad \sigma\in S_n. \tag{31}$$

[16]Note that the convolution of two class functions is again a class function.

Since the irreducible characters form a basis for the space of class functions, the Fourier coefficients $\alpha_\chi(f)$ exist and are uniquely determined by (31). We shall need the following facts concerning the coefficients $\alpha_\chi(f)$.

(i) $\alpha_\chi(f) = \langle f|\chi\rangle$,
(ii) $\alpha_\chi(f * g) = n!\alpha_\chi(f)\alpha_\chi(g)/\chi(1)$,
(iii) $\sum_\chi |\alpha_\chi(f)|^2 = \|f\|_2^2$.

The proof of (i) consists in evaluating the sum $\sum_\chi \langle f|\chi\rangle\chi(\sigma)$ via the orthogonality relation (21), while (iii) (Parseval's Equation) follows directly from properties of the scalar product $\langle\cdot|\cdot\rangle$. We focus on the proof of (ii). By (i),

$$\begin{aligned}
\alpha_\chi(f * g) &= \langle f * g \,|\, \chi\rangle \\
&= \frac{1}{n!}\sum_\pi (f * g)(\pi)\chi(\pi^{-1}) \\
&= \frac{1}{n!}\sum_\pi\sum_\sigma f(\sigma)g(\pi\sigma^{-1})\chi(\pi^{-1}) \\
&= \frac{1}{n!}\sum_\pi\sum_\sigma\sum_{\chi'}\sum_{\chi''} \alpha_{\chi'}(f)\alpha_{\chi''}(g)\chi'(\sigma)\chi''(\pi\sigma^{-1})\chi(\pi^{-1}) \\
&= \sum_\pi\sum_{\chi'}\sum_{\chi''} \alpha_{\chi'}(f)\alpha_{\chi''}(g)\chi(\pi^{-1})\frac{1}{n!}\sum_\sigma \chi''(\pi\sigma^{-1})\overline{\chi'(\sigma^{-1})} \\
&= \sum_\pi\sum_{\chi'}\sum_{\chi''} \alpha_{\chi'}(f)\alpha_{\chi''}(g)\chi(\pi^{-1})\chi''(\pi)\delta_{\chi',\chi''}/\chi''(1) \\
&= \sum_\pi\sum_{\chi'} \alpha_{\chi'}(f)\alpha_{\chi'}(g)\chi(\pi^{-1})\chi'(\pi)/\chi'(1) \\
&= \sum_{\chi'} \frac{n!\alpha_{\chi'}(f)\alpha_{\chi'}(g)}{\chi'(1)}\langle\chi'|\chi\rangle \\
&= n!\alpha_\chi(f)\alpha_\chi(g)/\chi(1),
\end{aligned}$$

where we have used the orthogonality relation (22) in step 6.

With (i)–(iii) in hand, the proof of Lemma 7 boils down to a straightforward calculation. More specifically, applying (i), the Fourier coefficient $\alpha_\chi(f)$ of the function $f = \frac{1}{|\mathbf{c}|}\mathbf{1}_\mathbf{c}$ is found to be

$$\begin{aligned}
\left\langle \frac{1}{|\mathbf{c}|}\mathbf{1}_\mathbf{c} \,\middle|\, \chi \right\rangle &= \frac{1}{n!}\sum_\sigma \left(\frac{1}{|\mathbf{c}|}\mathbf{1}_\mathbf{c}\right)(\sigma)\,\chi(\sigma^{-1}) \\
&= \frac{1}{n!}\sum_{\sigma\in\mathbf{c}} \chi(\sigma^{-1})/|\mathbf{c}| \\
&= \chi(\mathbf{c}^{-1})/n!.
\end{aligned}$$

Property (ii) together with induction on k then yields

$$\alpha_\chi\left(\left(\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}\right)^{*k}\right) = \frac{(\chi(\mathbf{c}^{-1}))^k}{n!(\chi(1))^{k-1}},$$

thus

$$\alpha_\chi\left(\left(\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}\right)^{*k} - \frac{2}{n!}\mathbf{1}_{A_n}\right) = \frac{(\chi(\mathbf{c}^{-1}))^k}{n!(\chi(1))^{k-1}} - \frac{1}{n!}\delta_{\chi,\chi_0} - \frac{1}{n!}\delta_{\chi,\chi_1},$$

where χ_1 is the sign character, χ_0 the trivial character of S_n. Equation (30) follows now from Parsival's Equation (iii). □

Remark. By an argument very similar to the proof of Lemma 7, one can show for instance that, for any finite group G, each conjugacy class $\mathbf{c}$ in G, and every positive integer k,

$$|G|^2 \left\| \left(\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}\right)^{*k} - \frac{1}{|G|}\mathbf{1}_G \right\|_2^2 = \sum_{\chi\neq\chi_0} \frac{|\chi(\mathbf{c})|^{2k}}{(\chi(1))^{2k-2}},$$

where χ_0 is the trivial character of G.

Now let $\mathbf{c} \subseteq S_n$ be a non-trivial conjugacy class. Then we infer from Lemma 7 that $w_{\mathbf{c}}$ has reached $\frac{1}{n}$-equidistribution with respect to the ℓ^2-norm after k steps if, and only if,

$$\sum_{\substack{\chi \\ \chi(1)\neq 1}} \frac{|\chi(\mathbf{c})|^{2k}}{(\chi(1))^{2k-2}} \leq \frac{2}{n}.$$

By the first part of Theorem 10, the left-hand side can be bounded above by

$$\sum_{\substack{\chi \\ \chi(1)\neq 1}} \big(\chi(1)\big)^{2-\frac{2k(1-1/\log n)}{6t_{\mathrm{comb}}(\mathbf{c})}}.$$

For $k \geq 10t_{\mathrm{comb}}(\mathbf{c})$ and sufficiently large n, the last expression is less than

$$\sum_{\substack{\chi \\ \chi(1)\neq 1}} \big(\chi(1)\big)^{-5/4},$$

which in turn is $\mathcal{O}\big(n^{-5/4}\big)$ by Corollary 1. Hence, for n sufficiently large, we obtain the bound $t_{\mathrm{stat}}(\mathbf{c}) \leq 10t_{\mathrm{comb}}(\mathbf{c})$ as required.

References

[1] G. Andrews, *The Theory of Partitions*, Cambridge University Press, New York, 1984.

[2] S. Ahlgren and K. Ono, Congruence properties for the partition function, *Proc. Nat. Acad. Sciences USA* **98** (2001), 12882–12884.

[3] S. Ahlgren and K. Ono, Congruences and conjectures for the partition function. In: q-Series with Applications to Combinatorics, Number Theory, and Physics (Urbana (IL), 2000), *Contemp. Math.* **291** (2001), Amer. Math. Soc., Providence (RI), 1–10.

[4] E. A. Bender, An asymptotic expansion for the coefficients of some formal power series, *J. London Math. Soc.* (2) **9** (1975), 451–458.

[5] B. Baumslag and S. Pride, Groups with two more generators than relators, *J. London Math. Soc.* **17** (1978), 425–426.
[6] K. S. Brown, *Cohomology of Groups*, Springer, New York, 1982.
[7] P. J. Cameron and T. W. Müller, A descent principle in modular subgroup arithmetic, *J. Pure Appl. Algebra* **203** (2005), 189–203.
[8] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley & Sons, New York, 1962.
[9] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. I, John Wiley & Sons, New York, 1981.
[10] H. Davenport, *The Higher Arithmetic*, sixth edition, Cambridge University Press, 1992.
[11] P. Diaconis, *Group Representations in Probability and Statistics*, IMS Lecture Notes Vol. 11, Hayward, California, 1988.
[12] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions, *Z. Wahrscheinlichkeitstheorie u. Verw. Gebiete* **57** (1981), 159–179.
[13] S. V. Fomin and N. Lulov, On the number of rim hook tableaux, *J. Math. Sciences* **87** (1997), 4118–4123.
[14] C. F. Gauß, *Disquisitiones Arithmeticae* (Lipsia in commissis apud Gerh. Fleischer Iun), 1801; English translation by A. Clarke (Springer, New York), 1986.
[15] M. Hall, Subgroups of finite index in free groups, *Canad. J. Math.* **1** (1949), 187–190.
[16] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, reprint of the fifth edition, 1989.
[17] E. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, Academische Verlagsgesellschaft, Leipzig, 1923; reprinted (Chelsea Publishing Company, New York), 1970. English translation by G. Bauer and J. Goldman with R. Kotzen as *Lectures on the Theory of Algebraic Numbers* (Springer, New York), 1981.
[18] B. Huppert, *Endliche Gruppen*, vol. 1, Springer, Heidelberg, 1979.
[19] N. Ito, On the degrees of irreducible representations of a finite group, *Nagoya Math. J.* **3** (1951), 5–6.
[20] A. Kerber, *Algebraic Combinatorics via Finite Group Actions*, BI-Wissenschaften, Mannheim, 1991.
[21] M. Knopp, *Modular Functions in Analytic Number Theory*, Markham, Chicago, 1970.
[22] E. Krätzel, *Zahlentheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1981.
[23] A.-M. Legendre, *Essai sur la Théorie des Nombres*, Paris, 1798. Fourth edition as *Théorie des Nombres*, 1830; reprinted (Albert Blanchard, Paris), 1955.
[24] R. C. Lyndon, Two notes on Rankin's book on the modular group, *J. Austral. Math. Soc.* **16** (1973), 454–457.
[25] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer, Berlin/Heidelberg, 1977.
[26] W. Magnus, *Noneuclidean Tesselations and Their Groups*, Academic Press, New York, 1974,
[27] T. Müller, Subgroup growth of free products, *Invent. math.* **126** (1996), 111–131.
[28] T. Müller, Finite group actions and asymptotic expansion of $e^{P(z)}$, *Combinatorica* **17** (1997), 523–554.
[29] T. Müller, Enumerating representations in finite wreath products, *Adv. in Math.* **153** (2000), 118–153.
[30] T. W. Müller, Modular subgroup arithmetic and a theorem of Philip Hall, *Bull. London Math. Soc.* **34** (2002), 587–598.
[31] T. W. Müller, Modular subgroup arithmetic in free products, *Forum Math.* **15** (2003), 759–810.
[32] T. W. Müller, Parity patterns in Hecke groups and Fermat primes. In: Proceedings 1999 Bielefeld conference 'Groups: Topological, Combinatorial and Arithmetic Aspects' (T. W. Müller ed.). LMS Lecture Notes Series 311, Cambridge University Press, Cambridge, 2004, 327–374.
[33] T. W. Müller and J.-C. Puchta, Character Theory of symmetric groups and subgroup growth of surface groups, *J. London Math. Soc.* (2) **66** (2002), 1–18.
[34] T. W. Müller and J.-C. Puchta, Parity patterns in one-relator groups, *J. Group Theory* **6** (2003), 245–260.

[35] T. W. Müller and J.-C. Schlage–Puchta, Classification and statistics of finite index subgroups in free products, *Adv. Math.* **188** (2004), 1–50.
[36] T. W. Müller and J.-C. Schlage–Puchta, Modular arithmetic of free subgroups, *Forum Math.* **17** (2005), 375–405.
[37] T. W. Müller and J.-C. Schlage–Puchta, Some examples in the theory of subgroup growth, *Monatsh. Math.* **146** (2005), 49–76.
[38] T. W. Müller and J.-C. Schlage–Puchta, Character theory of symmetric groups, subgroup growth of Fuchsian groups, and random walks, to appear.
[39] T. W. Müller and J.-C. Schlage–Puchta, Statistics of isomorphism types in free products, to appear.
[40] T. W. Müller and J.-C. Schlage–Puchta, Decomposition of the conjugacy representation for symmetric groups and subgroup growth, to appear.
[41] M. Newman, Asymptotic formulas related to free products of cyclic groups, *Math. Comp.* **30** (1976), 838–846.
[42] J. Nielsen, The commutator group of the free product of cyclic groups, *Mat. Tidsskr.* B (1948), 49–56.
[43] J.-L. Nicolas, I. Ruzsa, and A. Sárközy, On the parity of additive representation functions, *J. Number Theory* **73** (1998), 292–317.
[44] K. Ono, On the parity of the partition function in arithmetic progressions, *J. Reine u. Angew. Math.* **472** (1996), 1–15.
[45] S. J. Pride, The concept of largeness in group theory. In: Word Problems II, Amsterdam: North Holland, 1980, 299–335.
[46] T. Parkin and D. Shanks, On the distribution of parity in the partition function, *Math. Comp.* **21** (1967), 466–480.
[47] Y. Roichman, Upper bound on the characters of the symmetric groups, *Invent. math.* **125** (1996), 451–485.
[48] Y. Roichman, Decomposition of the conjugacy representation of the symmetric group, *Israel J. Math.* **97** (1997), 305–316.
[49] T. Scharf, Die Wurzelanzahlfunktion in symmetrischen Gruppen, *J. Algebra* **139** (1991), 446–457.
[50] R. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge University Press, New York, 1999.
[51] W. Stothers, The number of subgroups of given index in the modular group, *Proc. Royal Soc. Edinburgh* **78A** (1977), 105–112.
[52] M. Subbarao, Some remarks on the partition function, *Amer. Math. Monthly* **73** (1966), 851–854.
[53] E. M. Wright, A relationship between two sequences, *Proc. London Math Soc.* (3) **17** (1967), 296–304.
[54] E. M. Wright, Asymptotic relations between enumerative functions in graph theory, *Proc. London Math. Soc.* **20** (1970), 558–572.

Thomas W. Müller
School of Mathematical Sciences
Queen Mary & Westfield College
University of London
Mile End Road
E1 4NS London
United Kingdom