CHARACTER THEORY OF SYMMETRIC GROUPS, SUBGROUP GROWTH OF FUCHSIAN GROUPS, AND RANDOM WALKS

Thomas W. Müller and Jan-Christoph Schlage-Puchta

1. Introduction

The purpose of this paper is three-fold. On the one hand – and that was its original motivation – we establish an asymptotic estimate for the subgroup growth of Fuchsian groups, that is, groups Γ of the form

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

with integers $r, s, t \geq 0$ and $e_1, \ldots, e_s \geq 2$, and $a_1, \ldots, a_r \in \mathbb{N} \cup \{\infty\}$. Although this definition appears not to be standard, it encompasses all different notions of Fuchsian groups known to the authors.

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

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

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

$$s_n(\Gamma) \approx \delta L_\Gamma (n!)^{\mu(\Gamma)} \Phi_\Gamma(n) \Big\{ 1 + \sum_{\nu=1}^{\infty} a_\nu(\Gamma) n^{-\nu/m_\Gamma} \Big\}, \quad (n \to \infty). \tag{3}$$

Here,

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

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

Here, $\approx$ denotes an asymptotical series, confer the end of this section.

On the other hand, the proof of Theorem A requires the representation-theoretic approach initiated in [27], and large parts of the present paper are concerned with various statistical aspects of symmetric groups, and rather subtle estimates for values and multiplicities of their characters, which are also of independent interest. In particular, we show the following.

Theorem B. *Let $\varepsilon > 0$ and an integer q be given, n sufficiently large, and let χ be an irreducible character of S_n.*

(i) *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.

(ii) *We have*

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

(iii) *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. 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, Theorem B enables us to prove the following.

Theorem C. *Let $\mathbf{c}$ be a non-trivial conjugacy class in S_n. Denote by $t_c(\mathbf{c})$ 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* $t_s(\mathbf{c})$ *be the mixing time for the random walk generated by* $\mathbf{c}$. *Then, for* $n \geq 4000$, *we have*

$$t_c(\mathbf{c}) \leq t_s(\mathbf{c}) \leq 10 t_c(\mathbf{c}).$$

We call the quantity t_c *combinatorial mixing time*, since after t_c steps the distribution of a single point cannot be distinguished from the uniform distribution.

Theorem C establishes in full generality a conjecture of Roichman; cf. [29, Conj. 6.6]. For special choices of $\mathbf{c}$, Roichman's conjecture had already been known to hold: Diaconis and Shahshahani [8] established it for transpositions, Roichman [29] generalised their result to conjugacy classes having at least cn fixed points, and Fomin and Lulov [11] established a character bound implying Theorem C for conjugacy classes having only cycles of the same length.

In the remainder of this introduction, we describe in more detail the organisation of our paper, and the contents of individual sections. After a short introduction to random walks on finite groups generated by conjugacy classes and their connection with character theory, Section 2 establishes Theorem C and the first part of Theorem B. This includes the proof of a variety of preliminary character estimates for arbitrary conjugacy classes, which are used throughout the paper. The main tools here are the hook formula and the Murnaghan-Nakayama rule. Section 3 gives the proof of Theorem B (ii). In preparation for this argument, we derive a number of results concerning the statistics of symmetric groups, mostly dealing with the distribution of cycles in various subsets of S_n; cf. Subsection 3.1. Again, this group of results is also used in other sections. The theory developed up to this point would already enable us to estimate the subgroup growth of Fuchsian groups with $s = 0$; that is, of Fuchsian groups where none of the generators $y_1, \dots, y_s$ in (1) are present. However, in order to deal with Fuchsian groups in full generality, we also need some insight into the growth behaviour of multiplicities of root number functions for symmetric groups, measured against the degree of the corresponding irreducible character; in particular, we have to establish Theorem B (iii). Section 4 is devoted to the proof of this and related results.

Proof and discussion of Theorem A are the principal themes of Section 5. Following the argument establishing Theorem A, we demonstrate that condition (2) is in fact necessary. More specifically, we show the following.

Theorem D. *Let* Γ *be as in* (1) *with* $r = t = 0$, $s \geq 2$ *and* $\alpha(\Gamma) < 0$ *(that is,* Γ *is the one-relator group associated with the defining relation* $y_1^{e_1} y_2^{e_2} \cdots y_s^{e_s} = 1$*). Then, as n tends to infinity, we have*

$$s_n(\Gamma) \sim K (n!)^{\mu(\Gamma) - \alpha(\Gamma)/2} \exp\left(\sum_{j=1}^{s} \sum_{\substack{\nu_j \mid e_j \\ \nu_j < e_j}} \frac{n^{\nu_j / e_j}}{\nu_j} + \frac{\alpha(\Gamma) - 2\mu(\Gamma) + 2}{4} \log n \right).$$

This is the contents of Theorem 4, where also the constant K is given explicitly. According to Theorem D, the subgroup growth of these one-relator groups is faster than might be expected in view of Theorem A. In Subsection 5.2, we discuss the explicit computation of the coefficients $a_\nu(\Gamma)$ in general, and, as an example, compute the first 22 of these coefficients for the triangle group $\Gamma(2, 3, 7)$, only 10 of which turn out to be non-vanishing. As a further application of Theorem B (iii), we determine the subgroup growth of a discrete analogue of Demuškin groups. Demuškin groups are pro-p-groups 1 with Poincaré duality and homological dimension 2. For $p > 2$, these are known to be one-relator groups with defining relation of the form

$$R = x_1^{p^h}[x_1, x_2][x_3, x_4] \cdots [x_{m-1}, x_m], \quad h \in \mathbb{N} \cup \{\infty\}.$$

In Subsection 5.4, we prove the following result.

Theorem E. *For integers $q \geq 1$ and $d \geq 2$, let*

$$\Gamma_{q,d} = \Big\langle x_1, y_1, \ldots, x_d, y_d \,\Big|\, x_1^{q-1}[x_1, y_1] \cdots [x_d, y_d] = 1 \Big\rangle.$$

Then there exist explicitly computable constants $\gamma_\nu(\Gamma_{q,d})$, such that

$$s_n(\Gamma_{q,d}) \approx \delta n (n!)^{2d-2} \left\{ 1 + \sum_{\nu=1}^{\infty} \gamma_\nu(\Gamma_{q,d}) n^{-\nu} \right\}, \quad n \to \infty,$$

where

$$\delta = \begin{cases} 1, & q \text{ even} \\ 2, & q \text{ odd.} \end{cases}$$

Introduce an equivalence relation $\sim$ on the class of finitely generated groups via

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

In [25, Theorem 3] a characterisation in terms of structural invariants is given for the equivalence relation $\sim$ on the class of groups Γ of the form

$$\Gamma = G_1 * G_2 * \cdots * G_s * F_r$$

with $r, s \geq 0$ and finite groups G_σ, and it is shown that each $\sim$-class of free products decomposes into finitely many isomorphism classes. Our final section is concerned with the analogous problems for Fuchsian groups.

Theorem F. *The multi-set $\{a_1, a_2 \ldots, a_r\}$ together with the numbers $\mu(\Gamma)$ and δ form a complete system of invariants for the equivalence relation $\sim$ on the class $\mathcal{F}$ of all Fuchsian groups Γ satisfying $\alpha(\Gamma) > 0$.*

Theorem F allows us to construct an infinite sequence of pairwise non-isomorphic Fuchsian groups, all of which are $\sim$-equivalent to the same Fuchsian group Γ; in particular there cannot be a finiteness result for the relation $\sim$ on $\mathcal{F}$. The situation changes, if we take into account the full precision of (3) in Theorem A. More specifically, consider three refinements of the equivalence relation $\sim$ on $\mathcal{F}$: (i) the relation $\approx$ of strong equivalence[1] defined via

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

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

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

[1] The symbols $\sim$ and $\approx$ as relations on $\mathcal{F}$ correspond to the relations on functions denoted by the same symbols.

in the Fuchsian presentation (1), denoted $\Gamma = \Delta$ (strictly speaking, all these equivalence relations are now defined on the set $\mathcal{FP}$ of Fuchsian presentations in the sense of (1) satisfying $\alpha(\Gamma) > 0$). Clearly,

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

It can be shown that all these implications are in fact strict. For these relations, we have the following surprising result.

Theorem G. *Each $\approx$-equivalence class of $\mathcal{FP}$ decomposes into finitely many classes with respect to $=$; that is, each group $\Gamma \in \mathcal{F}$ has only finitely many presentations of the form* (1), *and is $\approx$-equivalent to at most finitely many non-isomorphic $\mathcal{F}$-groups.*

Some notation. Permutations are denoted by π, σ, or τ. For $\pi \in S_n$ and $1 \leq i \leq n$, let $c_i(\pi)$ be the number of i-cycles of π. The *support* $\operatorname{supp}(\pi)$ of π is the set of points moved by π. For integer partitions we mostly follow the conventions of [21, Chap. I, Sec. 1]. Specifically, a partition $\lambda = (\lambda_1, \lambda_2, \dots)$ is a weakly decreasing sequence of non-negative integers λ_j, such that $\lambda_j = 0$ for j sufficiently large. The *weight* $|\lambda|$ of λ is $|\lambda| = \sum_j \lambda_j$, and the *norm* $\|\lambda\|$ of λ is the largest j such that $\lambda_j \neq 0$. As usual, we write $\lambda \vdash n$ for $|\lambda| = n$, and say that λ is a partition of n. For partitions λ, μ we write $\mu \subseteq \lambda$, if $\mu_j \leq \lambda_j$ for all j (that is, the Ferrers diagram of μ is contained in the Ferrers diagram of λ). For a partition λ, we denote by λ' the conjugate partition: $\lambda'_i = \max\{j : \lambda_j \geq i\}$ (that is, the Ferrers diagram of λ' is obtained from that of λ by reflection through the main diagonal). By $\lambda \setminus \lambda_1$ we mean the partition $\lambda \setminus \lambda_1 = (\lambda_2, \lambda_3, \dots)$ (that is, the Ferrers diagram of $\lambda \setminus \lambda_1$ is obtained from that of λ by deleting the first row). Whenever convenient, we shall denote the integer $|\lambda| - \lambda_1$ by Δ. For a partition $\lambda \vdash n$, we denote by χ_λ the irreducible character of S_n associated with λ. For a finite group G, let $\operatorname{Irr}(G)$ be the set of irreducible characters of G. The usual scalar product on the space $\mathbb{C}^G$ is denoted by $\langle \cdot, \cdot \rangle_G$, or simply by $\langle \cdot, \cdot \rangle$ if G is a symmetric group.

We use what we believe to be standard number-theoretic notation. Specifically, the partition function is denoted $p(n)$, $\tau(n)$ and $\sigma(n)$ are the number of divisors and the sum of divisors of n, respectively, $S(n, m)$ is the number of (set theoretic) partitions of an n-set into m non-empty blocks (a Stirling number of the second kind). For integers m and n, we denote their greatest common divisor and least common multiple by (m, n) respectively $[m, n]$. For arithmetic functions $f, g : \mathbb{N} \to \mathbb{R}$ we use the Vinogradov symbol $f(n) \ll g(n)$ to mean $f(n) = \mathcal{O}(g(n))$. If $f(n) \ll g(n) \ll f(n)$, we write $f(n) \asymp g(n)$. Asymptotic equivalence is denoted by $\sim$: we write $f(n) \sim g(n)$ to mean $f(n) = g(n)(1 + o(1))$. We use $\approx$ to denote asymptotic expansions in the sense of Poincaré; for instance we write

$$f(n) \approx g(n) \left\{ 1 + \sum_{\nu=1}^{\infty} a_\nu n^{-\nu/q} \right\}, \quad (n \to \infty),$$

if for every integer A we have

$$f(n) = g(n) \left\{ 1 + \sum_{\nu=1}^{A} a_\nu n^{-\nu/q} + \mathcal{O}(n^{-(A+1)/q}) \right\},$$

where the implied constants may depend on A. Finally, we use some notation from probability theory: $\mathbf{1}_X$ denotes the characteristic function for a subset $X \subseteq \Omega$ of the sample space Ω, and $\mathbf{E}\xi$ is the expected value of the random variable ξ.

2. Character Estimates and Random Walks on symmetric groups

2.1. **Roichman's Conjectures.**

Let $\mathbf{E} = E_1, E_2, E_3, \ldots$ be a Markov chain on a metric space X. The random walk $(x_k)_{k\geq 0}$ 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, then $\mathbf{E}$ can be determined by its transition matrix P. In what follows, we will be interested in the case when X is a finite symmetric group given with the discrete metric.[2] 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 $x_0 = 1$ and the transition matrix $P_{\mathbf{c}} = (p^{\mathbf{c}}_{\sigma\pi})_{\sigma,\pi\in S_n}$ where

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

The distribution in the k-th step of $w_{\mathbf{c}}$ is given by the convolution formula

$$P(x_k = \pi) = \frac{1}{|\mathbf{c}|} \sum_{\sigma\in S_n} P(x_{k-1} = \pi\sigma^{-1}).$$

More generally, for two functions $f, g : S_n \to \mathbb{C}$, the convolution $f * g : S_n \to \mathbb{C}$ is given by

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

in particular, $P(x_k = \pi)$ is the k-fold convolution of the function $\frac{1}{|\mathbf{c}|}\mathbf{1}_{\mathbf{c}}$. In the sequel we shall always take k even, to avoid parity problems. Given a norm $\|\cdot\|$ on the complex algebra $\mathbb{C}^{S_n}$ and $\varepsilon > 0$, we say that the random walk $w_{\mathbf{c}}$ has reached ε-equidistribution with respect to $\|\cdot\|$ in step k, if

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

We define the *statistical mixing time* $t_s(\mathbf{c})$ 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. A first lower bound for $t_s(\mathbf{c})$ is given by the combinatorial mixing time $t_c(\mathbf{c})$ 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 $1 - \frac{1}{n}$. In [29], Roichman conjectured that for every non-trivial conjugacy class $\mathbf{c} \subseteq A_n$,

$$t_s(\mathbf{c}) \ll t_c(\mathbf{c}). \tag{4}$$

His main result [29, Theorem 6.1] establishes this conjecture for classes $\mathbf{c}$ with cn fixed points. Roichman suggests an approach to the general conjecture (4) via a certain estimate for character values in symmetric groups. More precisely, he conjectures that,

[2] Cf. [7] for more details on random walks on finite groups and their applications.

for every $\varepsilon > 0$, n sufficiently large, each conjugacy class $\mathbf{c} \subseteq S_n$, and every partition $\lambda \vdash n$

$$|\chi_\lambda(\mathbf{c})| \leq \chi_\lambda(1) \left(\max\left(\frac{\lambda_1}{n}, \frac{\|\lambda\|}{n}, \frac{1}{e} \right) \right)^{(1-\varepsilon) n \log \frac{n}{n - |\mathrm{supp}(\mathbf{c})| + 1}}, \tag{5}$$

which would imply (4). Unfortunately, as it stands, estimate (5) is false. This can be seen, for instance, as follows. For $\mathbf{c}$ fixed-point free, λ such that $\lambda_1, \|\lambda\| \leq \frac{n}{e}$, and $\varepsilon = \frac{1}{2}$, (5) simplifies to

$$|\chi_\lambda(\mathbf{c})| \leq \chi_\lambda(1) e^{-(n \log n)/2}. \tag{6}$$

The right-hand side of (6) 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 characters

$$\big\{\chi_\lambda : \lambda \vdash n, \max(\lambda_1, \|\lambda\|) > n/e\big\}$$

would generate the space of class functions on the set of fixed-point free conjugacy classes of S_n. Comparing the size of the former set with the dimension of the latter space, we find that, for large n,

$$2 \sum_{0 \leq \nu \leq n - n/e} p(\nu) \geq p(n) - p(n-1), \tag{7}$$

where $p(n)$ is the number of partitions of n. The right-hand side can be estimated via the first term of 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 sum in (7) by means of the estimate[3] $p(n) < \frac{\pi}{\sqrt{6n}} e^{\pi\sqrt{2n/3}}$ we obtain

$$2 \sum_{0 \leq \nu \leq n - n/e} p(\nu) \leq 2np(n - \lfloor n/e \rfloor) \leq 2\pi \sqrt{n/6} e^{\pi \sqrt{2(1-1/e)n/3}}.$$

From these two estimates it is clear that Inequality (7) is violated for large n.

However, the basic idea behind Roichman's approach turns out to be correct. As a substitute for (5), we prove the following.

Theorem 1. *For sufficiently large n, a non-trivial conjugacy class $\mathbf{c} \subseteq S_n$, and a partition $\lambda \vdash n$, we have*

$$|\chi_\lambda(\mathbf{c})| \leq \big(\chi_\lambda(1)\big)^{1 - \frac{1 - 1/(\log n)}{6 t_c(\mathbf{c})}} \tag{8}$$

and, for $1 \leq c_1(\mathbf{c}) \leq n-2$,

$$\left| t_c(\mathbf{c}) - \frac{2 \log n}{\log(n / c_1(\mathbf{c}))} \right| \leq 3, \tag{9}$$

whereas $t_c(\mathbf{c}) = 2$ for $c_1(\mathbf{c}) = 0$.

[3] Cf., for instance, [18, Satz 7.6].

This result in turn allows us to establish Roichman's conjecture (4) for the mixing time of random walks on symmetric groups.

Theorem 2. *For $n \geq 4000$ and each non-trivial conjugacy class $\mathbf{c} \subseteq S_n$, we have*

$$t_c(\mathbf{c}) \leq t_s(\mathbf{c}) \leq 10t_c(\mathbf{c}). \tag{10}$$

The constants in Theorems 1 and 2 are most certainly not optimal, but we have not attempted to tighten our numerical estimates.

This section is organised as follows. In Subsection 2.2 we describe the general connection between random walks on finite groups and character estimates, and we explain, how Theorem 2 can be deduced from Theorem 1. The next subsection establishes certain elementary estimates for values and degrees of irreducible characters of symmetric groups, which will be used throughout the paper. Finally, Subsections 2.4 and 2.5 contain the proof of Theorem 1.

2.2. **Character Theory and Random walks.** Here, we describe the connection between character theory and probability measures on finite groups. For a more detailed presentation, see [7] and [31]. Let G be a finite group. For a class function $\varphi : G \to \mathbb{C}$ and an irreducible character χ of G, define the Fourier coefficient $\alpha_\chi(\varphi)$ by means of the equation

$$\varphi(g) = \sum_\chi \alpha_\chi(\varphi)\chi(g), \quad g \in G.$$

There is some ambiguity as how to define the scalar product on the space of functions $\varphi : G \to \mathbb{C}$. In group theory one usually defines

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\psi(g)};$$

however, when adopting the point of view of distributions, the factor $\frac{1}{|G|}$ appears unnatural. Here, we shall adopt the convention of group theory, although we shall frequently change our point of view, which leads to formulae looking slightly unusual.

Since irreducible characters form a basis of the space of class functions, the Fourier coefficients exist and are uniquely defined by this equation. The following Lemma states the basic properties of Fourier coefficients.

Lemma 1. (i) $\alpha_\chi(\varphi) = \langle \varphi, \chi \rangle$,

(ii) $\alpha_\chi(\varphi * \psi) = \frac{\alpha_\chi(\varphi)\alpha_\chi(\psi)}{\chi(1)}$,

(iii) $\sum_\chi |\alpha_\chi(\varphi)|^2 = \frac{1}{|G|} \sum_{g \in G} |\varphi(g)|^2$.

Proof. With respect to the standard scalar product, the irreducible characters form an orhtonormal basis of the vector space of all class functions, hence, the first and the third statement follow from general facts about euclidean vector spaces. For the second statement we first compute with matrices. Let χ be a character, and ρ the associated representation. The advantage of this approach is the fact that $\rho(gh) = \rho(g)\rho(h)$, since

ρ is a homomorphism, whereas for χ, being the trace of this homomorphism, no simple formula for $\chi(gh)$ exists. We have

$$\begin{aligned}\alpha_\chi(\varphi*\psi) &= \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\rho(g))\sum_{h\in G}\varphi(h)\psi(h^{-1}g)\\ &= \frac{1}{|G|}\mathrm{tr}\Big(\sum_{g\in G}\rho(g)\sum_{h\in G}\sum_{\chi_1}\alpha_{\chi_1}(\varphi)\chi_1(h)\sum_{\chi_2}\alpha_{\chi_2}(\psi)\chi_2(h^{-1}g)\Big)\\ &= \frac{1}{|G|}\mathrm{tr}\Big(\sum_{\chi_1}\alpha_{\chi_1}(\varphi)\sum_{\chi_2}\alpha_{\chi_2}(\psi)\sum_{g,h\in G}\chi_1(g)\chi_2(h)\underbrace{\rho(gh)}_{=\rho(g)\rho(h)}\Big).\end{aligned}$$

By Schur's Lemma we see that for every conjugacy class $\mathbf{c}$ of G, the matrix $\sum_{g\in\mathbf{c}}\rho(g)$ is diagonal with entries $\frac{|\mathbf{c}|\chi(\mathbf{c})}{\chi(1)}$, thus, we obtain

$$\begin{aligned}\alpha_\chi(\varphi*\psi) &= \frac{1}{|G|\chi(1)}\sum_{\chi_1}\alpha_{\chi_1}(\varphi)\sum_{\chi_2}\alpha_{\chi_2}(\psi)\sum_{g,h\in G}\chi_1(g)\chi_2(h)\chi(g)\chi(h)\\ &= \frac{|G|}{\chi(1)}\sum_{\chi_1}\alpha_{\chi_1}(\varphi)\sum_{\chi_2}\alpha_{\chi_2}(\psi)\langle\chi,\chi_1\rangle\langle\chi,\chi_1\rangle\\ &= \frac{|G|}{\chi(1)}\alpha_\chi(\varphi)\alpha_\chi(\psi),\end{aligned}$$

and the second claim is proven. □

Using Lemma 1, we obtain the following, which is a variant of the upper bound lemma, confer [7, Lemma 1, Chapter 3B].

Lemma 2. *Let $\mathbf{c}\subseteq S_n$ be a conjugacy class, and let k be an integer. Suppose that k is even, or that $\mathbf{c}\subseteq A_n$. Then we have*

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

Proof. Let χ_0 be the trivial character of S_n, χ_1 be the sign character. Then

$$\alpha_{\chi_0}\big(\frac{1}{|\mathbf{c}|}\mathbf{1}_\mathbf{c}\big)=\alpha_{\chi_0}\big(\frac{1}{n!}\mathbf{1}_{A_n}\big)=\alpha_{\chi_0}\big(\frac{1}{n!}\mathbf{1}_{A_n}\big)=1,$$

whereas

$$\alpha_{\chi_0}\big(\frac{1}{|\mathbf{c}|}\mathbf{1}_\mathbf{c}\big)=\begin{cases}1, & \mathbf{c}\subseteq A_n,\\ -1, & \mathbf{c}\subseteq S_n\setminus A_n.\end{cases}$$

Hence, for k even or $\mathbf{c}\subseteq A_n$, the Fouriercoefficients of the linear characters of $\left(\frac{1}{|\mathbf{c}|}\mathbf{1}_\mathbf{c}\right)^{*k}-\frac{1}{n!}\mathbf{1}_{A_n}$ vanish, whereas the Fouriercoefficient for a non-linear character χ equal $\frac{\chi(\mathbf{c})^k}{n!\chi(1)^{k-1}}$ by Lemma 1 (ii). Our claim now follows from Lemma 1 (iii). □

In contrast to [7], we will only consider the ℓ^2-norm. The passage from the ℓ^2-norm to ℓ^p-norms with $p \leq 2$ is immediate by Hölder's inequality; however, in the context of random walks, the passage from ℓ^2 to ℓ^∞ is possible as well.

Lemma 3. *Let G be a finite group, and let $f : G \to [0, \infty)$ be a probability measure. Then we have*

$$\left\| f * f - \frac{1}{|G|}\mathbf{1} \right\|_\infty \leq \left\| f - \frac{1}{|G|}\mathbf{1} \right\|_2^2.$$

In particular, if $w_\mathbf{c}$ reaches ε-equidistribution with respect to the ℓ^2-norm after k steps, it reaches ε^2-equidistribution with respect to the ℓ^∞-norm after $2k$ steps.

Proof. We have

$$\begin{aligned}(f * f)(g) &= \sum_{h \in G} f(h) f(gh^{-1}) \\ &= \sum_{h \in G} \left(f(h) - \frac{1}{|G|}\right)\left(f(gh^{-1}) - \frac{1}{|G|}\right) + \frac{2}{|G|}\sum_{h \in G} f(h) - \frac{1}{|G|} \\ &= \frac{1}{|G|} + \sum_{h \in G} \left(f(h) - \frac{1}{|G|}\right)\left(f(gh^{-1}) - \frac{1}{|G|}\right),\end{aligned}$$

since $\sum f(h) = 1$. Applying the Cauchy-Schwarz-inequality to the last sum, our claim follows. □

We can now explain how to deduce Theorem 2 from Theorem 1. Let $\mathbf{c} \subseteq S_n$ be a non-trivial conjugacy class. Arguing as in the proof of Lemma 2 we know that $w_\mathbf{c}$ reaches $\frac{1}{n}$-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 Theorem 1, the left-hand side can be bounded above by

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

For $k \geq 10t_c(\mathbf{c})$, this in turn is less than

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

and from [27, Theorem 1] we deduce that the latter quantity is $\mathcal{O}(n^{-5/4})$. Hence, for n sufficiently large, we obtain the bound $t_s(\mathbf{c}) \leq 10t_c(\mathbf{c})$. We postpone the argument leading to the lower bound $n \geq 4000$ to the end of the proof of Theorem 1 in Subsection 2.4.

2.3. **Estimates for Character Values.** Our main tools in this subsection are the hook formula for the dimension of χ_λ and the Murnaghan-Nakayama rule.

The hook formula.[4] *We have*

$$\chi_\lambda(1) = \frac{n!}{\prod_{(i,j)\in\lambda} h_{i,j}}, \tag{11}$$

where $h_{i,j}$ is the hook length of the box (i,j).

The Murnaghan-Nakayama rule describes a procedure to recursively compute arbitrary character values.

Murnaghan-Nakayama rule.[5] *Let $\pi = \sigma\gamma$ be the disjoint product of $\sigma \in S_{n-k}$ and a k-cycle γ. Then we have*

$$\chi_\lambda(\pi) = \sum_\tau (-1)^{l(\tau)} \chi_{\lambda\setminus\tau}(\sigma). \tag{12}$$

Here, the sum extends over all rim hooks τ of size k in λ, and $l(\tau)$ is the leg length of τ.

Let λ be a partition of n. By $\mathrm{sq}(\lambda)$ we mean the side length of the largest square contained in the Ferrers diagram of λ; that is, the largest j such that $\lambda_j \geq j$. Note that for $\lambda \vdash n$ we have

$$(\mathrm{sq}(\lambda) - 1)\mathrm{sq}(\lambda) \leq n - \lambda_1, \tag{13}$$

which we will apply mostly in the simpler version $\mathrm{sq}(\lambda) \leq \sqrt{n-\lambda_1} + 1$. The quantity $\mathrm{sq}(\lambda)$ leads to a useful inequality for $\chi_\lambda(1)$.

Lemma 4. *Let λ be a partition of n, and let $s = \mathrm{sq}(\lambda)$. Then*

$$\chi_\lambda(1) \geq \binom{n}{s^2} \left(\frac{s}{n}\right)^{s^2} (s^2)!.$$

Proof. Each of the $n - s^2$ points of λ outside the maximal square lies in precisely s hooks h_{ij} with $i, j \leq s$, while the point (i,j) with $i, j \leq s$ lies in exactly $i + j - 1$ such hooks. Hence,

$$\sum_{i,j\leq s} h_{ij} = s(n - s^2) + \sum_{i,j\leq s} (i + j - 1) = sn.$$

By the arithmetic-geometric inequality, this gives

$$\prod_{i,j\leq s} h_{ij} \leq \left(\frac{1}{s^2} \sum_{i,j\leq s} h_{ij}\right)^{s^2} = \left(\frac{n}{s}\right)^{s^2}.$$

Bounding the product of the hook lengths corresponding to points outside the maximal square by $(n - s^2)!$, our claim follows from the hook formula. □

Our next result gives an upper bound for the modulus of character values $\chi_\lambda(\mathbf{c})$ in terms of $\mathrm{sq}(\lambda)$ and the number of cycles of $\mathbf{c}$.

[4] COnfer, for instance, [15, Theorem 2.3.21]

[5] Confer, for instance, [15, Formula 2.4.7]

Lemma 5. *Let* $\mathbf{c} \subseteq S_n$ *be a conjugacy class with* c *cycles, and let* $\lambda \vdash n$ *be a partition. Then we have*

$$|\chi_\lambda(\mathbf{c})| \leq (2\mathrm{sq}(\lambda))^c.$$

Proof. If $\mu \subseteq \lambda$ is a partition, then certainly $\mathrm{sq}(\mu) \leq \mathrm{sq}(\lambda)$, hence, arguing by induction on c and applying the Murnaghan-Nakayama rule, it suffices to show that for any given k, a partition λ has at most $2\mathrm{sq}(\lambda)$ removable rim hooks of length k. Let r be such a rim hook. The right-uppermost box of r is either to the right of the maximal square contained in the Ferrers diagram of λ, or the left-lowest box of r is below the maximal square of λ, or both. Since the right-uppermost box of a rim hook is always at the end of a row, while the left-lowest box is at the end of a column, our claim follows. □

If λ_1 is of similar size as n, Lemma 5 is of little use. In this case we will apply the following.

Lemma 6. *Let* $\lambda \vdash n$ *be a partition, and let* $\mathbf{c} \subseteq S_n$ *be a conjugacy class with* c *cycles of length* ≥ 2 *and* f *fixed points. Then we have the bounds*

$$|\chi_\lambda(\mathbf{c}))| \leq \chi_{\lambda\setminus\lambda_1}(1) \sum_{\substack{a,b\geq 0\\ a+2b\leq n-\lambda_1}} \binom{f}{a}\binom{c-f}{b}. \tag{14}$$

and

$$|\chi_\lambda(\mathbf{c})| \leq n \max_{\nu\leq n-\lambda_1} (2\sqrt{n-\lambda_1})^\nu \binom{c}{\nu}, \tag{15}$$

which improves on (14) *if* c *is considerably smaller then* $n - \lambda_1$.

Proof. Neglecting the sign in the Murnaghan-Nakayama rule, we see that the modulus of $\chi_\lambda(\mathbf{c})$ is bounded above by the number of possible ways to completely deconstruct λ by removing rim hooks of sizes given by the cycle structure of $\mathbf{c}$. To prove the first estimate, we classify these deconstructions by means of the number a of fixed points of $\mathbf{c}$ contained within $\lambda \setminus \lambda_1$, and the corresponding number b of cycles of lengths ≥ 2. Given a and b, there are $\binom{f}{a}$ ways to choose the fixed points of $\mathbf{c}$ to be removed from $\lambda \setminus \lambda_1$, and $\binom{c-f}{b}$ ways to choose the corresponding set of cycles. Once these sets are given, there are at most $\chi_{\lambda\setminus\lambda_1}(1)$ ways to remove these fixed points and cycles.

For the second bound we argue in a similar manner, this time bounding the number of deconstructions of $\lambda \setminus \lambda_1$ as in the proof of Lemma 5. □

The next lemma will be useful in computing values of characters of small degrees.

Lemma 7. *Let* $\lambda \vdash n$ *be a partition,* $\mu = \lambda \setminus \lambda_1$, *and let* $\pi \in S_n$ *be a permutation. Then*

$$\chi_\lambda(\pi) = \sum_{\substack{\tilde{\mu}\subseteq\mu\\ \tilde{\mu}_1=1}} (-1)^{|\tilde{\mu}|} \sum_{\mathbf{c}\subseteq S_{|\mu|-|\tilde{\mu}|}} \chi_{\mu,\tilde{\mu}}(\mathbf{c}) \prod_{i\leq|\mu|} \binom{c_i(\pi)}{c_i},$$

where $\mathbf{c}$ *runs over all conjugacy classes of* $S_{|\mu|-|\tilde{\mu}|}$, $\chi_{\mu,\tilde{\mu}}(\mathbf{c})$ *denotes the number of ways to obtain* $\tilde{\mu}$ *from* μ *by removing rim hooks according to the cycle structure of* $\mathbf{c}$, *counted* *with the sign prescribed by the Murnaghan-Nakayama rule, and c_i is the number of i-cycles of an element of* $\mathbf{c}$.

Proof. We may assume that $\lambda_1 > 2|\mu|$, and that π contains a cycle of length $> |\mu|$. For, if we replace λ_1 by $\lambda_1 + 2n$, and add a cycle of length $2n$ to π, both conditions are satisfied; on the other hand, the only way to remove a cycle of length $2n$ from the new partition is within the first row, hence $\chi_\lambda(\pi)$ is not affected by these changes. Now we use the Murnaghan-Nakayama rule to remove all cycles of length $\leq |\mu|$. If we are left with a partition not of the form $\tilde{\lambda} = (\tilde{\lambda}_1, 1, \dots, 1)$, the remaining partition cannot be removed by deleting rim hooks of length $> |\mu|$, so $\tilde{\mu} = \tilde{\lambda} \setminus \tilde{\lambda}_1$ can be assumed to be of the form $(1, \dots, 1)$. Since $\tilde{\lambda}$ can be removed in precisely one way by deleting rim hooks of lengths $> |\mu|$, and all but the last one are contained in the first row, the value of $\chi_{\tilde{\lambda}}(\tilde{\pi})$ is $(-1)^{|\tilde{\mu}|}$, where $\tilde{\pi}$ is the element obtained from π by removing all cycles of lengths $\leq |\mu|$. The rim hooks which are removed and do not contain any box from the first row define a conjugacy class $\mathbf{c}$ within $S_{|\mu|-|\tilde{\mu}|}$; counting all possible placements of the cycles of $\mathbf{c}$ in $\mu \setminus \tilde{\mu}$ with the sign prescribed by the Murnaghan-Nakayama rule yields $\chi_{\mu,\tilde{\mu}}(\mathbf{c})$. Finally, for fixed $\mathbf{c}$, the set of i-cycles to be placed in $\mu \setminus \tilde{\mu}$ among all i-cycles of π can be chosen in $\binom{c_i(\pi)}{c_i}$ ways, and our claim follows. □

Finally, we shall also need the following lower bounds for character degrees.

Lemma 8. *Let $\lambda \vdash n$ be a partition. Then*

(i) $\chi_\lambda(1) \geq 2^{n/8}, \quad \|\lambda\| \leq \lambda_1 \leq 3n/4;$

(ii) $\chi_\lambda(1) \geq \binom{\lambda_1}{n-\lambda_1}\chi_{\lambda\setminus\lambda_1}(1), \quad \lambda_1 \geq n/2.$

Proof. (i) We distinguish the cases $\lambda_1 \leq n/4$, $\lambda_1 \geq n/4$ and $\lambda_2 \leq n/8$, and $\lambda_1 \geq n/4, \lambda_2 \geq n/8$. In the first case it was shown in [27, Formula (23)] that $\chi_\lambda(1) \geq (3/2)^{n/4} \geq 2^{n/8}$. In the second case, for any given $\lfloor n/8 \rfloor$-tuple $(t_1, \dots, t_{\lfloor n/8 \rfloor})$ of 0's and 1's, we can start to deconstruct λ by choosing in the i-th step a box from the first row, if $t_i = 1$, and from $\lambda \setminus \lambda_1$, if $t_i = 0$. Hence, there are at least $2^{n/8}$ ways of deconstruction. In the final case, note that $\chi_\lambda(1) \geq \chi_\mu(1)$ for any partition μ contained in λ; choosing $\mu = (\lfloor n/4 \rfloor, \lfloor n/8 \rfloor)$, our claim follows by applying to μ the argument used in the second case.

(ii) This follows as in the proof of [27, Formula (21)], observing that the hook product $H[(\lambda_2, \dots, \lambda_k)]$ equals $\frac{(n-\lambda_1)!}{\chi_{\lambda\setminus\lambda_1}(1)}$. □

2.4. **Proof of Theorem 1.** The proof of Theorem 1 makes use of the following two auxiliary results, whose proofs will be given in the next subsection.

Lemma 9. *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 $3t_c(\mathbf{c})$ steps. Then, for each $k \geq 1$, 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 10. *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*

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

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*

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

The proof of Theorem 1 now proceeds as follows. Define $g_1 : S_n \to [0, \infty)$ to be the density of the random walk $w_{\mathbf{c}}$ after $3t_c(\mathbf{c})$ steps, and let g_2 be the corresponding density after $6t_c(\mathbf{c})$ steps. Using the fact that g_1 is a class function, we decompose g_1 as

$$g_1 = \sum_{\mathbf{c}'} \alpha_{\mathbf{c}'} \mathbf{1}_{\mathbf{c}'},$$

and compute g_2 in the form

$$g_2(\pi) = \sum_{\sigma \in S_n} g_1(\sigma) g_1(\pi\sigma^{-1}) = \sum_{\mathbf{c}_1, \mathbf{c}_2} \alpha_{\mathbf{c}_1}\alpha_{\mathbf{c}_2} \big|\big\{(c_1, c_2) \in \mathbf{c}_1 \times \mathbf{c}_2 : c_1c_2 = \pi\big\}\big|.$$

From Lemmas 5, 9, and 10 we deduce that

$$\begin{aligned}
|\langle g_2, \chi_\lambda\rangle| &\leq \frac{1}{n!}\sum_{\mathbf{c}_1,\mathbf{c}_2} \alpha_{\mathbf{c}_1}\alpha_{\mathbf{c}_2} \sum_{\substack{c_1 \in \mathbf{c}_1\\ c_2 \in \mathbf{c}_2}} (2\operatorname{sq}(\lambda))^{\#\text{ cycles of } c_1c_2}\\
&= \frac{1}{n!}\sum_{k,l} (2\operatorname{sq}(\lambda))^{k+l} \sum_{\mathbf{c}_1,\mathbf{c}_2} \alpha_{\mathbf{c}_1}\alpha_{\mathbf{c}_2} |\mathbf{c}_1||\mathbf{c}_2| P_{k,l}(\mathbf{c}_1, \mathbf{c}_2)\\
&\leq \frac{1}{n!}\sum_{k,l} (2\operatorname{sq}(\lambda))^{k+l} \sum_{f_1, f_2 \geq l} \sum_{\substack{\mathbf{c}_1,\mathbf{c}_2\\ c_1(\mathbf{c}_1) = f_1\\ c_1(\mathbf{c}_2) = f_2}} \alpha_{\mathbf{c}_1}\alpha_{\mathbf{c}_2} |\mathbf{c}_1||\mathbf{c}_2| \binom{n}{l}\left(\frac{f_1f_2}{n^2}\right)^l \frac{(\log n)^{k-1}}{(k-1)!}\\
&= \frac{1}{n!}\sum_{k,l}\sum_{f_1, f_2 \geq l} (2\operatorname{sq}(\lambda))^{k+l} \binom{n}{l}\left(\frac{f_1f_2}{n^2}\right)^l \frac{(\log n)^{k-1}}{(k-1)!}\\
&\qquad \times \Bigg(\sum_{\substack{\mathbf{c}_1\\ c_1(\mathbf{c}_1) = f_1}} \alpha_{\mathbf{c}_1}|\mathbf{c}_1|\Bigg)\Bigg(\sum_{\substack{\mathbf{c}_2\\ c_1(\mathbf{c}_2) = f_2}} \alpha_{\mathbf{c}_2}|\mathbf{c}_2|\Bigg)\\
&\leq \frac{1}{n!}\sum_{k,l}\sum_{f_1, f_2 \geq l} (2\operatorname{sq}(\lambda))^{k+l} \binom{n}{l}\left(\frac{f_1f_2}{n^2}\right)^l \frac{(\log n)^{k-1}}{(k-1)!}\\
&\qquad \times \max\Big(\frac{f_1 2^{f_1}}{f_1!}, \frac{2^{n/2}}{(\lfloor n/2\rfloor - 1)!}\Big) \max\Big(\frac{f_2 2^{f_2}}{f_2!}, \frac{2^{n/2}}{(\lfloor n/2\rfloor - 1)!}\Big).
\end{aligned}$$

Here, $P_{k,l}(\mathbf{c}_1, \mathbf{c}_2)$ denotes the probability that, for x_1 and x_2 chosen at random from $\mathbf{c}_1$ respectively $\mathbf{c}_2$, x_1 and x_2 have l common fixed points, and the product x_1x_2 has precisely k cycles on the remaining $n-l$ points. If f_1 is in the interval $[l, n/2]$, increasing f_1 by 1 changes the value of a summand by a factor

$$2\left(\frac{f_1+1}{f_1}\right)^{l+1}\frac{1}{f_1}\leq\frac{2e}{f_1},$$

while each summand increases with f_1 in the range $n/2 \leq f_1 \leq n$. The same is true for f_2; hence, by symmetry, we obtain

$$\begin{aligned} n!\,|\langle g_2,\chi_\lambda\rangle| &\leq 80n^2\sum_{k,l}(2\mathrm{sq}(\lambda))^{k+l}\binom{n}{l}\left(\frac{l^2}{n^2}\right)^l\frac{(\log n)^{k-1}}{(k-1)!}\left(\frac{2^l}{(l-1)!}\right)^2 \\ & +80n^2\sum_{k,l}(2\mathrm{sq}(\lambda))^{k+l}\binom{n}{l}\frac{(\log n)^{k-1}}{(k-1)!}\left(\frac{2^{n/2}}{(\lfloor n/2\rfloor-1)!}\right)^2. \end{aligned}$$

For $n\to\infty$, the second sum tends to zero; thus, applying Stirling's formula,

$$\begin{aligned} n!\,|\langle g_2,\chi_\lambda\rangle| &\leq 1+80n^2\sum_{k,l}\frac{(2\mathrm{sq}(\lambda)\log n)^k}{(k-1)!}\cdot\frac{(8\mathrm{sq}(\lambda)nl^2)^l}{l!((l-1)!)^2n^{2l}} \\ &\leq 1+80n^5\sum_{k,l}\frac{(2\mathrm{sq}(\lambda)\log n)^k}{k!}\cdot\left(\frac{8e^3\mathrm{sq}(\lambda)}{ln}\right)^l. \end{aligned}$$

Since $\mathrm{sq}(\lambda)\leq\sqrt{n}$, the second factor tends to zero, as n tends to infinity, while the summation over k yields an exponential series. Hence, we obtain the bound

$$n!\,|\langle g_2,\chi_\lambda\rangle|\leq n^{2\mathrm{sq}(\lambda)+7}.$$

On the other hand, from Lemma 4, we deduce the bound $\chi_\lambda(1)\geq(\mathrm{sq}(\lambda)/e)^{\mathrm{sq}(\lambda)^2}$, and for $\chi_\lambda(1)>e^{3(\log n)^4}$, we deduce that

$$n!\,|\langle g_2,\chi_\lambda\rangle|\leq\chi_\lambda(1)^{1/(\log n)}.$$

By Lemma 1 (ii), we have

$$n!\,|\langle g_2,\chi_\lambda\rangle| = n!\frac{\left|\left\langle\frac{1}{|c|}\mathbf{1}_{\mathbf{c}},\chi_\lambda\right\rangle\right|^{6t_c(\mathbf{c})}(n!)^{6t_c(\mathbf{c})-1}}{\chi_\lambda(1)^{6t_c(\mathbf{c})-1}} = \frac{|\chi_\lambda(\mathbf{c})|^{6t_c(\mathbf{c})}}{\chi_\lambda(1)^{6t_c(\mathbf{c})-1}},$$

and together with our estimate for $|\langle g_2,\chi_\lambda\rangle|$ we obtain

$$|\chi_\lambda(\mathbf{c})|\leq(\chi_\lambda(1))^{1-\frac{1-1/(\log n)}{6t_c(\mathbf{c})}}.$$

Before establishing the upper bound for $|\chi_\lambda(\mathbf{c})|$ for characters associated to partitions λ satisfying $n-\lambda_1\leq 3\log^4 n$, we prove the estimate for $t_c(\mathbf{c})$. Let ξ_k be the random variable which for permutations $\pi_1,\dots,\pi_k$ chosen independently at random from $\mathbf{c}$ counts the number of points fixed by all of them. The probability that 1 is fixed by all of the permutations equals $\left(\frac{c_1(\mathbf{c})}{n}\right)^k$, whereas the probability that both 1 and 2 are fixed by all the permutations equals

$$\left(\frac{c_1(\mathbf{c})(c_1(\mathbf{c})-1)}{n(n-1)}\right)^k.$$

Hence, $E\xi_k = n\left(\frac{c_1(\mathbf{c})}{n}\right)^k$, and

$$E(\xi_k^2) = n\left(\frac{c_1(\mathbf{c})}{n}\right)^k + n(n-1)\left(\frac{c_1(\mathbf{c})(c_1(\mathbf{c})-1)}{n(n-1)}\right)^k \leq E\xi_k + (E\xi_k)^2.$$

Using the fact that ξ_k takes only integral values, we deduce the inequality

$$1 - E\xi_k \leq P(\xi_k = 0) \leq 1 - E\xi_k + \frac{1}{2}\big(E\xi_k\big)^2;$$

hence, we obtain for $t_c(\mathbf{c})$ the bounds

$$\min\left\{k \in 2\mathbb{N} : \left(\frac{c_1(\mathbf{c})}{n}\right)^k \leq \frac{1}{n(n-1)}\right\} \leq t_c(\mathbf{c}) \leq \min\left\{k \in 2\mathbb{N} : \left(\frac{c_1(\mathbf{c})}{n}\right)^k \leq \frac{1}{n^2}\right\}.$$

Since $c_1(\mathbf{c}) \leq n-2$ for every non-trivial class, the solutions of the equations

$$\left(\frac{c_1(\mathbf{c})}{n}\right)^k = \frac{1}{n(n-1)} \quad \text{and} \quad \left(\frac{c_1(\mathbf{c})}{n}\right)^k = \frac{1}{n^2}$$

differ by less than 1. Solving for k gives our claim.

Now we bound $\chi_\lambda(\mathbf{c})$ with $n - \lambda_1 \leq 3\log^4 n$ using Lemma 6. We have

$$|\chi_\lambda(\mathbf{c})| \leq \chi_{\lambda\setminus\lambda_1}(1) \sum_{a+2b\leq n-\lambda_1} \binom{c_1(\mathbf{c})}{a}\binom{\lfloor n/2\rfloor}{b}.$$

Assume first that $c_1(\mathbf{c}) \leq n^{2/3}$. Then, using Lemma 8 (ii),

$$|\chi_\lambda(\mathbf{c})| \leq (n-\lambda_1)!^{1/2} \sum_{a+2b\leq n-\lambda_1} n^{2a/3+b} \leq 2(n-\lambda_1)!^{3/2}\binom{n}{\lfloor 2(n-\lambda_1)/3\rfloor} \leq \chi_\lambda(1)^{2/3+\varepsilon},$$

which is sufficiently small, since $t_c(\mathbf{c}) \geq 2$. If, on the other hand, $c_1(\mathbf{c}) > n^{2/3}$, replacing b by $b-1$ and a by $a+2$ changes the value of a summand by

$$\frac{(c_1(\mathbf{c})-a)(c_1(\mathbf{c})-a-1)b}{(a+1)(a+2)(n/2-b+1)} > n^{1/4},$$

and, if $a + 2b < n - \lambda_1$, replacing a by $a+1$ changes the value of a summand by $\frac{c_1(\mathbf{c})-a}{a+1} > n^{1/2}$, hence, for n sufficiently large, the whole sum over a and b is at most twice its greatest term. Again using Lemma 8, we deduce from this that

$$|\chi_\lambda(\mathbf{c})| \leq 2\chi_{\lambda\setminus\lambda_1}(1)\binom{c_1(\mathbf{c})}{n-\lambda_1} \leq 2\chi_\lambda(1)\left(\frac{c_1(\mathbf{c})}{n}\right)^{n-\lambda_1} < 2\chi_\lambda(1)^{1-\frac{\log(n/c_1(\mathbf{c}))}{\log n}},$$

which is again sufficiently small by the lower bound for $t_c(\mathbf{c})$.

We now sketch the computations needed to show that Theorem 2 holds in fact for all $n \geq 4000$. In the form given above, the proof only applies to $n \geq e^{40}$. First, in the deduction of Theorem 2 from Theorem 1, we can handle the characters $\chi_{(n-1,1)}$, $\chi_{(2,1,1,\dots,1)}$ separately, noting that for $n \geq 4000$ we have

$$\sum_\lambda{}^{*} \chi_\lambda(1)^{-0.7} < \frac{1}{n}$$

where the summation is extended over all partitions $\lambda \vdash n$ apart from (n), $(n-1,1)$, $(2,1,1,\dots,1)$ and $(1,1,\dots,1)$. Following through the proof of Theorem 1, we find that the contribution of all characters χ_λ with $\lambda_1 \leq 3n/4$ or $n-\lambda_1 \leq n^{1/3}$ is sufficiently small. To close this gap, we estimate $|\langle g_2, \chi_\lambda\rangle|$ as above, but use Lemma 6 instead of Lemma 5, that is, the bound for $|\chi_\lambda(\mathbf{c})|$ now reads

$$\min\left(\chi_\lambda(1), \max_{\nu\leq n-\lambda_1}(2\sqrt{n-\lambda_1})^\nu\binom{k+l}{\nu}\right) \quad \text{instead of } (2\mathrm{sq}(\lambda))^{k+l};$$

as a result, we obtain a bound of sufficient quality for all characters χ_λ satisfying $\chi_\lambda(1) > 2e^{\frac{10}{19}\log^2 n+\frac{20}{19}\log n}$; and we conclude the proof by noting that for $n \geq 4000$, the degree of a character χ_λ with $\|\lambda\| \leq \lambda_1 < n - n^{1/3}$ is larger than this bound.

Note that in the intermediate range, we established a bound somewhat weaker than Theorem 1; in particular, we do not claim that Theorem 1 holds for all $n \geq 4000$. However, it may well be true that both theorems are in fact true for all integers n without any exception.

2.5. **Proof of Lemmas 9 and 10.** To complete the proof of Theorem 1, it remains to establish Lemmas 9 and 10.

Proof of Lemma 9. Let a, b be integers, and let $\pi_1,\dots,\pi_{3t_c(\mathbf{c})} \in \mathbf{c}$ be elements chosen at random. Denote by $P(a,b)$ the probability that the points $1,\dots,a$ are fixed by all the π_i, and that, for each β with $a+1 \leq \beta \leq a+b$, there is some i such that π_i moves β, while the product $\pi_1\cdots\pi_{3t_c(\mathbf{c})}$ fixes β. We have

$$P(a,0) = P(\pi_1 \text{ fixes } 1,\dots,a)^{3t_c(\mathbf{c})} \leq P(\pi_1 \text{ fixes } 1)^{3at_c(\mathbf{c})} = \left(\left(\frac{c_1(\mathbf{c})}{n}\right)^{t_c(\mathbf{c})}\right)^{3a}.$$

By the definition of $t_c(\mathbf{c})$, we have $\left(\frac{c_1(\mathbf{c})}{n}\right)^{t_c(\mathbf{c})} < \frac{1}{n}$; hence, $P(a,0)$ is bounded by n^{-3a}. Next, consider $P(0,b)$. The product $\pi_1\cdots\pi_{3t_c(\mathbf{c})}$ fixes β if and only if

$$\big(\pi_1\cdots\pi_{3t_c(\mathbf{c})-1}\big)(\beta) = \pi^{-1}_{3t_c(\mathbf{c})}(\beta).$$

Let $h \in \mathrm{Sym}\big([n]\setminus\{(\pi_1\cdots\pi_{3t_c(\mathbf{c})-1})(\gamma) : \gamma \leq b, \gamma\neq\beta\}\big)$ be chosen at random. Then replacing $\pi_{3t_c(\mathbf{c})}$ by $\pi^h_{3t_c(\mathbf{c})}$ does not alter $(\pi_1\cdots\pi_{3t_c(\mathbf{c})-1})(\gamma)$ for $\gamma \leq b, \gamma \neq \beta$, while $\big(\pi_1\cdots\pi_{3t_c(\mathbf{c})-1}\big)(\beta) = \big(\pi^h_{3t_c(\mathbf{c})}\big)^{-1}(\beta)$ holds with probability $\frac{1}{n-b-1}$ or 0. Since the π_i are chosen from a conjugacy class, conjugating with a random element from some subgroup does not affect the equidistribution of the π_i, hence, we obtain $P(0,b) \leq (n-b+1)^b$. Finally, a permutation $\pi \in S_n$ that fixes the points $1,\dots,a$ can be viewed as a permutation on $n-a$ elements, thus $P(a,b) \leq n^{-3a}(n-a-b+1)^{-b}$. If $a+b \leq n/2$, we deduce $P(a,b) \leq \frac{2^b}{n^{3a+b}}$, and, summing over all pairs a,b with $a+b \geq k$ we obtain our claim. Note that P is decreasing in both a and b; hence, if $a+b > n/2$, we may replace the pair (a,b) by some pair (a',b') satisfying $a'+b' = \lfloor n/2\rfloor$ and use our estimate for the latter pair. Since the probability that there exist k points which are fixed by the product $\pi_1\cdots\pi_{3t_c(\mathbf{c})}$ is at most $\binom{n}{k}$ times the probability that $\pi_1\cdots\pi_{3t_c(\mathbf{c})}$ fixes the points $1,\dots,k$, our claim follows. □

Proof of Lemma 10. The probability that both x_1 and x_2 fix 1 equals $\frac{f_1 f_2}{n^2}$, and the conditional probability

$$P\big(x_1 \text{ and } x_2 \text{ fix } 1 \,|\, \exists a_1, \dots a_k : a_i \neq 1,\, x_1 \text{ and } x_2 \text{ fix } a_i, \forall i \leq k\big)$$

is smaller, thus, the first claim of the lemma follows. Now let x_1, x_2 be chosen at random from $\mathbf{c}_1$ and $\mathbf{c}_2$, respectively. Assume that not both of them fix 1, without loss we assume that $x_1(1) \neq 1$. Then 1 lies in a cycle of length i of x_1x_2 if and only if

$$\big(x_2(x_1x_2)^{i-1}\big)(1) = x_1^{-1}(1) \tag{16}$$

with i chosen minimal among all positive integers with this property. Choose an element $h \in \mathrm{Sym}\big([n] \setminus \{x_2(x_1x_2)^j(1) : 0 \leq j \leq i-2\}\big)$ at random, and replace x_1 by x_1^h. Then (16) becomes true with probability $\frac{1}{n-i+1}$. Increasing i until (16) happens to hold, we obtain one cycle of x_1x_2. Next, choose some point outside this cycle, and repeat the procedure, where h is to be chosen in such a way that h fixes all points in all cycles already determined as well as the points already constructed in the current cycle. In this way, we obtain the number c of cycles of x_1x_2 as the value returned by the following

Stochastic Algorithm

```
(i) Set $m := n, i := 0$ and $c := 0$.
(ii) Increase $i$ by 1.
(iii) With probability $1 - \frac{1}{m-i+1}$, go to (ii); otherwise continue with (iv).
(iv) Set $m := m - i$, $c := c + 1$ and $i := 0$.
(v) If $m = 0$, stop and return $c$; otherwise go to (ii).
```

Let P be the probability that x_1x_2 has k cycles, and that their lengths are $c_1, \dots c_k$. Then, in step (iii) of the algorithm, the second possibility was chosen k times, and the probabilities were $\frac{1}{n-c_1+1}, \frac{1}{n-c_1-c_2+1}, \dots, \frac{1}{n-c_1-\dots-c_k+1}$, respectively. Hence, P is bounded above by the product of these probabilities; and, writing $i_j := c_{k-j+1} + \cdots + c_k + 1$, we obtain

$$\begin{aligned} P(x_1x_2 \text{ has } k \text{ cycles}) &\leq \sum_{1=i_1<i_2<\cdots<i_k\leq n} \prod_{j=1}^{k} \frac{1}{i_j} \\ &\leq \frac{1}{(k-1)!} \sum_{2\leq i_2,\dots,i_k\leq n} \prod_{j=1}^{k} \frac{1}{i_j} \\ &= \frac{1}{(k-1)!} \left(\sum_{2\leq i\leq n} \frac{1}{i} \right)^{k-1} \\ &\leq \frac{(\log n)^{k-1}}{(k-1)!}, \end{aligned}$$

which proves our claim. □

3. Character estimates for elements of prescribed order

As it stands, Theorem 1 is not strong enough to obtain an asymptotic estimate for the subgroup growth of Fuchsian groups. When combined with the methods of Subsection 3.2, it could be used to determine the asymptotics of $s_n(\Gamma)$ for certain Fuchsian groups Γ, namely those given by a presentation of the form

$$\Gamma = \Big\langle x_1, \dots, x_r \,\Big|\, x_1^{a_1} = x_2^{a_2} = \cdots = x_r^{a_r} = x_1 x_2 \cdots x_r = 1 \Big\rangle$$

where $a_i \geq 2$ and $r \geq 73$. Unfortunately, this would exclude all better known examples in this class. From the point of view of an application to the subgroup growth of Fuchsian groups, the weakness of Theorem 1 is caused by its generality. Combining instead an estimate by Fomin and Lulov [11] for character values $\chi_\lambda(\pi)$ where all cycle lengths of π are equal, with combinatorial arguments plus the estimates of Subsection 2.3, we shall derive the following sharper estimate.

Proposition 1. *Let $q \geq 2$ be an integer, $\varepsilon > 0$, and let n be sufficiently large. Then, for every partition $\lambda \vdash n$, we have*

$$\sum_{\substack{\pi \in S_n \\ \pi^q = 1}} |\chi_\lambda(\pi)| \leq \big(\chi_\lambda(1)\big)^{\frac{1}{q}+\varepsilon} |\operatorname{Hom}(C_q, S_n)|. \tag{17}$$

We begin with some results concerning the statistical distribution of permutations in S_n and in wreath products, which will be used in the proof of Proposition 1 as well as in the next section.

3.1. Statistics of the symmetric group.

For integers $n \geq 1$ and $q \geq 2$, define $N(n, q)$ to be the number of elements $\pi \in S_n$ with $\pi^q = 1$. Furthermore, for integers c_t with $t|q$ and $t < q$, define $N(n, q, c_1, \dots, c_T)$, to be the number of elements $\pi \in S_n$ with $\pi^q = 1$ and $c_t(\pi) = c_t$ for all $t|q, t < q$.

Lemma 11. *Let $q \geq 2$ be an integer, n sufficiently large, and let $c_1, \dots, c_T$ be given in such a way that $n \equiv 1 \cdot c_1 + \cdots + T \cdot c_T \pmod q$. Then we have the estimate*

$$\frac{N(n, q, c_1, \dots, c_T)}{N(n, q)} \leq q^{\sigma(q)} \prod_{\substack{t \\ c_t > 2en^{t/q}}} \left(\frac{en^{t/q}}{tc_t}\right)^{c_t}, \tag{18}$$

where $\sigma(q)$ denotes the sum of divisors of q.

Proof. Put $\mathcal{S} := \sum\limits_{\substack{t|q \\ t \neq q}} tc_t$. We have

$$N(n, q, c_1, \dots, c_T) = \frac{n!}{((n - \mathcal{S})/q)! c_1! \cdots c_T! 1^{c_1} \cdots T^{c_T} \cdot q^{(n-\mathcal{S})/q}}.$$

Let

$$\tilde{c_t} := \begin{cases} c_t, & c_t \leq 2en^{t/q}, \\ c_t \bmod q/t, & c_t > 2en^{t/q} \end{cases} \qquad (t|q,\, t < q),$$

where c_t mod q/t takes values in $\{0, 1, \dots, q/t-1\}$, and put $\tilde{\mathcal{S}} := \sum\limits_{\substack{t|q\\ t\neq q}} t\tilde{s}_t$. Then we get

$$\begin{aligned}
\frac{N(n,q,c_1,\dots,c_T)}{N(n,q)} &\leq \frac{N(n,q,c_1,\dots,c_T)}{N(n,q,\tilde{s}_1,\dots,\tilde{s}_T)}\\
&= \frac{((n-\tilde{\mathcal{S}})/q)!\tilde{s}_1!\cdots\tilde{s}_T!1^{\tilde{s}_1}\cdots T^{\tilde{s}_T}\cdot q^{(n-\tilde{\mathcal{S}})/q}}{((n-\mathcal{S})/q)!c_1!\cdots c_T!1^{c_1}\cdots T^{c_T}\cdot q^{(n-\mathcal{S})/q}}\\
&\leq \prod_{\substack{t\\ c_t>2en^{t/q}}} \frac{n^{tc_t/q}(q/t)!}{c_t!t^{c_t-q/t}}\\
&\leq \prod_{\substack{t\\ c_t>2en^{t/q}}} q^{q/t}\left(\frac{en^{t/q}}{tc_t}\right)^{c_t}\\
&\leq q^{\sigma(q)}\prod_{\substack{t\\ c_t>2en^{t/q}}}\left(\frac{en^{t/q}}{tc_t}\right)^{c_t},
\end{aligned}$$

as claimed. □

For a conjugacy class $\mathbf{c}$ of S_n, denote by $C_{S_n}(\mathbf{c})$ the centraliser of $\mathbf{c}$ in S_n. Then $C_{S_n}(\mathbf{c})$ is isomorphic to a direct product of the form

$$C_{S_n}(\mathbf{c}) \cong \prod_{d|q} C_d \wr S_{c_d(\sigma)},$$

where σ is some element of $\mathbf{c}$.

Lemma 12. *Let q and k be integers, and let $\mathbf{c}\in S_n$ be a conjugacy class with $\mathbf{c}^q = 1$.*

(i) *The number of $\pi\in S_n$ with at least k cycles is bounded above by*

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

(ii) *The number of $\pi\in C_{S_n}(\mathbf{c})$ with at least k cycles is bounded above by*

$$|C_{S_n}(\mathbf{c})|\left(\frac{3q\log n}{k}\right)^{k/q},$$

provided that $k\geq(\log n)^3$ and $n\geq n_0(q)$.

Proof. (i) Let $\pi\in S_n$ be chosen at random. Then 1 is a fixed point of π with probability $\frac{1}{n}$. If it is not a fixed point, then it lies in a 2-cycle with probability $\frac{1}{n-1}$, and, more generally, the conditional probability for 1 to lie in a cycle of length c, provided that it lies in a cycle of length at least c is $\frac{1}{n-c+1}$. Arguing now as in the proof of Lemma 10 establishes our claim.

(ii) Consider a single direct factor $G := C_d\wr S_{c_d(\sigma)}$ of $C_{S_n}(\mathbf{c})$, and let $\phi : G\to S_{c_d(\sigma)}$ be the canonical projection. Let c be a cycle in G. Then, the projection $\overline{c}$ of c in $S_{c_d(\sigma)}$ is a cycle, too, and there are at most d cycles $c_1,\dots,c_d\in G$ which have the same image in

$S_{c_d(\sigma)}$. We deduce that the probability that a permutation π, chosen at random in G, has k cycles is at most the probability that a permutation chosen at random in $S_{c_d(\sigma)}$ has $\lceil k/d \rceil$ cycles. Together with part (i) of this lemma, we obtain

$$\begin{aligned}
\frac{1}{|C_{S_n}(\mathbf{c})|}\left|\Big\{\pi \in C_{S_n}(\mathbf{c}) :\ |\mathrm{Orbits}(\pi)| \geq k\Big\}\right| &\leq \sum_{\sum_{d|q} d\kappa_d = k}\ \prod_{d|q} \min\left(1, \frac{(\log n)^{\kappa_d - 1}}{(\kappa_d - 1)!}\right)\\
&\leq k^{\tau(q)} \max_{\sum_{d|q} d\kappa_d = k} \prod_{d|q} \min\left(1, \frac{(\log n)^{\kappa_d - 1}}{(\kappa_d - 1)!}\right)\\
&\leq k^{\tau(q)} \max_{\sum_{d|q} d\kappa_d = k} \prod_{\substack{d|q\\ \kappa_d \geq 3\log n}} \frac{(\log n)^{\kappa_d - 1}}{(\kappa_d - 1)!}.
\end{aligned}$$

If we replace κ_d by $\kappa_d + \frac{q}{d}$, and κ_q by $\kappa_q - 1$, a single summand is changed by a factor

$$\frac{(\log n)^{\frac{q}{d}-1}(\kappa_q - 1)}{\kappa_d(\kappa_d + 1)\cdots(\kappa_d + q/d - 1)},$$

which is less than 1, provided that $\kappa_d > (\log n)\sqrt{\kappa_q}$. Hence, the maximum is attained for some tuple $(\kappa_1, \dots, \kappa_q)$ satisfying $\kappa_q \geq k/q - q\sqrt{k}\log n$. From this we deduce

$$\begin{aligned}
\frac{1}{|C_{S_n}(\mathbf{c})|}\left|\Big\{\pi \in C_{S_n}(\mathbf{c}) : |\mathrm{Orbits}(\pi)| \geq k\Big\}\right| &\leq k^{\tau(q)} \frac{(\log n)^{k/q - q\sqrt{k}(\log n) - 1}}{\lfloor k/q - q\sqrt{k}(\log n) - 1\rfloor !}\\
&\leq \left(\frac{3q\log n}{k}\right)^{k/q},
\end{aligned}$$

provided that $k \geq (\log n)^3$ and $n \geq n_0(q)$. □

Lemma 13. *Let $\pi \in S_n$ be chosen at random, and let d, d_1, d_2 be positive integers.*

(i) *As $n \to \infty$, the distribution of $c_d(\pi)$ converges to a Poisson distribution with mean $\frac{1}{d}$, and we have*

$$\frac{1}{n!}\sum_{\pi \in S_n} \big(c_d(\pi)\big)^q \to \sum_{\nu=1}^{q} d^{-\nu} S(q, \nu), \quad n \to \infty,$$

where the $S(q, \nu)$ are Stirling numbers of the second kind.

(ii) *As $n \to \infty$, the random variables $c_{d_1}(\pi)$ and $c_{d_2}(\pi)$ are asymptotically independent.*

Proof. (i) Let $P(d, k)$ be the probability that for π chosen at random from S_n, π contains the d-cycles $(12\dots d), (d+1\dots 2d), \dots, ((k-1)d+1\dots kd)$. Then, as $P(d, k) = \frac{(n-kd)!}{n!}$, we have for $k \leq n/d$,

$$\frac{1}{n!}\sum_{\pi \in S_n} \binom{c_d(\pi)}{k} = \frac{n!}{d^k k!(n-kd)!} P(d, k) = \frac{1}{d^k k!}.$$

On the other hand, for a random variable ξ which has Poisson distribution with mean $1/d$, we have

$$\mathbf{E}\binom{\xi}{k} = \sum_{\nu=0}^{\infty} \binom{\nu}{k} \frac{e^{-1/d}}{d^\nu \nu!} = \frac{e^{-1/d}}{d^k k!} \sum_{\nu=k}^{\infty} \frac{1}{(\nu-k)! d^{\nu-k}} = \frac{1}{d^k k!}.$$

We conclude that the first $\lfloor n/d \rfloor$ moments of ξ and $c_d(\pi)$ coincide, hence, by the method of moments,[6] the distributions are identical, proving the first assertion. Let ξ be a random variable with mean $1/d$ and Poisson distribution. Then $\mathbf{E}\xi^q$ is the expected number of q-multi-sets in $[\xi]$. A set S of ν elements gives rise to $S(q,\nu)$ different multi-sets M, such that $M = S$ as sets, and the computation of $\mathbf{E}\binom{\xi}{\nu}$ shows, that the expected number of ν-sets is $d^{-\nu}$, whence the second assertion.

(ii) For $i \leq t, i \neq d$, fix integers e_i. We compute the conditional expectation

$$\mathbf{E}\left(\binom{c_d(\pi)}{k} \,\Big|\, c_i(\pi) = e_i, i \leq t,\, i \neq d\right) = \frac{(n-\mathcal{E})!}{d^k k! (n - \mathcal{E} - kd)!} P(d,k),$$

where $\mathcal{E} = \sum\limits_{q \neq i \leq t} ie_i$. As n tends to infinity, the right hand side converges to $\frac{1}{d^k k!}$, proving our claim. □

Our next group of results describes the distribution of cycles in permutations of prescribed order. The proof makes use of the following purely analytic result.

Lemma 14. *Let $P(z) = \sum_{k=1}^q a_k z^k$ be a real polynomial, and let $Q(z) = \sum_{k=1}^q |a_k| z^k$. Assume that $P(z) \neq \pm Q(\pm z)$, and that $\{k : a_k \neq 0\}$ has greatest common divisor 1. Define the sequences $(b_n), (b_n^+)$ by means of the equations*

$$e^{P(z)} = \sum_{n=0}^{\infty} b_n\, z^n/(n!), \qquad e^{Q(z)} = \sum_{n=0}^{\infty} b_n^+\, z^n/(n!).$$

Then we have $|b_n| < b_n^+ e^{-cn^{1/q}}$ for some $c > 0$ and sufficiently large n.

Proof. We first claim that there is some constant c, such that for all real numbers r sufficiently large, and all complex numbers z with $|z| = r$, we have $\Re P(z) \leq Q(r) - cr$. For otherwise we would have $\Re a_k z^k \geq |a_k| r^k - cr$, that is, $\left|\frac{z}{|z|} - \zeta\right| < \varepsilon$ for some $(2k)$-th root of unity ζ, and ε arbitrarily small. Since by assumption the set $\{k : a_k \neq 0\}$ has greatest common divisor 1, we deduce that $|\arg z| < \varepsilon$ or $|\arg z - \pi| < \varepsilon$. However, the assumptions $P(z) \neq \pm Q(\pm z)$ and $a_k \neq 0$ for at least one odd k imply, that in these cases $\Re a_k z^k$ was negative for at least one value of k. From this we obtain that $|e^{P(z)}| \leq e^{Q(r) - cr}$ for some $c > 0$ and all z with $|z| = r$. Let r_n be the solution of the equation $rQ'(r) = n$. Then we deduce from Cauchy's bound that $\beta_n \leq \frac{e^{Q(r_n) - cr_n}}{r_n^n}$, while from [14, Corollary II] we obtain the lower bound $\beta_n^+ \geq \frac{e^{Q(r_n)}}{r_n^n n^c}$ with some absolute constant c. From these bounds and the asymptotics $r_n \sim \sqrt[q]{n/(qa_q)}$ the lemma follows. □

Lemma 15. *Let $q \geq 2$ and $e_t \geq 0\,(t|q,\, t < q)$ be integers.*

[6] Cf., for instance, [10].

(i) *There exist constants* $\alpha^{(d)}_{e_1,\dots,e_T}$, *such that, for all* $n \geq 1$,

$$\sum_{\pi^q=1} \prod_{\substack{t|q\\ t<q}} \big(c_t(\pi)\big)^{e_t} = \sum_{\nu=0}^{D} \alpha^{(\nu)}_{e_1,\dots,e_T} \frac{n!}{(n-\nu)!} |\operatorname{Hom}(C_q, S_{n-\nu})|, \tag{19}$$

where $D = \sum_t te_t$. *The coefficients* $\alpha^{(d)}_{e_1,\dots,e_T}$ *are recursively determined by means of the equations*

$$\alpha^{(d)}_{e_1,\dots,e_q} = \begin{cases} \dfrac{1}{d} \displaystyle\sum_{\substack{t|q\\ t<q}} \sum_{\nu=1}^{e_t} \binom{e_t}{\nu} \alpha^{(d-t)}_{e_1,\dots,e_t-\nu,\dots,e_T}, & d \geq 1\\ 1, & d = 0. \end{cases}$$

(ii) *We have*

$$\sum_{\pi^q=1} \prod_{\substack{t|q\\ t<q}} \big(c_t(\pi)\big)^{e_t} = \Big(1 + \mathcal{O}(n^{-1/q})\Big) \alpha^{D}_{e_1,\dots,e_T} n^{D/q}.$$

(iii) *If* q *is even, then there exists a constant* $c > 0$ *such that, for* n *sufficiently large,*

$$\sum_{\pi^q=1} \prod_{\substack{t|q\\ t<q}} (-1)^{(t-1)c_t(\pi)} \big(c_t(\pi)\big)^{e_t} < e^{-cn^{1/q}} |\operatorname{Hom}(C_q, S_{n-\nu})|. \tag{20}$$

Proof. (i) It will be convenient to allow t to run over all divisors of q, setting $e_q := 0$. Abbreviate the left-hand side of (19) as $\mathcal{S}_{e_1,\dots,e_q}(n)$, and let π be a permutation in S_n with $\pi^q = 1$. Then n occurs in some cycle of π of length t for some $t|q$. Let $\pi' \in S_{n-t}$ be the permutation resulting from π by deleting the cycle containing n. We have $c_d(\pi') = c_d(\pi)$ for $d \neq t$, and $c_t(\pi') = c_t(\pi) - 1$, that is,

$$\prod_{d|q} \big(c_d(\pi)\big)^{e_d} = \big(c_t(\pi') + 1\big)^{e_t} \prod_{d|q} \big(c_d(\pi')\big)^{e_d}.$$

The t-cycle containing n can be chosen in $\frac{(n-1)!}{(n-t)!}$ ways; hence, we obtain for $n \geq 1$ the recursion formula

$$\mathcal{S}_{e_1,\dots,e_q}(n) = \sum_{t|q} \frac{(n-1)!}{(n-t)!} \sum_{\nu=0}^{e_t} \binom{e_t}{\nu} \mathcal{S}_{e_1,\dots,e_t-\nu,\dots,e_q}(n-t), \tag{21}$$

where

$$S_{e_1,\dots,e_q}(0) = \begin{cases} 1, & (e_1,\dots,e_q) = (0,\dots,0)\\ 0, & \text{otherwise,} \end{cases}$$

and $S_{e_1,\dots,e_q}(n) = 0$ if one of the e_t or n is negative. Introducing the exponential generating functions

$$\mathfrak{S}_{e_1,\dots,e_q}(z) = \sum_{n=0}^{\infty} \mathcal{S}_{e_1,\dots,e_q}(n)\, z^n/(n!),$$

multiplying (21) by $\frac{z^{n-1}}{(n-1)!}$, and summing over $n \geq 1$, this recurrence relation translates into the differential equation

$$\mathfrak{S}'_{e_1,\dots,e_q}(z) - \Bigg(\sum_{t|q} z^{t-1}\Bigg)\mathfrak{S}_{e_1,\dots,e_q}(z) = \sum_{t|q} z^{t-1} \sum_{\nu=1}^{e_t} \binom{e_t}{\nu} \mathfrak{S}_{e_1,\dots,e_t-\nu,\dots,e_q}(z).$$

Integrating the latter equation, we find that

$$\mathfrak{S}_{e_1,\dots,e_q}(z) = \exp\Bigg(\sum_{t|q}\frac{z^t}{t}\Bigg) \sum_{t|q}\sum_{\nu=1}^{e_t}\binom{e_t}{\nu}\int_0^z \Bigg(\zeta^{t-1}\exp\Bigg(-\sum_{t|q}\frac{\zeta^t}{t}\Bigg)\mathfrak{S}_{e_1,\dots,e_t-\nu,\dots,e_q}(\zeta)\Bigg)\,d\zeta \\ + \exp\Bigg(\sum_{t|q}\frac{z^t}{t}\Bigg), \quad (22)$$

where the value of the integration constant has been determined by comparing the coefficients of z. We claim that there exist polynomials $P_{e_1,\dots,e_q}(z)$, such that

$$\mathfrak{S}_{e_1,\dots,e_q}(z) = P_{e_1,\dots,e_q}(z)\exp\Bigg(\sum_{t|q}\frac{z^t}{t}\Bigg). \quad (23)$$

The proof is by induction on $\mathbf{e} = \sum_{t|q} e_t$. If $e_t = 0$ for all t, then $\mathcal{S}_{0,\dots,0}(n) = |\operatorname{Hom}(C_q, S_n)|$, that is[7], $\mathfrak{S}_{0,\dots,0}(z) = \exp\big(\sum_{t|q}\frac{z^t}{t}\big)$, and (23) holds with $P_{0,\dots,0}(z) = 1$. Suppose now that our claim holds for all tuples $(e'_1,\dots,e'_q)$ with $\sum_{t|q} e'_t < \mathbf{e}$, and some $\mathbf{e} \geq 1$, and let $(e_1,\dots,e_q)$ be a tuple with $\sum_{t|q} e_t = \mathbf{e}$. Inserting (23) into the right-hand side of (22), we find that

$$\mathfrak{S}_{e_1,\dots,e_q}(z) = \exp\Bigg(\sum_{t|q}\frac{z^t}{t}\Bigg)\sum_{t|q}\sum_{\nu=1}^{e_t}\binom{e_t}{\nu}\int_0^z \zeta^{t-1}P_{e_1,\dots,e_t-\nu,\dots,e_q}(\zeta)\,d\zeta + \exp\Bigg(\sum_{t|q}\frac{z^t}{t}\Bigg),$$

that is, (23) holds for $(e_1,\dots,e_q)$ with

$$P_{e_1,\dots,e_q}(z) = 1 + \sum_{t|q}\sum_{\nu=1}^{e_t}\binom{e_t}{\nu}\int_0^z \zeta^{t-1}P_{e_1,\dots,e_t-\nu,\dots,e_q}(\zeta)\,d\zeta.$$

Comparing coefficients in (23) and in the recurrence relation determining the polynomials $P_{e_1,\dots,e_q}(z)$, the assertions of (i) follow.

(ii) By [25, Eq. (22)], we have

$$\frac{|\operatorname{Hom}(C_q, S_n)||}{|\operatorname{Hom}(C_q, S_{n-k})|} = \big(1 + \mathcal{O}(n^{-1/q})\big)n^{k(1-1/q)}.$$

Together with part (i), our claim follows.

(iii) Denote the left-hand side of (20) by $\mathcal{S}^*_{e_1,\dots,e_q}(n)$. In this case, we obtain the recurrence relation

$$\mathcal{S}^*_{e_1,\dots,e_q}(n) = \sum_{t|q}(-1)^{t-1}\frac{(n-1)!}{(n-t)!}\sum_{\nu=0}^{e_t}\binom{e_t}{\nu}\mathcal{S}^*_{e_1,\dots,e_t-\nu,\dots,e_q}(n-t).$$

[7] Cf., for instance, [9, Prop. 1].

Arguing as in part (i), the corresponding exponential generating function $\mathfrak{S}^*_{e_1,\ldots,e_q}(z)$ is found to satisfy

$$\mathfrak{S}^*_{e_1,\ldots,e_q}(z) = P^*_{e_1,\ldots,e_q}(z) \exp\left(\sum_{t|q}(-1)^{t-1}\frac{z^t}{t}\right)$$

with certain polynomials $P^*_{e_1,\ldots,e_q}$. Our claim follows from this and Lemma 14. □

Lemma 16. *Define the polynomials $P_{e_1,\ldots,e_q}$ as in the proof of Lemma* 15*. Then we have*

$$\begin{aligned} P_{\vec{e}_t}(z) &= 1+\frac{z^t}{t}, \\ P_{\vec{e}_{t_1}+\vec{e}_{t_2}}(z) &= 1+\frac{z^{t_1}}{t_1}+\frac{z^{t_2}}{t_2}+\frac{t_1+t_2}{(t_1t_2)^2}z^{t_1+t_2}, \\ P_{k\cdot\vec{e}_t}(z) &= \sum_{\nu=0}^{k} S(k+1,\nu+1)\frac{z^{\nu t}}{t^\nu}, \end{aligned}$$

where $\vec{e}_t$ denotes the tuple with $e_t = 1$ and $e_d = 0$ for $d \neq t$.

Proof. The first two equations follow directly from the definition. The third equation is established by induction on k. For $k = 1$ the claim is already proven. Assuming the result for $P_{\kappa\cdot\vec{e}_t}(z)$ with $\kappa < k$ and some $k \geq 2$, we find that

$$\begin{aligned} P_{k\cdot\vec{e}_t}(z) &= 1+\sum_{\nu=1}^{k}\binom{k}{\nu}\int_0^z \zeta^{t-1}P_{(k-\nu)\cdot\vec{e}_t}(\zeta)\,d\zeta \\ &= 1+\sum_{\nu=1}^{k}\binom{k}{\nu}\sum_{\mu=0}^{k-\nu}S(k-\nu+1,\mu+1)\frac{z^{(\mu+1)t}}{(\mu+1)t^{\mu+1}} \\ &= 1+\sum_{\mu=0}^{k-1}\frac{z^{(\mu+1)t}}{t^{\mu+1}}\cdot\frac{1}{\mu+1}\sum_{\nu=1}^{k-\mu}\binom{k}{\nu}S(k-\nu+1,\mu+1). \end{aligned}$$

Hence, our claim would follow from the identity

$$(\mu+1)S(k+1,\mu+2) = \sum_{\nu=1}^{k-\mu}\binom{k}{\nu}S(k-\nu+1,\mu+1),$$

which can be seen to hold as follows: the left-hand side counts the number of partitions of a set with $k+1$ points, with one special point distinguished, into $\mu+2$ non-empty parts with one part distinguished, which does not contain the special point. On the right-hand side, we first determine the size ν of the distinguished part, then select the points for this part avoiding the distinguished point, and finally partition the remaining $(k+1-\nu)$-set into $\mu+1$ non-empty parts. The number of possibilities in the latter case clearly matches the combinatorial description of the left-hand side, and the result follows. □

3.2. **Proof of Proposition 1.**

Lemma 17. *Let $\pi \in S_n$ be a permutation consisting only of cycles of length q. Then, for every irreducible character χ, we have $|\chi(\pi)| \leq \sqrt{n}\,\big(\chi(1)\big)^{1/q}$.*

This follows from [11, Theorem 1.1] together with the Murnaghan-Nakayama rule.

Lemma 18. *Let $q \geq 2$ be an integer, let $\pi \in S_n$ be a permutation with s cycles of lengths different from q, and let λ be a partition of n. Then*

$$|\chi_\lambda(\pi)| \leq \sqrt{n}\,\big(2\,\mathrm{sq}(\lambda)\big)^{s(q-1)/q}\big(\chi_\lambda(1)\big)^{1/q}. \tag{24}$$

Proof. For every partition μ denote by $N(\mu,\lambda)$ the number of ways to obtain μ from λ by stripping off s rim hooks of lengths according to the cycle structure of π, ending in an element π_0 containing only cycles of length q. By the Murnaghan-Nakayama rule, we have

$$\chi_\lambda(1) \geq \sum_\mu N(\mu,\lambda)\chi_\mu(1). \tag{25}$$

Neglecting the sign in the Murnaghan-Nakayama rule, and applying Lemma 17, Hölder's inequality, and the estimate (25), we get

$$\begin{aligned}
|\chi_\lambda(\pi)| &\leq \sum_\mu N(\mu,\lambda)\,|\chi_\mu(\pi_0)|\\
&\leq \sqrt{n}\sum_\mu N(\mu,\lambda)\big(\chi_\mu(1)\big)^{1/q}\\
&\leq \sqrt{n}\left(\sum_\mu N(\mu,\lambda)\right)^{(q-1)/q}\left(\sum_\mu \chi_\mu(1)\,N(\mu,\lambda)\right)^{1/q}\\
&\leq \sqrt{n}\left(\sum_\mu N(\mu,\lambda)\right)^{(q-1)/q}\big(\chi_\lambda(1)\big)^{1/q}.
\end{aligned}$$

Arguing as in the proof of Lemma 5, we see that the s cycles of length different from q can be chosen in at most $(2\,\mathrm{sq}(\lambda))^f$ ways, that is,

$$\sum_\mu N(\mu,\lambda) \leq \big(2\,\mathrm{sq}(\lambda)\big)^s,$$

and our claim follows. □

Lemma 19. *Let $q \geq 2$ be an integer, let $\pi \in S_n$ be a permutation with cycle lengths $\leq q$, and let $\lambda \vdash n$ be a partition of n satisfying $\lambda_1 \geq \|\lambda\|$. Set $\Delta = n - \lambda_1$, and let $\varepsilon > 0$ be given. Then there exists a constant $C = C(q,\varepsilon)$, such that, for $\Delta \in [C, n/C]$ and n sufficiently large,*

$$|\chi_\lambda(\pi)| \leq \chi_\lambda(1)^{\frac{1}{q}+\varepsilon}\prod_{t<q} E(n,\Delta,t,c_t(\pi)),$$

where

$$E(n,\Delta,t,s) = \begin{cases} \Big(\dfrac{\Delta^{(q+2t-1)/2q}}{n^{t/q}}\Big)^{s}, & \text{if } ts \leq \Delta \\ \Big(\dfrac{s}{\Delta^{\frac{2qt-2t-q+1}{2qt}} n^{t/q}}\Big)^{\Delta}, & \text{if } ts > \Delta. \end{cases}$$

Proof. The proof is by induction on the minimum $m(\pi)$ of the cycle lengths in π from q down to 1. For $m(\pi) = q$, our claim follows immediately from Lemma 17. Suppose that our assumption holds for all π with $m(\pi) \geq t+1$ and some $t \in [q-1]$. Write $\mu = \lambda \setminus \lambda_1$. For a partition $\nu \subseteq \lambda$ denote by $N(\nu,\lambda)$ the number of ways to obtain ν from λ by removing $c_t(\pi)$ rim hooks of length t, let $\pi \in S_n$ be a permutation with $m(\pi) = t$, and let $\pi_0 \in S_{n-tc_t(\pi)}$ be a permutation whose cycle structure is the same as that of π with all t-cycles removed. Then we have

$$|\chi_\lambda(\pi)| \leq \sum_\nu N(\nu,\lambda)\,|\chi_\nu(\pi_0)|.$$

We claim that for a partition ν such that $N(\nu,\lambda) \neq 0$,

$$|\chi_\nu(\pi_0)| \leq \big(\chi_\lambda(1)\big)^{\varepsilon}\big(\chi_\nu(1)\big)^{\frac{1}{q}+\varepsilon} \prod_{t<\tau<q} E(n,\Delta,\tau,c_\tau(\pi)).$$

Indeed, if $\Delta' = n - tc_t(\pi) - \nu_1 \geq \varepsilon\Delta$, then this assumption holds (even without the factor $(\chi_\lambda(1))^\varepsilon$) by the inductive hypothesis; otherwise, using Lemma 8 and the fact that $\Delta \leq n/C$, we get

$$|\chi_\nu(\pi_0)| \leq \chi_\nu(1) \leq n^{\Delta'} \leq n^{\varepsilon\Delta} \leq (\chi_\lambda(1))^{2\varepsilon}.$$

Setting

$$E := \prod_{t<\tau<q} E(n,\Delta,\tau,c_\tau(\pi)),$$

this gives

$$\begin{aligned} |\chi_\lambda(\pi)| &\leq E\big(\chi_\lambda(1)\big)^{\varepsilon} \sum_\nu N(\nu,\lambda)\big(\chi_\nu(1)\big)^{1/q} \\ &= E\big(\chi_\lambda(1)\big)^{\varepsilon} \sum_{a\leq c_t(\pi)} \sum_{\substack{\nu \\ \nu_1=\lambda_1-(c_t(\pi)-a)t}} N(\nu,\lambda)\big(\chi_\nu(1)\big)^{1/q}. \end{aligned} \tag{26}$$

Put $\kappa := \nu \setminus \nu_1$. Given a, we bound $\chi_\nu(1)$ as follows: we choose a set I of $|\kappa| = \Delta - at$ integers in $[n - tc_t(\pi)]$, and then count the number of ways of removing all boxes of ν in such a way that, in the i-th step, a box outside the first row is removed if and only if $i \in I$. We claim that the latter number is bounded by $\chi_\kappa(1) \leq \chi_\mu(1)N(\kappa,\mu)^{-1}$. Indeed, refining the removal of a rim hook into a sequence of removals of single boxes, we see that there are at least $N(\kappa,\mu)$ ways to obtain κ from μ by removing single boxes, while there are $\chi_\kappa(1)$ ways to remove κ completely by deleting boxes. Hence, we have $\chi_\mu(1) \geq N(\kappa,\mu)\chi_\kappa(1)$, from which the last claim follows. Since I can be chosen in $\binom{n-tc_t(\pi)}{\Delta-at}$ different ways, we obtain that

$$\chi_\nu(1) \leq \binom{n-tc_t(\pi)}{\Delta-at}\chi_\mu(1)N(\kappa,\mu)^{-1}. \tag{27}$$

Next, if $\nu_1 = \lambda_1 - (c_t(\pi) - a)t$, $N(\nu, \lambda)$ is the number of ways to remove $c_t(\pi) - a$ rim hooks from the first row of λ, and a rim hooks from μ. The position in the sequence of steps where a rim hook is removed from the first row can be chosen in $\binom{c_t(\pi)}{a}$ ways, thus

$$N(\nu, \lambda) = \binom{c_t(\pi)}{a} N(\kappa, \mu). \tag{28}$$

Inserting (27) and (28) into (26), we get

$$|\chi_\lambda(\pi)| \leq E\big(\chi_\lambda(1)\big)^\varepsilon \sum_{a \leq c_t(\pi)} \sum_{\substack{\kappa \subseteq \mu \\ \kappa \vdash \Delta - at}} \binom{c_t(\pi)}{a} \binom{n - tc_t(\pi)}{\Delta - at}^{1/q} N(\kappa, \mu)^{1-1/q} \big(\chi_\mu(1)\big)^{1/q}.$$

Finally,

$$\sum_{\substack{\kappa \subseteq \mu \\ \kappa \vdash \Delta - at}} N(\kappa, \mu)$$

is the number of ways to remove a rim hooks from μ, which can be done in at most $(2\mathrm{sq}(\mu))^a \leq (2\sqrt{\Delta})^a$ ways, as we saw in the proof of Lemma 2. Applying Hölder's inequality, and observing the fact that the number of partitions of Δ is $e^{c\sqrt{\Delta}} \leq (\chi_\lambda(1))^\varepsilon$, we obtain

$$|\chi_\lambda(\pi)| \leq E\big(\chi_\lambda(1)\big)^\varepsilon \sum_{a \leq c_t(\pi)} \binom{c_t(\pi)}{a} \binom{n - tc_t(\pi)}{\Delta - at}^{1/q} (2\sqrt{\Delta})^{(1-1/q)a} \big(\chi_\mu(1)\big)^{1/q}.$$

Since by Lemma 8 (ii) we have for $C > 3/\varepsilon$

$$\big(\chi_\lambda(1)\big)^{\frac{1}{q}+\varepsilon} \geq \left(\frac{n^\Delta}{\Delta!}\right)^{1/q} \big(\chi_\mu(1)\big)^{1/q},$$

we obtain

$$\frac{|\chi_\lambda(\pi)|}{\big(\chi_\lambda(1)\big)^{\frac{1}{q}+\varepsilon}} \leq E \left(\frac{\Delta!}{n^\Delta}\right)^{1/q} \sum_{a \leq c_t(\pi)} \binom{c_t(\pi)}{a} \binom{n - tc_t(\pi)}{\Delta - at}^{1/q} (2\sqrt{\Delta})^{(1-1/q)a}. \tag{29}$$

Since by assumption $\Delta \geq C$, the number $c_t(\pi) \leq n$ of summands is of order at most $(\chi_\lambda(1))^\varepsilon$; in particular, we can estimate the sum over a by its largest term. We now distinguish two cases, according to whether $\Delta \geq tc_t(\pi)$ or $\Delta < tc_t(\pi)$.

Case 1: $\Delta \geq tc_t(\pi)$. We first note that terms of the order of magnitude $e^{c\Delta}$ can be neglected on the right-hand side of (29), since they are bounded above by $(\chi_\lambda(1))^\varepsilon$; in particular, $\binom{c_t(\pi)}{a} \leq 2^{\Delta/t}$ and $2^a \leq 2^{\Delta/t}$ are absorbed into the term $(\chi_\lambda(1))^\varepsilon$. We now split the summation over a into the ranges $a \leq \varepsilon c_t(\pi)$, $\varepsilon c_t(\pi) < a < c_t(\pi) - \varepsilon\Delta$ and

$a \geq c_t(\pi) - \varepsilon\Delta$. In the last case, we have

$$\begin{aligned}\left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{n-tc_t(\pi)}{\Delta-at}^{1/q}\Delta^{\frac{q-1}{2q}a} &\leq \left(\frac{\Delta! n^{\Delta-tc_t(\pi)+\varepsilon\Delta t}}{n^\Delta(\Delta-tc_t(\pi)+\varepsilon\Delta t)!}\right)^{1/q}\Delta^{\frac{q-1}{2q}c_t(\pi)}\\ &\leq n^{\varepsilon\Delta t/q}\left(\frac{\Delta^{\frac{1}{2}+\frac{t}{q}-\frac{1}{2q}}}{n^{t/q}}\right)^{c_t(\pi)}\\ &\leq \big(\chi_\lambda(1)\big)^\varepsilon\left(\frac{\Delta^{\frac{1}{2}+\frac{t}{q}-\frac{1}{2q}}}{n^{t/q}}\right)^{c_t(\pi)}.\end{aligned}$$

Hence, every term in this range is of the desired magnitude, and therefore this part of the sum is sufficiently small.

Next, we turn our attention to terms with $a \leq \varepsilon c_t(\pi)$. In this case, we obtain

$$\begin{aligned}\left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{n-tc_t(\pi)}{\Delta-at}^{1/q}\Delta^{\frac{q-1}{2q}a} &\leq \left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{n}{\Delta}^{1/q}\Delta^{\varepsilon\frac{q-1}{2q}c_t(\pi)}\\ &\leq \big(\chi_\lambda(1)\big)^\varepsilon.\end{aligned}$$

Finally, consider the range $\varepsilon c_t(\pi) < a < c_t(\pi) - \varepsilon\Delta$. It suffices to consider the case where the terms in this range are not dominated by terms in the other ranges, that is, we may assume that the maximal term lies within this range. If we increase a by 1, a single summand in (29) is changed by a factor

$$F(a) := \frac{\big((n-tc_t(\pi)-\Delta+at)\cdots(n-tc_t(\pi)-\Delta+at-t+1)\big)^{1/q}}{\big((\Delta-at+1)\cdots(\Delta-at+t)\big)^{1/q}\Delta^{1/2-1/2q}}.$$

$F(a)$ is monotonically increasing, hence there is a unique positive solution x_0 of the equation $F(x) = 1$, and the value $a_{\max}$ for which the corresponding summand is maximal, differs from x_0 by at most 1. Using the bounds for a, we find that

$$F(a) \asymp \frac{n^{t/q}}{\Delta^{\frac{q+2t-1}{2q}}}, \quad a \in (\varepsilon c_t(\pi), c_t(\pi) - \varepsilon\Delta);$$

hence, we can neglect this range, unless the expression on the right-hand side, which does not depend on a, is $\asymp 1$; that is, $n \asymp \Delta^{(q+2t-1)/2t}$. In the latter case, we have

$$\begin{aligned}\left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{n-tc_t(\pi)}{\Delta-at}^{1/q}\Delta^{\frac{q-1}{2q}a} &\leq \frac{\Delta^{at/q+\frac{q-1}{2q}a}}{n^{at/q}}\\ &\leq \left(\frac{\Delta^{q+2t-1}}{n^{2t}}\right)^{\frac{a}{2q}}\\ &\leq e^{c\Delta}\\ &\leq \big(\chi_\lambda(1)\big)^\varepsilon.\end{aligned}$$

Case 2: $tc_t(\pi) > \Delta$. Note that we have $a \leq \Delta/t$. We begin with a in the range $a \geq (1-\varepsilon)\Delta/t$. Then we have

$$\begin{aligned}\left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{c_t(\pi)}{a}\binom{n-tc_t(\pi)}{\Delta-at}^{1/q}\Delta^{\frac{q-1}{2q}a} &\leq \left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{c_t(\pi)}{\Delta}\binom{n-tc_t(\pi)}{\varepsilon\Delta}^{1/q}\Delta^{\frac{q-1}{2qt}\Delta}\\ &\leq \big(\chi_\lambda(1)\big)^\varepsilon\left(\frac{c_t(\pi)}{\Delta^{\frac{2qt-2t-q+1}{2qt}}n^{1/q}}\right)^\Delta,\end{aligned}$$

which is the desired result.

If $a \leq \varepsilon\Delta/t$, then we have

$$\begin{aligned}\left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{c_t(\pi)}{a}\binom{n-tc_t(\pi)}{\Delta-at}^{1/q}\Delta^{\frac{q-1}{2q}a} &\leq \left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{c_t(\pi)}{\varepsilon\Delta/t}\binom{n}{\Delta}^{1/q}\Delta^{\varepsilon\frac{q-1}{2q}\Delta}\\ &\leq \big(\chi_\lambda(1)\big)^\varepsilon\left(\frac{c_t(\pi)}{\Delta}\right)^{\varepsilon\Delta},\end{aligned}$$

which is less than $(\chi_\lambda(1))^\varepsilon E(n, \Delta, t, c_t(\pi))$.

Finally, if $a \in (\varepsilon\Delta/t, (1-\varepsilon)\Delta/t)$, increasing a by 1 changes a single summand by a factor

$$\begin{aligned}F(a) := \frac{(c_t(\pi)-a)\big((n-\Delta-tc_t(\pi)+at)\cdots(n-\Delta-tc_t(\pi)+at-t+1)\big)^{1/q}}{(a+1)\Delta^{1/2-1/2q}\big((\Delta-at+1)\cdots(\Delta-at+t)\big)^{1/q}}&\\ \asymp \frac{n^{t/q}\Delta^{1/2-t/q+1/2q}}{c_t(\pi)};&\end{aligned}$$

and, as in the first case, the summands corresponding to these values of a can be neglected, unless the last expression is $\asymp 1$. If this is the case, we compute a single summand to be

$$\begin{aligned}\left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\binom{c_t(\pi)}{a}\binom{n-tc_t(\pi)}{\Delta-at}^{1/q}\Delta^{\frac{q-1}{2q}a} &\leq \big(\chi_\lambda(1)\big)^\varepsilon\left(\frac{\Delta!}{n^\Delta}\right)^{1/q}\left(\frac{c_t(\pi)}{\Delta^{1/2+1/2q}}\right)^a\left(\frac{n^{1/q}}{\Delta^{1/q}}\right)^{\Delta-at}\\ &\leq \big(\chi_\lambda(1)\big)^\varepsilon\left(\frac{c_t(\pi)}{\Delta^{1/2-t/q+1/2q}n^{t/q}}\right)^a\\ &\leq \big(\chi_\lambda(1)\big)^\varepsilon e^{c\Delta}.\end{aligned}$$

□

We are now in a position to prove Proposition 1. Let λ be a partition of n, $q \geq 2$ an integer, and $\pi \in S_n$ a permutation such that $\pi^q = 1$. Then $c_t(\pi) = 0$, unless $t|q$. We prove (17), using estimates in different ranges for cycle numbers of π and $\Delta = n - \lambda_1$.

If $\Delta = 0$, the assertion is trivial, and if $1 \leq \Delta \leq n^\varepsilon$, and $c_t(\pi) \geq 2en^{t/q}$ for some t, then we use the trivial estimate $\chi_\lambda(\pi) \leq \chi_\lambda(1) \leq n^\Delta$, together with Lemma 11 to see that the contribution of such terms to the sum in question is $< e^{-cn^{1/q}}$. If on the other hand

$c_t(\pi) < 2en^{t/q}$ for all t, we estimate $|\chi_\lambda(\pi)|$ as follows. As in the proof of Lemma 6, we choose a_t cycles of length t without boxes from the first row, and obtain

$$|\chi_\lambda(\pi)| \leq \Delta! \sum_{\sum_t ta_t \leq \Delta} \prod_t \binom{2en^{t/q}}{a_t} \leq \Delta!\, \Delta^{\tau(q)} (2en)^{\Delta/q} \leq (\Delta!)^2 \big(\chi_\lambda(1)\big)^{1/q},$$

and this is of the desired order of magnitude, since

$$\big(\chi_\lambda(1)\big)^{3\varepsilon} \geq \Big(\frac{n}{\Delta}\Big)^{3\varepsilon\Delta} \geq n^{2\varepsilon\Delta} \geq \Delta^{2\Delta}.$$

Next, we consider the case where Δ is in the range $[n^\varepsilon, n/C]$ for some sufficiently large constant C. Assume first, that there is some t such that $c_t(\pi) < 2en^{t/q}$. Then we have $E(n, \Delta, t, c_t(\pi)) \leq (\chi_\lambda(1))^\varepsilon$. For, either $\Delta < tc_t(\pi)$, which implies

$$c_t(\pi) < 2en^{t/q} \leq \Delta^{1/2q} n^{t/q} \leq \Delta^{\frac{q-2t+1}{2q}} n^{t/q};$$

or $tc_t(\pi) \leq \Delta \leq tc_t(\pi)^{1+1/2q}$, in which case

$$\Delta^{\frac{q-2t+1}{2q}} \leq \Delta^{1-1/(2q)} \leq t\big(c_t(\pi)\big)^{1-1/(4q^2)} \leq n^{t/q};$$

or, finally, $\Delta > tc_t(\pi)^{1+1/2q}$, which implies

$$E(n, \Delta, t, c_t(\pi)) \leq n^{c_t(\pi)} \leq 2^\Delta \leq \big(\chi_\lambda(1)\big)^\varepsilon.$$

Hence, disregarding the factor corresponding to such a value of t does not change the estimate in Lemma 19 significantly. From this observation and Lemmas 11 and 19 we obtain for π of order dividing q

$$\frac{N(q, n, c_1(\pi), \dots c_t(\pi))}{N(q, n)} |\chi(\pi)| \leq \big(\chi_\lambda(1)\big)^{\frac{1}{q}+\varepsilon} \prod_{\substack{t|q \\ t<q \\ c_t(\pi)\geq 2en^{t/q}}} \left(\frac{en^{t/q}}{tc_t(\pi)}\right)^{c_t(\pi)} E(n, \Delta, t, c_t(\pi)). \tag{30}$$

If t is such that $c_t(\pi) > \Delta$, then

$$\left(\frac{en^{t/q}}{c_t(\pi)}\right)^{c_t(\pi)} E(n, \Delta, t, c_t(\pi)) = \left(\frac{en^{t/q}}{c_t(\pi)}\right)^{c_t(\pi)-\Delta} \Delta^{-\frac{2qt-2t-q+1}{2qt}\Delta} < 1;$$

if $\Delta/t \leq c_t(\pi) \leq \Delta$, we find that

$$\begin{aligned}
\left(\frac{en^{t/q}}{c_t(\pi)}\right)^{c_t(\pi)} E(n, \Delta, t, c_t(\pi)) &= \left(\frac{en^{t/q}}{c_t(\pi)}\right)^{c_t(\pi)-\Delta} \Delta^{-\frac{2qt-2t-q+1}{2qt}\Delta} \\
&\leq e^{c\Delta} \left(\frac{\Delta}{n^{t/q}}\right)^{(1-\frac{1}{t})\Delta} \Delta^{-\frac{2qt-2t-q+1}{2qt}\Delta} \\
&\leq e^{c\Delta} \left(\frac{\Delta^{-\frac{1}{2t}+\frac{1}{q}-\frac{1}{2qt}}}{n^{(t-1)/q}}\right)^{\Delta} \\
&\leq \big(\chi_\lambda(1)\big)^\varepsilon,
\end{aligned}$$

since t is bounded by $q/2$. Finally, if $tc_t(\pi) \leq \Delta$, we have

$$\left(\frac{en^{t/q}}{c_t(\pi)}\right)^{c_t(\pi)} E(n,\Delta,t,c_t(\pi)) = \left(\frac{e\Delta^{\frac{q+2t-1}{2q}}}{c_t(\pi)}\right)^{c_t(\pi)} \leq \left(\frac{e\Delta^{1-1/2q}}{c_t(\pi)}\right)^{c_t(\pi)},$$

and either $c_t(\pi) < \Delta^{1-1/4q}$, in which case this factor is $\leq (\chi_\lambda(1))^\varepsilon$, or $c_t(\pi) \geq \Delta^{1-1/4q}$, in which case it is less than 1. Hence, in any case the right-hand side of (30) is bounded by $(\chi_\lambda(1))^\varepsilon$. Summing over all possible values for the $c_t(\pi)$ gives an additional factor $\leq n^{\tau(q)}$, which is absorbed into $(\chi_\lambda(1))^\varepsilon$ as well. Hence, for these characters (17) holds.

Finally, we have to consider partitions with $\Delta > n/C$. By Lemma 8, this implies $\chi_\lambda(1) \geq e^{cn}$. By Lemma 18, we have

$$|\chi_\lambda(\pi)| \leq (2\sqrt{n})^{\frac{q-1}{q}s}\big(\chi_\lambda(1)\big)^{\frac{1}{q}+\varepsilon},$$

where $s = \sum_{t<q} c_t(\pi)$. Together with Lemma 11, we deduce

$$\begin{aligned}\frac{|\chi_\lambda(\pi)|N(n,q,c_1(\pi),\dots,c_t(\pi))}{(\chi_\lambda(1))^{1/q+\varepsilon}N(n,q)} &\leq (4n)^{\frac{q-1}{2q}s}\prod_{\substack{t|q\\ t<q}}\left(\frac{en^{t/q}}{c_t(\pi)}\right)^{c_t(\pi)}\\ &= \prod_{\substack{t|q\\ t<q}}\left(\frac{4en^{\frac{q+2t-1}{2q}}}{c_t(\pi)}\right)^{c_t(\pi)}.\end{aligned}$$

In the last product, all factors with $c_t(\pi) > 4en^{\frac{q+2t-1}{2q}}$ are bounded by 1, while for t such that $c_t(\pi) \leq 4en^{\frac{q+2t-1}{2q}}$ the corresponding factor is at most $n^{n^{1-\frac{1}{2q}}} < (\chi_\lambda(1))^\varepsilon$. Hence, also in this case, the left-hand side of (17) has the desired order of magnitude, and the proof of Proposition 1 is complete.

4. The multiplicities of root number functions

In order to be able to estimate the subgroup growth of Fuchsian groups, we also need to establish certain properties of the multiplicities of root number functions for symmetric groups. These are summarised in our next two results. For a positive integer q, define the q-th root number function $r_q : S_n \to \mathbb{N}_0$ via

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

and, for each irreducible character χ of S_n, let

$$m_\chi^{(q)} := \langle r_q, \chi\rangle$$

be the multiplicity of χ in r_q. It is known that the functions r_q are proper characters, that is, the $m_\chi^{(q)}$ are non-negative integers; cf. [30].

Proposition 2. *Let $q \geq 2$ be an integer, $\varepsilon > 0$, $n \geq n_0(\varepsilon)$, and let $\lambda \vdash n$ be a partition with corresponding character χ_λ.*

(i) *We have $m_{\chi_\lambda}^{(q)} \leq (\chi_\lambda(1))^{1-2/q+\varepsilon}$.*

(ii) *Given a partition $\mu \vdash \Delta$, there exists some constant C^q_μ, depending only on μ and q, such that, for $\lambda \setminus \lambda_1 = \mu$ and n sufficiently large, we have $m^{(q)}_{\chi_\lambda} = C^q_\mu$. In particular, we have*

$$\begin{aligned} C^q_{(1)} &= \tau(q) - 1, \\ C^q_{(2)} &= \frac{1}{2}\big(\sigma(q) + \tau(q)^2 - 3\tau(q) + \tau_{\text{odd}}(q)\big), \\ C^q_{(1,1)} &= \frac{1}{2}\big(\sigma(q) + \tau(q)^2 - 3\tau(q) - \tau_{\text{odd}}(q)\big) + 1, \end{aligned}$$

where $\sigma(q$ is the sum of divisors of q, $\tau(q)$ is the number of divisors of q, and $\tau_{\text{odd}}(q)$ is the number of odd divisors of q.

(iii) *For a partition $\mu \vdash \Delta$, q odd, and sufficiently large n, we have $m^{(q)}_{\chi_{\lambda'}} = 0$. If q is even, then $m^{(q)}_{\chi_{\lambda'}} = m^{(q)}_{\chi_\lambda}$.*

Proposition 3. *Let $\varepsilon > 0$ be given, let $q \geq 2$ be an integer, $\Delta \geq \Delta_0(q, \varepsilon)$ and $n \geq n_0(q, \Delta, \varepsilon)$. Then, for partitions $\mu \vdash \Delta$ and $\lambda \vdash n$ with $\lambda \setminus \lambda_1 = \mu$, we have that*

$$\left| \frac{m^q_{\chi_\lambda} \Delta!}{\chi_\mu(1) Q_\Delta(q)} - 1 \right| < \varepsilon,$$

where $Q_\Delta(q) = \sum_{i=1}^{\Delta} S(\Delta, \Delta - i)\, q^i$.

This section is devoted to the proofs of these results.

4.1. **Proof of Proposition 2.** We begin by translating the problem of bounding $m^{(q)}_\chi$ from an algebraic into a combinatorial question.

Lemma 20. *For $q \geq 2$ and $\chi \in \operatorname{Irr}(S_n)$, we have*

$$m^{(q)}_\chi \leq \sum_{\mathbf{c}^q = 1} \big\langle \mathbf{1}, \big|\chi{\downarrow}_{C_{S_n}(\mathbf{c})}\big| \big\rangle_{C_{S_n}(\mathbf{c})},$$

where the summation extends over all conjugacy classes $\mathbf{c}$ in S_n, whose orders divide q, and $C_{S_n}(\mathbf{c})$ denotes the centraliser of some element $\pi \in \mathbf{c}$.

Proof. It is shown in [30] that, for every class $\mathbf{c}$, there exists a linear character $\phi_{\mathbf{c}}$ of $C_{S_n}(\mathbf{c})$ such that $r_q = \sum\limits_{\mathbf{c}^q=1} \phi_{\mathbf{c}}{\uparrow}^{S_n}$. By Frobenius reciprocity this implies

$$\begin{aligned} m^{(q)}_\chi &= \sum_{\mathbf{c}^q=1} \big\langle \phi_{\mathbf{c}}{\uparrow}^{S_n}, \chi \big\rangle_{S_n} \\ &= \sum_{\mathbf{c}^q=1} \big\langle \phi_{\mathbf{c}}, \chi{\downarrow}_{C_{S_n}(\mathbf{c})} \big\rangle_{C_{S_n}(\mathbf{c})} \\ &\leq \sum_{\mathbf{c}^q=1} \big\langle \mathbf{1}, \big|\chi{\downarrow}_{C_{S_n}(\mathbf{c})}\big| \big\rangle_{C_{S_n}(\mathbf{c})}. \end{aligned}$$

□

Proof of Proposition 2. (i) Let $\varepsilon > 0$ be given. We first consider characters χ_λ with $\chi_\lambda(1) > n^{n^{1-\varepsilon/4}}$, starting from the formula

$$m_{\chi_\lambda}^{(q)} \leq \sum_{\mathbf{c}^q=1} \frac{1}{|C_{S_n}(\mathbf{c})|} \sum_{\pi\in C_{S_n}(\mathbf{c})} |\chi_\lambda(\pi)|.$$

The number of summands of the outer sum is $\leq n^{\tau(q)}$ and therefore negligible. In the inner sum, we bound $\chi_\lambda(\pi)$ by either using Lemma 5 or via the trivial bound $\chi_\lambda(1)$, depending on the number of cycles of π. Estimating the number of elements $\pi \in C_{S_n}(\mathbf{c})$ with k cycles using Lemma 12 (ii) for $k \geq (\log n)^3$, and trivially otherwise, we obtain

$$m_{\chi_\lambda}^{(q)} \leq \big(\chi_\lambda(1)\big)^{\varepsilon}(2\sqrt{n})^{(\log n)^3} + \big(\chi_\lambda(1)\big)^{\varepsilon} \sum_{k\geq(\log n)^3} \min\big((2\sqrt{n})^k, \chi_\lambda(1)\big)\frac{(3q\log n)^{k/q}}{\lfloor k/q\rfloor!}.$$

The first summand is negligible. The greatest term of the sum is coming from one of $k = \lfloor\frac{2\log\chi_\lambda(1)}{\log n}\rfloor$ and $k = \lceil\frac{2\log\chi_\lambda(1)}{\log n}\rceil$, and these terms differ by a factor n at most; hence, using Stirling's formula, we obtain

$$m_{\chi_\lambda}^{(q)} \leq \big(\chi_\lambda(1)\big)^{1+\varepsilon} e^{-\frac{2}{q}\log\chi_\lambda(1)\frac{\log\log\chi_\lambda(1)}{\log n}} \leq \big(\chi_\lambda(1)\big)^{1-\frac{2}{q}+2\varepsilon},$$

and our claim is proven in this case. In particular, setting $\Delta = n - \lambda_1$, our first claim holds true for all characters χ_λ belonging to a partition λ with $\Delta > n^{1-\varepsilon/2}$.

Next, we consider the range $(\log n)^4 \leq \Delta \leq n^{1-\varepsilon/2}$. In this range we estimate $\chi_\lambda(\pi)$ by means of Lemma 6 and Equation (15), and we bound the number of centraliser elements with k cycles again via Lemma 12 (ii), or trivially. In this way, we obtain

$$\begin{aligned} m_{\chi_\lambda}^{(q)} &\leq \big(\chi_\lambda(1)\big)^{\varepsilon} + \big(\chi_\lambda(1)\big)^{\varepsilon} \sum_{k\geq(\log n)^3} \min\left(\max_{\nu\leq\Delta}(2\sqrt{\Delta})^{\nu}\binom{k}{\nu}, \chi_\lambda(1)\right)\frac{(3q\log n)^{k/q}}{\lfloor k/q\rfloor!} \\ &\leq \big(\chi_\lambda(1)\big)^{2\varepsilon} \sum_{k\geq(\log n)^3} \min\Big((4\sqrt{\Delta})^k, \chi_\lambda(1)\Big)\frac{(3q\log n)^{k/q}}{\lfloor k/q\rfloor!} \\ &\leq \big(\chi_\lambda(1)\big)^{1+3\varepsilon} e^{-\frac{2}{q}\log\chi_\lambda(1)\frac{\log\log\chi_\lambda(1)}{\log\Delta}}. \end{aligned}$$

On the other hand, from Lemma 8 (ii) we see that $\frac{\log\log\chi_\lambda(1)}{\log\Delta} \geq 1$ for all $\Delta < n/5$, hence, our claim holds in this case as well.

Finally, for $\Delta < (\log n)^4$, we see from Lemma 12 (ii) that we may neglect the contribution of permutations with at least $(\log n)^3$ cycles. For the remaining ones we have $\chi_\lambda(\pi) \leq (\log n)^{3\Delta}$ by Lemma 6, Equation (14), which is less then $(\chi_\lambda(1))^{\varepsilon}$. This completes the proof of Proposition 2 (i).

(ii) We describe the computation of $m_{\chi_\lambda}^{(q)}$ for bounded Δ. We have

$$m_{\chi_\lambda}^{(q)} = \langle\chi_\lambda, r_q\rangle = \frac{1}{n!}\sum_{\pi\in S_n}\chi_\lambda(\pi^q).$$

Let $\mu \vdash \Delta$ be a partition. By Lemma 7, there exists a polynomial $P_\mu(x_1, \dots, x_\Delta)$, such that, for every n and $\lambda \vdash n$ with $\lambda \setminus \lambda_1 = \mu$, we have $\chi_\lambda = P_\mu(c_1, \dots, c_\Delta)$. Moreover, if

x_d has weight d, then P_μ has weight at most $|\mu|$. We have

$$c_d(\pi^q) = \sum_{\substack{\kappa \\ \kappa/(\kappa,q)=d}} (\kappa, q) c_\kappa(\pi), \tag{31}$$

since the q-th power of a cycle of length κ consists of (κ, q) cycles, each of length $\frac{\kappa}{(\kappa,q)}$. Thus, we have to compute

$$\frac{1}{n!} \sum_{\pi \in S_n} Q_{\mu,q}\big(c_1(\pi), c_2(\pi), \dots, c_{\Delta q}(\pi)\big)$$

for a certain polynomial $Q_{\mu,q}$ of weight at most Δq.

By Lemma 13, the last expression converges to some constant. Hence, $m_{\chi_\lambda}^{(q)}$ converges to some real number, but as $m_{\chi_\lambda}^{(q)}$ is integral, it has to become constant for n sufficiently large.

We now consider the cases $\mu = (1), (2)$ and $(1,1)$. If $\lambda = (n-1,1)$, we have

$$m_{\chi_\lambda}^{(q)} = \frac{1}{n!} \sum_{\pi \in S_n} \chi_\lambda(\pi^q) = \frac{1}{n!} \sum_{\pi \in S_n} c_1(\pi^q) - 1 = \frac{1}{n!} \sum_{\pi \in S_n} \sum_{d|q} d c_d(\pi) - 1.$$

By Lemma 13, the expected number of d-cycles is $\frac{1}{d}$; hence, $m_{\chi_\lambda}^{(q)} = \tau(q) - 1$. Next, for $\lambda = (n-2,2)$, Lemma 7 yields

$$\chi_\lambda = \frac{c_1^2}{2} - \frac{3c_1}{2} + c_2.$$

Inserting (31), we deduce

$$\begin{aligned} m_{\chi_\lambda}^{(q)} &= \frac{1}{n!} \sum_{\pi \in S_n} \left(\frac{1}{2} \Big(\sum_{d|q} d c_d(\pi) \Big)^2 - \frac{3}{2} \sum_{d|q} d c_d(\pi) + \sum_{\substack{d|q \\ (2d,q)=d}} d c_d(\pi) \right) \\ &= \frac{1}{2} \sum_{d_1, d_2 | q} \frac{1}{n!} \sum_{\pi \in S_n} \big(d_1 d_2 c_{d_1}(\pi) c_{d_2}(\pi) \big) - \frac{3}{2} \sum_{d|q} \frac{1}{n!} \sum_{\pi \in S_n} d c_s(\pi) \\ &\qquad + \sum_{\substack{d|q \\ (2d,q)=d}} \frac{1}{n!} \sum_{\pi \in S_n} d c_d(\pi). \end{aligned}$$

If $d_1 \neq d_2$ then, by Lemma 13, $s_{d_1}(\pi)$ and $s_{d_2}(\pi)$ are asymptotically independent for $\pi \in S_n$ chosen at random, and have mean values $\frac{1}{d_1}$ and $\frac{1}{d_2}$, respectively, while $(c_d(\pi))^2$ has mean value $\frac{1}{d} + \frac{1}{d^2}$. Hence, the first sum is asymptotically equal to $\sigma(q) + \tau(q)^2$. The second sum equals $\tau(q)$, whereas the last sum yields $|\{d|q : (2d, q) = d\}|$, which equals $\tau_{\text{odd}}(q)$. We deduce that, as $n \to \infty$,

$$m_{\chi_\lambda}^{(q)} \to \frac{1}{2} \big(\sigma(q) + \tau(q)^2 - 3\tau(q) + \tau_{\text{odd}}(q) \big),$$

which implies our claim, since $m_{\chi_\lambda}^{(q)}$ is always integral. A similar computation leads to the value of $m_{\chi_\lambda}^{(q)}$ for $\lambda = (n-2,1,1)$.

(iii) For q odd, we have

$$m^{(q)}_{\chi_{\lambda'}} = \sum_{\pi\in S_n} \chi_{\lambda'}(\pi^q) = \sum_{\pi\in S_n} \chi_\lambda(\pi^q)\epsilon(\pi^q) = \sum_{\pi\in S_n} \chi_\lambda(\pi^q)\epsilon(\pi),$$

where ϵ is the sign character. As in the proof of part (ii), we can write $m^q_{\chi_{\lambda'}}$ as a linear combination of sums of the form

$$\frac{1}{n!}\sum_{\pi\in S_n} \epsilon(\pi)\prod_{j=1}^{lq}\big(c_j(\pi)\big)^{e_j}.$$

Observe first that the contribution coming from permutations π with $\sum_{j=1}^{ql} jc_j(\pi) > n/2$ is $o(1)$ by Lemma 13. The sum over permutations π with $\sum_{j=1}^{ql} jc_j(\pi) \leq n/2$ vanishes, since it can be expressed as a linear combination of sums of the form

$$\sum_{\substack{\pi\in S_n\\ c_i(\pi)\geq c_i\,(i\leq lq)}} \epsilon(\pi) = \pm \sum_{\pi\in S_{n-\mathcal{C}}} \epsilon(\pi) = 0,$$

where $\mathcal{C} = \sum_{j=1}^{lq} c_j$. Hence, for q odd and n large, $m^{(q)}_{\chi_{\lambda'}} < 1$ and, being an integer, vanishes. The argument for q even is trivial. □

4.2. **Proof of Proposition 3.** We compute the scalar product $\langle r_q, \chi_\lambda\rangle$, and evaluate χ_λ using Lemma 7, to obtain

$$m^{(q)}_{\chi_\lambda} = \frac{\chi_\mu(1)}{n!}\sum_{\pi\in S_n}\binom{c_1(\pi^q)}{\Delta} + \mathcal{O}\left(\frac{\Delta\chi_\mu(1)}{n!}\sum_{i\leq\Delta-1}\sum_{\pi\in S_n}\binom{c_1(\pi^q)+\ldots+c_\Delta(\pi^q)}{i}\right). \quad (32)$$

By Lemma 13, we have as $n\to\infty$

$$\frac{1}{n!}\big|\{\pi\in S_n : c_l(\pi) = a\}\big| \sim \frac{e^{-1/l}}{l^a a!},$$

and the events "$c_l(\pi) = a$" and "$c_{l'}(\pi) = b$" are asymptotically independent. From this together with Equation (31) we deduce

$$\begin{aligned}
\frac{1}{n!}\sum_{\pi\in S_n}\big(c_1(\pi^q)\big)^\Delta &= \frac{1}{n!}\sum_{\pi\in S_n}\left(\sum_{t|q} tc_t(\pi)\right)^\Delta\\
&\sim \sum_{\substack{d_t, t|q\\ \sum_t d_t=\Delta}}\prod_{t|q}\left(\frac{1}{n!}\sum_{\pi\in S_n} tc_t(\pi)\right)^{d_t}\\
&\sim \sum_{\substack{d_t, t|q\\ \sum_t d_t=\Delta}}\prod_{t|q}\sum_{a=1}^{\infty}\frac{e^{-1/t}(ta)^{d_t}}{t^a a!}\\
&= \sum_{\substack{d_t, t|q\\ \sum_t d_t=\Delta}}\prod_{t|q} t^{d_t}\sum_{\nu=1}^{d_t} S(d_t,\nu)t^{-\nu}.
\end{aligned}$$

The last quantity can be written as

$$\sum_{\substack{d_t, t|q \\ \sum_t d_t = \Delta}} \prod_{t|q} Q_{d_t}(t), \tag{33}$$

where

$$Q_n(t) = \sum_{\nu=0}^{n-1} S(n, n-\nu) t^\nu.$$

For fixed n, the sequence $S(n,m)$ is unimodal in m; define m_0 to be the least m with $S(n, m_0) = \max_m S(n,m)$. Kanold [16] has shown that

$$m_0 \sim \frac{n}{\log n};$$

moreover, it can be deduced from his proof that

$$\sum_{m=(1-\varepsilon)m_0}^{(1+\varepsilon)m_0} S(n,m) \sim \sum_{m=1}^{n} S(n,m), \quad n \to \infty. \tag{34}$$

This estimate implies $Q_{d_t}(t) \leq (t/q)^{d_t(1-\varepsilon)} Q_{d_t}(q)$ for all $t|q$ and $d_t \geq d_0(\varepsilon)$.

Next, we establish the inequality $Q_n(x)Q_{n'}(x) \leq Q_{n+n'}(x)$ for all real positive x and $n, m \geq 1$. More precisely, we show that each single coefficient of $Q_n(x)Q_{n'}(x)$ is less than or equal to the corresponding coefficient of $Q_{n+n'}(x)$, which implies our claim. Computing the m-th coefficient explicitly, we have to show that

$$\sum_{i+j=m} S(n, n'-i) S(n', n'-j) \leq S(n+n', n+n'-m),$$

which is true since the right-hand side is the number of partitions of a set with $n+n'$ elements into $n+n'-m$ parts, while the left-hand side is the number of these partitions that respect some fixed partition of the large set into two sets with n and n' elements. Together with (34), we deduce that, for d sufficiently large, and a fixed tuple $d_1, \dots, d_q$ with $d_1 + \cdots + d_q = \Delta$,

$$\prod_{t|q} Q_{d_t}(t) \leq \prod_{t|q} (t/q)^{2d_t/3} Q_{d_t}(q) \leq (2/3)^{\Delta - d_q} \prod_{t|q} Q_{d_t}(q) \leq (2/3)^{\Delta - d_q} Q_\Delta(q).$$

We now split the sum (33) into three ranges, according to whether $d_q = \Delta$, $\Delta - C\tau(q) \leq d_q \leq \Delta - 1$, or $d_q < \Delta - C\tau(q)$, and we want to show that the sum over the latter two ranges is negligible compared to the first term. From the last estimate we find that, for $\varepsilon > 0$ and $\Delta > \Delta_0(q, \varepsilon)$, there is some $C = C(\varepsilon)$, such that[8]

$$\sum_{\substack{d_t, t|q \\ \sum_t d_t = \Delta \\ d_q \leq \Delta - C\tau(q)}} \prod_{t|q} Q_{d_t}(t) \leq Q_\Delta(q) \sum_{\nu \geq C\tau(q)} (2/3)^\nu \binom{\nu + \tau(q) - 1}{\tau(q) - 1} \leq \varepsilon Q_\Delta(q).$$

[8] Complex integration shows that we may take $C(\varepsilon) = 10 + 7\log \varepsilon^{-1}$.

In the range $\Delta - C\tau(q) \leq d_q \leq \Delta - 1$, the number of summands is bounded, and their sum can be estimated by $CQ_{\Delta-1}(q)$, and we obtain

$$\sum_{\substack{d_t, t|q\\ \sum_t d_t = \Delta\\ d_q \neq \Delta}} \prod_{t|q} Q_{d_t}(t) \leq \varepsilon Q_\Delta(q) + CQ_{\Delta-1}(q).$$

Now we use the inequalities (cf. [16, Satz 1])

$$\frac{(m+1)^n}{m!}\left(1 - \frac{m}{(1-1/m)^n}\right) \leq S(n,m) \leq \frac{(m+1)^n}{m!},$$

to see that $S(n, n-\mu)\,q^\mu$ in monotonically decreasing with μ for n sufficiently large and $\mu > n - \frac{n}{2\log n}$; in particular, we have

$$\sum_{\mu > n - n/(2\log n)} S(n, n-\mu)\,q^\mu < \frac{1}{n} Q_n(q).$$

Since $S(\Delta+1, \Delta-\mu) \geq (\Delta-\mu)S(\Delta, \Delta-\mu)$, the latter inequality implies

$$\begin{aligned} Q_\Delta(q) &\geq \sum_{\mu \leq \Delta - \Delta/(2\log\Delta)} S(\Delta, \Delta-\mu)\,q^\mu \\ &\geq \frac{\Delta}{2\log\Delta} \sum_{\mu \leq \Delta - \Delta/(2\log\Delta)} S(\Delta-1, \Delta-\mu)\,q^\mu \\ &\geq \frac{\Delta}{2\log\Delta}\left(1 - \frac{1}{\Delta-1}\right) Q_{\Delta-1}(q), \end{aligned}$$

and we deduce that

$$Q_\Delta(q) \leq \frac{1}{n!} \sum_{\pi \in S_n} \big(c_1(\pi^q)\big)^\Delta \leq (1+\varepsilon) Q_\Delta(q),$$

provided that $\Delta \geq \Delta_0(q,\varepsilon)$ and $n \geq n_0(\Delta, q, \varepsilon)$. Estimating the error term in (32) in a way similar to our treatment of the main term, and using the fact that

$$\binom{c_1(\pi^q)}{\Delta} = \frac{1}{\Delta!}\big(c_1(\pi^q)\big)^\Delta + \mathcal{O}\big(c_1(\pi^q)^{\Delta-1}\big),$$

Proposition 3 follows.

5. Subgroup growth of Fuchsian groups

5.1. **The generic case.** Let $r, s, t \geq 0$ be integers, $a_1, \dots, a_r \geq 2$ in $\mathbb{N} \cup \{\infty\}$, and let $e_1, \dots, e_s \geq 2$ be integral. Define the group $\Gamma = \Gamma(t; a_1, \dots, a_r; e_1, \dots, e_s)$ associated with these data by

$$\begin{aligned} \Gamma = \Big\langle & x_1, \dots, x_r, y_1, \dots, y_s, u_1, v_1, \dots, u_t, v_t \;\Big| \\ & x_1^{a_1} = x_2^{a_2} = \cdots = x_r^{a_r} = x_1 x_2 \cdots x_r y_1^{e_1} y_2^{e_2} \cdots y_s^{e_s} [u_1, v_1][u_2, v_2] \cdots [u_t, v_t] = 1 \Big\rangle. \end{aligned} \quad (35)$$

Define

$$\begin{aligned}
\mu(\Gamma) &= \sum_{i=1}^{r}\left(1-\frac{1}{a_i}\right)+s+2(t-1),\\
\alpha(\Gamma) &= \mu(\Gamma)-\sum_{j=1}^{s}\left(1-\frac{2}{e_j}\right),\\
m_\Gamma &= [a_1,\dots,a_r].
\end{aligned}$$

The main result of this section provides an asymptotic expansion for the number of index n subgroups of these groups.

Theorem 3. *Let Γ be given as in* (35), *and suppose that $\alpha(\Gamma)>0$. Then the number $s_n(\Gamma)$ of index n subgroups in Γ satisfies an asymptotic expansion*

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

Here,

$$\begin{aligned}
\delta &= \begin{cases}2, & \forall i: a_i \text{ finite and odd}, \forall j: e_j \text{ even}\\ 1, & \text{otherwise},\end{cases}\\
L_\Gamma &= (2\pi)^{-1/2-\sum_i(1-1/a_i)}\Big(\prod_{i:a_i\neq\infty}a_i^{-1/2}\Big)\exp\left(-\sum_{\substack{i\\ 2|a_i}}\frac{1}{2a_i}\right),\\
\Phi_\Gamma(n) &= n^{3/2-\sum_i(1-1/a_i)}\exp\left(\sum_{i=1}^{r}\sum_{\substack{t|a_i\\ t<a_i}}\frac{n^{t/a_i}}{t}\right),
\end{aligned}$$

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

Corollary 1. *Let Γ be as in* (35), *and suppose that $\alpha(\Gamma)>0$. Then we have*

$$\frac{s_{n+1}(\Gamma)}{s_n(\Gamma)}\sim (n+1)^{\mu(\Gamma)},\quad (n\to\infty);$$

in particular, $s_n(\Gamma)$ is strictly increasing for sufficiently large n.

Proof of Theorem 3. The proof proceeds in three steps: first we express $h_n(\Gamma):=|\operatorname{Hom}(\Gamma,S_n)|/n!$ in character theoretic terms; next, we use results from Sections 3 and 4 to obtain an asymptotic estimate for $h_n(\Gamma)$. The assertions of the theorem are then deduced by means of an asymptotic method for divergent power series due to Bender [2].

Set

$$R=x_1x_2\cdots x_r y_1^{e_1}y_2^{e_2}\cdots y_s^{e_s}[u_1,v_1][u_2,v_2]\cdots[u_t,v_t],$$

and define $N_R(\pi)$ to be the number of solutions of the equation $R=\pi$, subject to the conditions $x_i^{a_i}=1$ for those i for which x_i occurs in w. We now represent N_w as a convolution product. Define functions

$$\begin{aligned}
\alpha_i(\pi) &= \begin{cases} 1, & \pi^{a_i} = \mathrm{id} \\ 0 & \text{otherwise} \end{cases}, \qquad 1 \leq i \leq r; \\
\beta_i(\pi) &= \#\{\sigma \in S_n : \sigma^{e_i} = \pi\}, \qquad 1 \leq i \leq s \\
\gamma(\pi) &= \#\{\sigma, \tau \in S_n : [\sigma, \tau] = \pi\}.
\end{aligned}$$

Then we have $N_R = \alpha_1 * \cdots * \alpha_r * \beta_1 * \ldots \beta_s * \gamma^{*t}$, and Lemma 1 yields the Fourier coefficients of N_R. In fact, we have

$$\begin{aligned}
\langle \alpha_i, \chi \rangle &= \frac{1}{n!} \sum_{\pi : \pi^{a_i} = 1} \chi(\pi), \\
\langle \beta_i, \chi \rangle &= \frac{1}{n!} \sum_{\pi \in S_n} \chi(\pi^{a_i}) = m_\chi^{(e_i)}, \\
\langle \gamma, \chi \rangle &= \frac{n!}{\chi(1)};
\end{aligned}$$

thus,

$$N_R(\pi) = \sum_\chi \frac{n!^{s+2t-1}}{\chi(1)^{r+s+2t-1}} \prod_{i=1}^r \left(\sum_{\pi : \pi^{a_i} = 1} \chi(\pi) \right) \prod_{j=1}^s m_\chi^{(e_j)} \chi(\pi).$$

In view of (17) it is convenient to rewrite this formula as

$$N_R(\pi) = \sum_\chi \frac{n!^{s+2t-1}}{\chi(1)^{r+s+2t-1}} \prod_{i=1}^r |\operatorname{Hom}(C_{a_i}, S_n)| \prod_{i=1}^r \alpha_\chi^{a_i} \prod_{j=1}^s m_\chi^{(e_j)} \chi(\pi),$$

where

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

satisfies $|\alpha_\chi^{a_i}| \leq \chi(1)^{\frac{1}{a_i} + \epsilon}$. Noting that $h_n(\Gamma) = \frac{1}{n!} N_R(1)$, we finally obtain

$$h_n(\Gamma) = (n!)^{s+2t-2} \prod_{i=1}^r |\operatorname{Hom}(C_{a_i}, S_n)| \sum_{\lambda \vdash n} \frac{\prod_{i=1}^r \alpha_{\chi_\lambda}^{(a_i)} \prod_{j=1}^s m_{\chi_\lambda}^{(e_j)}}{(\chi_\lambda(1))^{r+s+2t-2}}. \tag{36}$$

We now concentrate on the sum over characters. Let $A > 0$ be given, and split the sum into three parts $\sum_1, \sum_2, \sum_3$, according to whether $\lambda_1 \geq n - A$, $\|\lambda\| \geq n - A$, or $\lambda_1, \|\lambda\| < n - A$. Note that the first two cases are mutually exclusive for $n > 2A + 1$. For $\varepsilon > 0$ and n sufficiently large, we have by Propositions 1 and 2 (i)

$$\begin{aligned}
\sum\nolimits_3 &< \sum_{\substack{\lambda \vdash n \\ \|\lambda\|, \lambda_1 < n - A}} \big(\chi_\lambda(1)\big)^{\sum_i 1/a_i + \sum_j (1 - 2/e_j) - r - s - 2t + 2 + \varepsilon} \\
&\leq 2 \sum_{\substack{\lambda \vdash n \\ \|\lambda\| \leq \lambda_1 < n - A}} \big(\chi_\lambda(1)\big)^{-\alpha(\Gamma) + \varepsilon}.
\end{aligned}$$

If $\lambda_1 > 3n/4$, Lemma 8 (ii) gives $\chi_\lambda(1) > \binom{\lambda_1}{n-\lambda_1}$, thus

$$\sum_{\substack{\lambda\vdash n\\ 3n/4<\lambda_1<n-A}} \big(\chi_\lambda(1)\big)^{-\alpha(\Gamma)+\varepsilon} < \sum_{3n/4<\nu<n-A} \binom{\nu}{n-\nu}^{-\alpha(\Gamma)+\varepsilon} p(n-\nu) \ll \binom{n-A}{A}^{-\alpha(\Gamma)+\varepsilon};$$

whereas for $\lambda_1 \leq 3n/4$, Lemma 8 (i) implies $\chi_\lambda(1) > 2^{n/8}$, hence

$$\sum_{\substack{\lambda\vdash n\\ \|\lambda\|\leq\lambda_1\leq 3n/4}} \big(\chi_\lambda(1)\big)^{-\alpha(\Gamma)+\varepsilon} < 2^{-n/8}p(n) < 2^{-n/9}.$$

We conclude that $\sum_3 \ll n^{-\alpha(\Gamma)A+\varepsilon}$.

Next, we consider $\sum_2$. Suppose that $\delta = 2$. Then every permutation of order a_i, every e_j-th power of a permutation and every commutator is even, hence $\chi_\lambda(\pi) = \chi_{\lambda'}(\pi)$ for π with $\pi^{a_i} = 1$, and $m_{\chi_\lambda}^{(e_j)} = m_{\chi_{\lambda'}}^{(e_j)}$, and we obtain $\sum_2 = \sum_1$ in this case. If, on the other hand, $\delta = 1$, then either there is some i such that a_i is even, or there is some j such that e_j is odd. In the first case, write

$$\begin{aligned}\alpha_{\chi_\lambda}^{(a_i)} &= \frac{1}{|\operatorname{Hom}(C_{a_i}, S_n)|}\sum_{\pi^{a_i}=1}\chi_\lambda(\pi)\\ &= \frac{1}{|\operatorname{Hom}(C_{a_i}, S_n)|}\sum_{\pi^{a_i}=1}\sum_{\sum_{t\leq\Delta} te_t=\Delta}\gamma_{e_1,\dots,e_\Delta}\prod_{t|a_i}(-1)^{(t-1)c_t(\pi)}\big(c_t(\pi)\big)^{e_t},\end{aligned}$$

where $\Delta = n - \|\lambda\|$, and the coefficients $\gamma_{e_1,\dots,e_\Delta}$ are determined via Lemma 7. Interchanging summations and applying Lemma 15 (ii), we see that $\alpha_{\chi_\lambda}^{(a_i)} < e^{-cn^{1/a_i}}$, and $\sum_2$ is negligible. In the second case, we have $m_{\chi_\lambda}^{(e_i)} = 0$ for some i and n sufficiently large by Proposition 2 (iii), hence $\sum_3$ vanishes. By what we have shown so far,

$$\sum\nolimits_1 + \sum\nolimits_2 + \sum\nolimits_3 = \delta\sum\nolimits_1 + \mathcal{O}(n^{-A\alpha(\Gamma)+\varepsilon}).$$

To deal with $\sum_1$, we fix a partition $\lambda \vdash n$ with $\lambda_1 \geq n - A$. Then $\prod_{j=1}^s m_{\chi_\lambda}^{(e_j)}$ is ultimately constant, and $\chi_\lambda(1)$ is a polynomial in n of degree $n - \lambda_1$. Using Lemmas 7 and 15 (i), we compute

$$\begin{aligned}\alpha_{\chi_\lambda}^{(a_i)} &= \frac{1}{|\operatorname{Hom}(C_{a_i}, S_n)|}\sum_{\pi^{a_i}=1}\chi_\lambda(\pi)\\ &= \frac{1}{|\operatorname{Hom}(C_{a_i}, S_n)|}\sum_{\pi^{a_i}=1}\sum_{\sum_{t|a_i} te_t\leq\Delta}\gamma_{e_1,\dots,e_{a_i}}\prod_{t|a_i}\big(c_t(\pi)\big)^{e_t}\\ &= \sum_{\sum_{t|a_i} te_t\leq\Delta}\gamma_{e_1,\dots,e_{a_i}}\sum_{k\leq\sum_{t|a_i} te_t}\alpha_{e_1,\dots,e_{a_i}}^{(k)}\frac{n!}{(n-k)!}\frac{|\operatorname{Hom}(C_{a_i}, S_{n-k})|}{\operatorname{Hom}(C_{a_i}, S_n)|}.\end{aligned}$$

By [25, Eq. (22)] we have, for every finite group G and each fixed k, an asymptotic expansion

$$\frac{|\operatorname{Hom}(G, S_n)|}{|\operatorname{Hom}(G, S_{n-k})|} \approx n^{k(1-1/m)}\exp\left(\sum_{\nu=1}^{\infty} Q_\nu^{(k)} n^{-\nu/m}\right), \quad (n\to\infty), \qquad (37)$$

where the coefficients $Q_\nu^{(k)}$ are given in [25] after Equation (22). Putting $G = C_{a_i}$, we find that

$$\alpha_{\chi_\lambda}^{(a_i)} \approx n^{\Delta/a_i}\left(\sum_{\nu=0}^\infty A_\nu^{\lambda,a_i} n^{-\nu/a_i}\right), \quad n \to \infty.$$

Inserting these results into (36), we obtain an asymptotic formula

$$\beta_{\chi_\lambda}^{(R)} = (n!)^{s+2t} n^{(1-l(r+s+2t)+\sum_i 1/a_i)\Delta}\left(\sum_{\nu=0}^\infty B_\nu^{\lambda,R} n^{-\nu/m_\Gamma}\right), \quad n \to \infty.$$

For fixed A, there are only finitely many partitions $\lambda \vdash n$ with $\Delta \leq A$, hence, we obtain an asymptotic expansion for $\sum_1$ with leading term given by the partition $\lambda = (n)$. In this case, $\alpha_{\chi_{(n)}}^{(a_i)} = m_{\chi_{(n)}}^{(e_i)} = 1$, thus, $\beta_{\chi_{(n)}}^{(R)} = (n!)^{s+2t}$, and therefore, as $n \to \infty$,

$$|\operatorname{Hom}(\Gamma, S_n)| = N_R(1) \approx \delta (n!)^{s+2t-1} \prod_{i=1}^r |\operatorname{Hom}(C_{a_i}, S_n)| \left(1 + \sum_{\nu=1}^\infty C_\nu(\Gamma) n^{-\nu/m_\Gamma}\right).$$

Using the asymptotic expansion [24, Theorem 5] for $|\operatorname{Hom}(G, S_n)|$, the main term of the last expression is found to be

$$\delta L_\Gamma (n!)^{\mu(\Gamma)+1} n^{-1} \Phi_\Gamma(n),$$

with $\mu(\Gamma), L_\Gamma, \Phi_\Gamma$ and δ as defined above. Mimicking the proof of [25, Prop. 1] and using our assumption that $\mu(\Gamma) \geq \alpha(\Gamma) > 0$, we find that, for each fixed $K \geq 1$,

$$\sum_{k=K}^{n-K} \frac{h_k(\Gamma) h_{n-k}(\Gamma)}{h_n(\Gamma)} \ll n^{-K\mu(\Gamma)}.$$

Combining the latter estimate with the Lemma from [25, Sec. 3] (cf. also [2]) and the transformation formula[9]

$$s_n(\Gamma) = n h_n(\Gamma) - \sum_{k=1}^{n-1} h_{n-k}(\Gamma) s_k(\Gamma), \tag{38}$$

now gives

$$\frac{s_n(\Gamma)}{n h_n(\Gamma)} \approx 1 + \sum_{k=1}^\infty d_k(\Gamma) \frac{h_{n-k}(\Gamma)}{h_n(\Gamma)}, \quad (n \to \infty), \tag{39}$$

where $d_k(\Gamma)$ is the coefficient of z^k in the formal power series $\left(\sum_{n\geq 0} h_n(\Gamma) z^n\right)^{-1}$. Expanding $\frac{h_{n-k}(\Gamma)}{h_n(\Gamma)}$ by means of the asymptotic formula for $h_n(\Gamma)$ and the Taylor-series of $\Phi_\Gamma(n)$, the theorem follows. □

The condition $\alpha(\Gamma) > 0$ in Theorem 3 is essentially necessary. It can be violated in one of two ways: either $\mu(\Gamma) \leq 0$, or $\mu(\Gamma) > 0$, but there are sufficiently many large values among the e_j to keep $\alpha(\Gamma)$ small. Here, we deal with the first possibility; cf. Subsection 5.3 for the second case.

The groups Γ with a presentation of the form (35) and $\mu(\Gamma) \leq 0$ naturally fall into three classes, according to whether $\mu(\Gamma) = 0$, and either $s = 0$, or $e_j = 2$ for all $j \leq s$;

[9] Cf. [9, Prop. 1] or [23, Prop. 1]. A far reaching generalisation of this counting principle is found in [26].

or $\mu(\Gamma) = 0$ and $e_j > 2$ for some j; or $\mu(\Gamma) < 0$. We will show that in each of these cases the assertion of Theorem 3 fails to hold.

(i) $\mu(\Gamma) = 0$, and either $s = 0$ or $e_j = 2$ for all $j \leq s$. Then Γ is virtually abelian of rank 2, hence, $s_n(\Gamma) \ll n^c$; cf. [20, Chapter III, Prop. 7.10]. This would certainly contradict the assertion of Theorem 3, provided that $r \neq 0$. If $r = 0$, we have $\Gamma = \langle x, y \,|\, [x, y] = 1\rangle$ or $\Gamma = \langle x, y \,|\, x^2y^2 = 1\rangle$, and $s_n(\Gamma) = \sigma(n)$ in both cases, whereas Theorem 3 would predict $s_n(\Gamma) \sim n^{3/2}$.

(ii) $\mu(\Gamma) = 0$, and $e_1 > 2$, say. Then either $r = 2$, $a_1 = a_2 = 2$, or $r = 0, s = 2, t = 0$. In the first case, Γ maps homomorphically onto $C_2 * C_{e_1}$, whereas in the second case, Γ maps homomorphically onto $C_{e_1} * C_{e_2}$; that is, in both cases Γ maps onto a free product with negative Euler characteristic, and therefore $s_n(\Gamma) \gg s_n(C_2 * C_3) \gg (n!)^{1/6}$, while Theorem 3 would predict that Γ is of subexponential growth.

(iii) $\mu(\Gamma) < 0$. In this case, Γ is finite, and $s_n(\Gamma)$ is ultimately 0, which contradicts the assertion of Theorem 3 as well.

5.2. **Computation of the coefficients $a_\nu(\Gamma)$.** In this section we describe how the coefficients $a_\nu(\Gamma)$ can be computed explicitly. We begin by giving explicit values to some of the quantities shown to exist in the previous sections.

Combining Lemmas 7, 15, and 16, we evaluate the constants $\alpha_{\chi_\lambda}^{(q)}$ for partitions $\lambda \vdash n$ with $\Delta \leq 2$.

Lemma 21. *Let $q \geq 2$ be an integer. Then we have*

$$\alpha_{\chi_{(n-1,1)}}^{(q)} = |\operatorname{Hom}(C_q, S_n)|^{-1} \sum_{\pi^q=1} \chi_{(n-1,1)}(\pi) \quad = n\frac{|\operatorname{Hom}(C_q, S_{n-1})|}{|\operatorname{Hom}(C_q, S_n)|},$$

and for q even

$$\alpha_{\chi_{(n-2,2)}}^{(q)} = |\operatorname{Hom}(C_q, S_n)|^{-1} \sum_{\pi^q=1} \chi_{(n-2,2)}(\pi) \quad = \frac{n^2}{2}\frac{|\operatorname{Hom}(C_q, S_{n-2})|}{|\operatorname{Hom}(C_q, S_n)|}$$

$$\alpha_{\chi_{(n-2,1,1)}}^{(q)} = |\operatorname{Hom}(C_q, S_n)|^{-1} \sum_{\pi^q=1} \chi_{(n-2,1,1)}(\pi) \quad = 1 + \frac{n^2}{2}\frac{|\operatorname{Hom}(C_q, S_{n-2})|}{|\operatorname{Hom}(C_q, S_n)|}$$

whereas for q odd

$$\alpha_{\chi_{(n-2,2)}}^{(q)} = |\operatorname{Hom}(C_q, S_n)|^{-1} \sum_{\pi^q=1} \chi_{(n-2,2)}(\pi) \quad = -1 + \frac{n(n-1)}{2}\frac{|\operatorname{Hom}(C_q, S_{n-2})|}{|\operatorname{Hom}(C_q, S_n)|},$$

$$\alpha_{\chi_{(n-2,1,1)}}^{(q)} = |\operatorname{Hom}(C_q, S_n)|^{-1} \sum_{\pi^q=1} \chi_{(n-2,1,1)}(\pi) \quad = \frac{n(n-1)}{2}\frac{|\operatorname{Hom}(C_q, S_{n-2})|}{|\operatorname{Hom}(C_q, S_n)|}.$$

We now use (37) and [24, Theorem 6] to compute the first terms of the asymptotic series for $\alpha^{(q)}_{\chi_{(n-2,2)}}$. We obtain

$$\alpha^{(q)}_{\chi_{(n-2,2)}} = n^{2/q}\big(1+R_q(n^{-1/q})\big)\left(1-2\sum_{\nu=1}^{q+3}\tilde{Q}^{(q)}_{\nu}n^{-\nu/q}+S_q(n^{-1/q})\right)+\mathcal{O}(n^{-\frac{q+2}{q}}),$$

where the polynomials R_q, S_q are given as follows.

q	$R_q(z)$	$S_q(z)$
2	$\frac{1}{2}z^2-\frac{1}{4}z^3+\frac{1}{8}z^4+\frac{1}{32}z^5$	$\frac{3}{4}z^2-\frac{7}{8}z^3+\frac{23}{64}z^4+\frac{5}{128}z^5$
3	$\frac{1}{3}z^3-\frac{2}{9}z^5+\frac{5}{36}z^6$	$\frac{1}{3}z^4-\frac{1}{3}z^5+\frac{17}{108}z^6$
4	$\frac{1}{4}z^4-\frac{1}{8}z^6$	$\frac{3}{16}z^4+\frac{3}{8}z^5+\frac{25}{64}z^6+\frac{33}{64}z^7$
5	$\frac{1}{5}z^5$	$\frac{3}{25}z^8$
6	$\frac{1}{6}z^6-\frac{1}{12}z^9$	$\frac{1}{12}z^6+\frac{1}{6}z^7+\frac{1}{4}z^8-\frac{55}{216}z^9$
7	$\frac{1}{7}z^7$	0
8, 12	$\frac{1}{q}z^q$	$\frac{3}{q^2}\big(z^q+z^{q+2}+z^{q+3}\big)$
9	$\frac{1}{9}z^9$	$\frac{1}{27}z^{12}$
10, 18	$\frac{1}{q}z^q$	$\frac{3}{q^2}\big(z^q+z^{q+3}\big)$
14, 16	$\frac{1}{q}z^q$	$\frac{3}{q^2}z^q$
$q \geq 20$, even	$\frac{1}{q}z^q$	$\frac{3}{q^2}z^q$
$q \geq 11$, odd	$\frac{1}{q}z^q$	0

Note that by Lemma 21, we have $\alpha^{(q)}_{\chi_{(n-2,1,1)}} = 1+\alpha^{(q)}_{\chi_{(n-2,2)}}$, that is, the asymptotic series above contains all necessary information for both characters.

As an example, consider the triangle group

$$\Gamma = \Big\langle x,y,z \,\Big|\, x^2=y^3=z^7=xyz=1\Big\rangle.$$

Here, $\mu(\Gamma)=\alpha(\Gamma)=\frac{1}{42}$ and $m_\Gamma=42$. We first show how to determine the contribution of characters χ_λ with $\Delta>2$. By Lemmas 7 and 15 (ii), we see that, for fixed Δ and q prime,

$$\alpha^{(q)}_{\chi_\lambda} = \Big(1+\mathcal{O}(n^{-1/q})\Big)\chi_{\lambda\setminus\lambda_1}(1)\frac{n^{\Delta/q}}{\Delta!}.$$

Hence, for the triangle group Γ we obtain

$$\beta^{(R)}_{\chi_\lambda} = \Big(1+\mathcal{O}(n^{-1/7})\Big)\frac{(\chi_{\lambda\setminus\lambda_1}(1))^3 n^{41\Delta/42}}{(\Delta!)^3(\chi_\lambda(1))^2}.$$

Thus, from (36), we obtain

$$|\operatorname{Hom}(\Gamma, S_n)| = \frac{|\operatorname{Hom}(C_2, S_n)||\operatorname{Hom}(C_3, S_n)||\operatorname{Hom}(C_7, S_n)|}{n!}$$
$$\times \left(\sum_{\substack{\lambda\\ \Delta\leq 2}} \chi_\lambda(1)\beta_{\chi_\lambda}^{(R)} + \sum_{\substack{\lambda\\ 3\leq\Delta\leq 22}} \frac{(\chi_{\lambda\backslash\lambda_1}(1))^3 n^{41\Delta/42}}{(\Delta!)^3\chi_\lambda(1)} + \mathcal{O}(n^{-23/42})\right).$$

Given our previous work in this section, the sum over Δ can be computed to whatever length is required. We have cut the sum after the term $\Delta = 22$, since this is the smallest precision bringing to bear all phenomena occurring in such computations at arbitrary scale. For $\Delta = 0$, we have $\beta_{\chi_\lambda}^{(R)} = 1$, whereas for $1 \leq \Delta \leq 2$, we use the asymptotic for $\alpha_{\chi_\lambda}^{(q)}$ computed above, to obtain

$$\sum_{\substack{\lambda\\ \Delta\leq 2}} \chi_\lambda(1)\beta_{\chi_\lambda}^{(R)} = 1 + n^{-1/42} + \frac{1}{2}n^{-1/21} + \frac{1}{2}n^{-11/21} + \mathcal{O}(n^{-23/42}).$$

From Lemma 7, we obtain, for Δ fixed and $n \to \infty$, the asymptotic estimate

$$\chi_\lambda(1) = \Big(1 + \mathcal{O}(n^{-1})\Big)\frac{\chi_{\lambda\backslash\lambda_1}(1) n^\Delta}{\Delta!},$$

which implies

$$\begin{aligned}\sum_{\substack{\lambda\\ 3\leq\Delta\leq 22}} \frac{(\chi_{\lambda\backslash\lambda_1}(1))^3 n^{41\Delta/42}}{(\Delta!)^3\chi_\lambda(1)} &= \Big(1 + \mathcal{O}(n^{-1})\Big) \sum_{\substack{\lambda\\ 3\leq\Delta\leq 22}} \frac{(\chi_{\lambda\backslash\lambda_1}(1))^2 n^{-\Delta/42}}{(\Delta!)^2}\\ &= \Big(1 + \mathcal{O}(n^{-1})\Big) \sum_{3\leq\Delta\leq 22} \frac{n^{-\Delta/42}}{\Delta!};\end{aligned}$$

and combining these estimates we obtain

$$|\operatorname{Hom}(\Gamma, S_n)| = \frac{1}{n!}|\operatorname{Hom}(C_2, S_n)||\operatorname{Hom}(C_3, S_n)||\operatorname{Hom}(C_7, S_n)|$$
$$\times \left(1 + \sum_{\Delta=1}^{22} \frac{n^{-\Delta/42}}{\Delta!} + \frac{1}{2}n^{-11/21} + \mathcal{O}(n^{-23/42})\right).$$

For $1 \leq k \leq 22$, we compute $s_k(\Gamma)$ using the software package GAP [12], and obtain

$$s_k(\Gamma) = \begin{cases} 1, & k = 1, 8, 9\\ 2, & k = 7\\ 3, & k = 15\\ 9, & k = 14, 21\\ 13, & k = 22\\ 0, & \text{otherwise,}\end{cases} \qquad 1 \leq k \leq 22.$$

From these values, $h_k(\Gamma)$ and hence $d_k(\Gamma)$ are easily computed for $1 \leq k \leq 22$. The first three coefficients of the asymptotic series for $|\operatorname{Hom}(C_q, S_n)|$ are given in [24], after

Corollary 2. Putting together the various expansions, our final result is that

$$\begin{aligned} s_n(\Gamma) = {} & \frac{(2\pi)^{-\frac{53}{21}} e^{-\frac{1}{4}}}{\sqrt{42}} (n!)^{\frac{1}{42}} n^{-\frac{11}{21}} \exp\left(n^{1/2} + n^{1/3} + n^{1/7}\right) \\ & \times \Big\{ 1 - \frac{2}{7} n^{-1/6} - \frac{1}{8} n^{-4/21} - \frac{1}{9} n^{-3/14} - \frac{113}{147} n^{-1/3} - \frac{23}{140} n^{-5/14} + \frac{319}{8064} n^{8/21} \\ & \qquad + \frac{1}{72} n^{-17/42} + \frac{1}{162} n^{-3/7} + \frac{745}{8232} n^{-1/2} - \frac{28309}{64680} n^{11/21} + \mathcal{O}(n^{-23/42}) \Big\}. \end{aligned}$$

5.3. **One-relator groups.** The result of this subsection, apart from its inherent interest, also demonstrates that certain Fuchsian groups Γ with $\mu(\Gamma) > 0$ and $\alpha(\Gamma) < 0$ have a much faster growth than would be predicted by Theorem 3. Consider a one-relator group

$$\Gamma = \Big\langle y_1, y_2, \dots, y_s \,\Big|\, y_1^{e_1} y_2^{e_2} \cdots y_s^{e_s} = 1 \Big\rangle, \tag{40}$$

and let $\bar{\Gamma} := C_{e_1} * C_{e_2} * \cdots * C_{e_s}$.

Theorem 4. *Let* Γ *be as in* (40), *and suppose that* $s \geq 2$ *and*

$$\alpha(\Gamma) = -2 + \sum_{1 \leq j \leq s} \frac{2}{e_j} < 0.$$

Then, as n tends to infinity, we have

$$s_n(\Gamma) \sim s_n(\bar{\Gamma}) \sim K (n!)^{\mu(\Gamma) - \alpha(\Gamma)/2} \exp\left(\sum_{j=1}^{s} \sum_{\substack{\nu \mid e_j \\ \nu < e_j}} \frac{n^{\nu/e_j}}{\nu} + \frac{\alpha(\Gamma) - 2\mu(\Gamma) + 2}{4} \log n \right),$$

where

$$K = \frac{\exp\left(-\sum\limits_{\substack{j \\ 2 \mid e_j}} (2e_j)^{-1} \right)}{(2\pi)^{\frac{2 + 2\mu(\Gamma) - \alpha(\Gamma)}{4}} \sqrt{e_1 e_2 \cdots e_s}}.$$

Proof. We have

$$\begin{aligned} |\operatorname{Hom}(\Gamma, S_n)| &= \Big| \Big\{ (\pi_1, \dots, \pi_s) \in S_n^s : \pi_1^{e_1} \pi_2^{e_2} \cdots \pi_s^{e_s} = 1 \Big\} \Big| \\ &= \sum_{\mathbf{c}_1, \dots, \mathbf{c}_s} r_{e_1}(\mathbf{c}_1) r_{e_2}(\mathbf{c}_2) \cdots r_{e_s}(\mathbf{c}_s) N(\mathbf{c}_1, \dots, \mathbf{c}_s), \end{aligned} \tag{41}$$

where

$$N(\mathbf{c}_1, \dots, \mathbf{c}_s) := \Big| \Big\{ (\pi_1, \dots, \pi_s) \in S_n^s : \pi_1 \pi_2 \cdots \pi_s = 1,\ \pi_i \in \mathbf{c}_i \, (1 \leq i \leq s) \Big\} \Big|.$$

The contribution in (41) of the term corresponding to $\mathbf{c}_1 = \mathbf{c}_2 = \cdots = \mathbf{c}_s = 1$ is

$$|\operatorname{Hom}(C_{e_1}, S_n)| \cdot |\operatorname{Hom}(C_{e_2}, S_n)| \cdots |\operatorname{Hom}(C_{e_s}, S_n)| = |\operatorname{Hom}(\bar{\Gamma}, S_n)|.$$

We shall show that the sum over the remaining terms is of lesser order of magnitude. Since $N(\mathbf{c}_1, \dots, \mathbf{c}_s)$ is invariant under permutation of its arguments, we may assume that $|\mathbf{c}_1| \geq |\mathbf{c}_j|$ for all j. Hence,

$$\begin{aligned} N(\mathbf{c}_1, \dots, \mathbf{c}_s) &= \Big|\Big\{(\pi_2, \dots, \pi_s) \in S_n^{s-1} : \pi_2\pi_3\cdots\pi_s \in \mathbf{c}_1, \, \pi_j \in \mathbf{c}_j \, (2 \leq j \leq s)\Big\}\Big| \\ &\leq |\mathbf{c}_2| \cdot |\mathbf{c}_3| \cdots |\mathbf{c}_s| \\ &\leq \prod_{1\leq j\leq s} |\mathbf{c}_j|^{1-\delta_j} \end{aligned}$$

for any choice of non-negative real numbers $\delta_1, \delta_2 \dots, \delta_s$ such that $\sum_j \delta_j = 1$. For a non-empty set $J \subseteq [s]$, define $S_J := \sum_{j\in J} 1/e_j$. By our assumption, $S_J < 1$, and, by definition, $\sum_{j\in J} 1/(S_J e_j) = 1$. Using the above estimate for $N(\mathbf{c}_1, \dots, \mathbf{c}_s)$ with $\delta_j = 1/(S_J e_j)$, dividing Equation (41) by $|\operatorname{Hom}(\bar{\Gamma}, S_n)|$, and interchanging product and sum, we find that

$$\begin{aligned} 0 \leq \frac{|\operatorname{Hom}(\Gamma, S_n)|}{|\operatorname{Hom}(\bar{\Gamma}, S_n)|} - 1 &\leq \sum_{\substack{J \\ \emptyset\neq J\subseteq[s]}} \sum_{\substack{\mathbf{c}_1,\dots,\mathbf{c}_s \\ \mathbf{c}_j\neq 1 \Leftrightarrow j\in J}} \prod_{j\in J} \frac{r_{e_j}(\mathbf{c}_j)|\mathbf{c}_j|^{1-1/(S_J e_j)}}{|\operatorname{Hom}(C_{e_j}, S_n)|} \\ &= \sum_{\substack{J \\ \emptyset\neq J\subseteq[s]}} \prod_{j\in J} \sum_{\mathbf{c}\neq 1} \frac{r_{e_j}(\mathbf{c})|\mathbf{c}|^{1-1/(S_J e_j)}}{|\operatorname{Hom}(C_{e_j}, S_n)|}. \end{aligned}$$

Consider the factor in the last expression corresponding to $j \in J$ for a given set J. Classifying the conjugacy classes according to the number ℓ of points moved by each of its elements, this factor can be written as

$$\sum_{2\leq\ell\leq n} \sum_{\substack{\mathbf{c} \\ \mathbf{c} \text{ moves } \ell \text{ points}}} \frac{r_{e_j}(\mathbf{c})|\mathbf{c}|^{1-1/(S_J e_j)}}{|\operatorname{Hom}(C_{e_j}, S_n)|} =$$

$$\sum_{2\leq\ell\leq n} \binom{n}{\ell}^{1-1/(S_J e_j)} \frac{|\operatorname{Hom}(C_{e_j}, S_{n-\ell})|}{|\operatorname{Hom}(C_{e_j}, S_n)|} \sum_{\mathbf{c}}{}^{*} r_{e_j}(\mathbf{c})|\mathbf{c}|^{1-1/(S_J e_j)}, \quad (42)$$

where the innermost sum extends over all fixed-point free conjugacy classes of S_ℓ. From [24, Corollary 2] we deduce that

$$\frac{|\operatorname{Hom}(C_{e_j}, S_{n-\ell})|}{|\operatorname{Hom}(C_{e_j}, S_n)|} \ll \left[\binom{n}{\ell}\ell!\right]^{-(1-1/e_j)}.$$

Applying the Cauchy-Schwarz inequality, we find for the innermost sum in (42) that

$$\begin{aligned} \sum_{\mathbf{c}}{}^{*} r_{e_j}(\mathbf{c})|\mathbf{c}|^{1-1/(S_J e_j)} &\leq \left(\sum_{\mathbf{c}} \big(r_{e_j}(\mathbf{c})\big)^2 |\mathbf{c}|\right)^{1/2} \left(\sum_{\mathbf{c}} |\mathbf{c}|^{1-2/(S_J e_j)}\right)^{1/2} \\ &\leq \left(\sum_{\chi\in\operatorname{Irr}(S_\ell)} \big(\chi(1)\big)^{2-\frac{4}{e_j}+\varepsilon}\right)^{1/2} \left(\sum_{\mathbf{c}} |\mathbf{c}|^{1-2/(S_J e_j)}\right)^{1/2}, \end{aligned}$$

where we have used Proposition 2 (i) to estimate the first factor. If $S_J e_j > 2$, then we bound the second factor by $(\ell!)^{1-2/(S_J e_j)+\varepsilon}$; otherwise, each summand is ≤ 1, and

$$\sum_{\mathbf{c}} |\mathbf{c}|^{1-2/(S_J e_j)} \ll (\ell!)^{\varepsilon}.$$

In both cases,

$$\sum_{\mathbf{c}} r_{e_j}(\mathbf{c})|\mathbf{c}|^{1-1/(S_J e_j)} \leq \max\Big((\ell!)^{1-\frac{1}{e_j}-\frac{1}{S_J e_j}+\varepsilon}, (\ell!)^{\frac{1}{2}-\frac{1}{e_j}+\varepsilon}\Big). \tag{43}$$

Putting (43) back into (42), we find that the left-hand side of (42) is bounded above by

$$\sum_{2\leq\ell\leq n} \binom{n}{\ell}^{1-1/(S_J e_j)} \left[\binom{n}{\ell}\ell!\right]^{-(1-1/e_j)} \max\Big((\ell!)^{1-\frac{1}{e_j}-\frac{1}{S_J e_j}+\varepsilon}, (\ell!)^{\frac{1}{2}-\frac{1}{e_j}+\varepsilon}\Big) =$$

$$\sum_{2\leq\ell\leq n} \binom{n}{\ell}^{\frac{1}{e_j}-\frac{1}{S_J e_j}} \max\Big((\ell!)^{-\frac{1}{S_J e_j}+\varepsilon}, (\ell!)^{-\frac{1}{2}+\varepsilon}\Big).$$

For sufficiently large n, increasing ℓ by 1 decreases a summand by at least a factor $\frac{1}{2}$; hence, as $n \to \infty$,

$$\sum_{2\leq\ell\leq n} \sum_{\substack{\mathbf{c} \\ \mathbf{c} \text{ moves } \ell \text{ points}}} \frac{r_{e_j}(\mathbf{c})|\mathbf{c}|^{1-1/(S_J e_j)}}{|\operatorname{Hom}(C_{e_j}, S_n)|} \ll n^{-2(\frac{1}{S_J e_j}-\frac{1}{e_j})},$$

and, therefore,

$$|\operatorname{Hom}(\Gamma, S_n)| \sim |\operatorname{Hom}(\bar{\Gamma}, S_n)|, \quad n \to \infty.$$

Since $\chi(\bar{\Gamma}) = \sum_j 1/e_j - s + 1 < 0$, and since the proof of [25, Proposition 1] only depends on an asymptotic estimate, we infer in particular that

$$\sum_{0<k<n} \binom{n}{k} \frac{|\operatorname{Hom}(\Gamma, S_k)||\operatorname{Hom}(\Gamma, S_{n-k})|}{|\operatorname{Hom}(\Gamma, S_n)|} \to 0 \text{ as } n \to \infty.$$

Combining this fact with the transformation formula (38) and [32, Theorem 3], we find that

$$s_n(\Gamma) \sim |\operatorname{Hom}(\Gamma, S_n)|/(n-1)! \sim |\operatorname{Hom}(\bar{\Gamma}, S_n)|/(n-1)! \sim s_n(\bar{\Gamma}).$$

The explicit asymptotic formula given for $s_n(\bar{\Gamma})$ results from [25, Theorem 1]. □

Remark. Theorem 4 was proved in [28, Example 1(ii)] for $\alpha(\Gamma) < -1$ (note that the invariant $\alpha(\Gamma)$ defined in [28, Sec. 2] is $\frac{\alpha(\Gamma)+2}{2}$ in our present notation).

5.4. **Demuškin groups.** Let p be a prime. A pro-p-group Γ is termed a Poincaré group of dimension n, if Γ has cohomological dimension n, and the algebra $H^*(\Gamma)$ is finite dimensional and satisfies Poincaré duality. A Poincaré group of dimension 2 is called a Demuškin group. These are one-relator groups

$$\Gamma = \big\langle x_1, \dots, x_m \,|\, R(x_1, \dots, x_m) = 1\big\rangle, \quad m = \dim H^1(\Gamma),$$

and, for $p \neq 2$, the defining relation may be taken to be

$$R = x_1^{p^h}[x_1, x_2][x_3, x_4]\cdots[x_{m-1}, x_m], \quad h \in \mathbb{N} \cup \{\infty\},$$

with the understanding that $x_1^{p^h}=1$ if $h=\infty$; cf [4]–[6] and [19]. With the convention $p^\infty=0$, the occurring relations are ordinary relations, although the group defined is to be understood as a pro-p-group. Hence, the same relator defines a discrete one-relator group having the Demuškin group as pro-p-completion. For this reason, it is interesting to study the subgroup growth of these discrete groups. For $m=2$, these groups are metacyclic, and their subgroup growth can be computed using the methods of [13]. The similarity of R to a surface group relation would allow us to estimate $s_n(\Gamma)$ asymptotically for $m\geq 6$, using only tools from [27]. The case $m=4$ however needs a more careful analysis. As another application of our estimates for multiplicities of root number functions, we prove the following result.

Theorem 5. *For integers $q\geq 1$ and $d\geq 2$, let*

$$\Gamma_{q,d}=\Big\langle x_1,y_1,\dots,x_d,y_d\,\Big|\,x_1^{q-1}[x_1,y_1][x_2,y_2]\cdots[x_d,y_d]=1\Big\rangle.$$

Then there exist explicitly computable constants $\gamma_\nu(\Gamma_{q,d})$, such that

$$s_n(\Gamma_{q,d})\approx\delta n(n!)^{2d-2}\left\{1+\sum_{\nu=1}^\infty\gamma_\nu(\Gamma_{q,d})n^{-\nu}\right\},\quad (n\to\infty),$$

where

$$\delta=\begin{cases}1, & q\text{ even}\\ 2, & q\text{ odd.}\end{cases}$$

The proof runs parallel to the proof of Theorem 3, once we have established the following.

Lemma 22. *Let $q\geq 2$ an integer. For a partition $\lambda\vdash n$, define the coefficient $l_{\chi_\lambda}^{(q)}$ by means of the equation*

$$\big|\{(\sigma,\tau)\in S_n^2:\sigma^{q-1}[\sigma,\tau]=\pi\}\big|=n!\sum_{\lambda\vdash n}l_{\chi_\lambda}^{(q)}\chi_\lambda(\pi).$$

Then we have $|l_{\chi_\lambda}^{(q)}|\leq\sqrt{\frac{m_{\chi_\lambda}^{(q)}}{\chi_\lambda(1)}}$. Moreover, for a partition $\mu\vdash l$, and a partition $\lambda\vdash n$ with $\lambda\setminus\lambda_1=\mu$, the quantity $\chi_\lambda(1)l_{\chi_\lambda}^{(q)}$ is a constant depending only on μ, provided n is sufficiently large.

Proof. Writing the equation $x^{k-1}[x,y]=\pi$ as $x^k(x^{-1})^y=\pi$, we see that the number of solutions can be computed as

$$\sum_{\mathbf{c}}|C_{S_n}(\mathbf{c})|\cdot\big|\{\sigma,\tau\in\mathbf{c}:\,\sigma^n\tau=\pi\}\big|=\sum_{\mathbf{c}}|\mathbf{c}|\sum_{\lambda\vdash n}\frac{\chi_\lambda(\mathbf{c})\chi_\lambda(\mathbf{c}^k)\chi_\lambda(\pi)}{\chi_\lambda(1)},$$

that is,

$$\begin{aligned}
l_{\chi_\lambda}^{(q)} &= \frac{1}{n!}\sum_{\mathbf{c}} |\mathbf{c}| \frac{\chi_\lambda(\mathbf{c})\chi_\lambda(\mathbf{c}^q)}{\chi_\lambda(1)}\\
&\leq \frac{1}{n!\chi_\lambda(1)}\left(\sum_{\mathbf{c}} |\mathbf{c}|(\chi_\lambda(\mathbf{c}))^2\right)^{1/2}\left(\sum_{\mathbf{c}} |\mathbf{c}|(\chi_\lambda(\mathbf{c}^q))^2\right)^{1/2}\\
&\leq \frac{1}{\sqrt{\chi_\lambda(1)}}\left(\frac{1}{n!}\sum_{\mathbf{c}} |\mathbf{c}|\chi_\lambda(\mathbf{c}^q)\right)^{1/2}\\
&= \sqrt{\frac{m_{\chi_\lambda}^{(q)}}{\chi_\lambda(1)}}.
\end{aligned}$$

For the second claim we have to compute

$$\frac{1}{n!}\sum_{\pi\in S_n}\frac{\chi_\lambda(\pi)\chi_\lambda(\pi^k)}{\chi_\lambda(1)}.$$

We express $\chi_\lambda(\pi)$ as a polynomial in the functions $s_i(\pi)$. Then $\chi_\lambda(\pi)\chi_\lambda(\pi^k)$ is also a polynomial in these functions, and our claim follows from Lemma 13. □

As an example, consider $\lambda=(n-1,1)$. Then

$$\chi_\lambda(\pi)\chi_\lambda(\pi^k) = (c_1(\pi)-1)\Big(\sum_{t|q} tc_t(\pi)-1\Big).$$

The expected value of the first factor is 0, and it is stochastically independent of $c_2,\dots,c_q$. Hence, we have

$$l_{\chi_\lambda}^{(q)} = \frac{1}{\chi_\lambda(1)n!}\sum_{\pi\in S_n}\big((c_1(\pi))^2-c_1(\pi)\big),$$

and the computations leading to the second assertion in Proposition 2 (ii) give $l_{\chi_\lambda}^{(q)} = \frac{1}{\chi_\lambda(1)} = \frac{1}{n-1}$.

For $\lambda=(n-2,2)$, we find in the case q even

$$\begin{aligned}
\chi_\lambda(\pi)\chi_\lambda(\pi^q) &= \frac{1}{4}(c_1(\pi))^4 - \frac{3}{2}(c_1(\pi))^3 + \frac{13}{4}(c_1(\pi))^2 - 3c_1(\pi) + 1\\
&+ c_2(\pi)\big(-2(c_1(\pi))^2 + 6c_1(\pi) - 4\big) + (c_2(\pi))^2\big((c_1(\pi))^2 - 3c_1(\pi) + 5\big) - 2(c_2(\pi))^3\\
&+ \underbrace{\Big(\frac{1}{2}(c_1(\pi))^2 - \frac{3}{2}c_1(\pi) - c_2(\pi) + 1\Big)}_{=:A}\Bigg(\frac{1}{2}\sum_{\substack{t|q\\ t\geq 3}} t^2(c_t(\pi))^2 - \frac{3}{2}\sum_{\substack{t|q\\ t\geq 3}} tc_t(\pi) + \sum_{\substack{t|2q\\ t=2(t,q)\\ t\geq 3}} tc_t(\pi)\Bigg).
\end{aligned}$$

Note that the expected value of A is 0, hence, since the second factor contains only terms $c_t(\pi)$ with $t\geq 3$, it is stochastically independent of the first factor, and the expectation of the last summand vanishes; using Lemma 13, we find that the remaining terms vanish as well. Dealing in a similar way with the other cases, we obtain

	q even	q odd
$l^{(q)}_{\chi_{(n-2,2)}}$	0	$\dfrac{1}{n^2-3n}$
$l^{(q)}_{\chi_{(n-2,1,1)}}$	$\dfrac{13}{2(n^2-3n+2)}$	$\dfrac{9}{2(n^2-3n+2)}$

As an example for the computation of the coefficients $\gamma_\nu(\Gamma_{q,d})$, we consider the case $d=2$ and $q\geq 2$. From the values given above we deduce the estimate

$$\frac{h_n(\Gamma)}{(n!)^2} = 1 + \frac{1}{(n-1)^3} + \begin{Bmatrix} \frac{26}{(n^2-3n+2)^3}, & q \text{ even} \\ \frac{4}{(n^2-3n)^3} + \frac{18}{(n^2-3n+2)^3}, & q \text{ odd.} \end{Bmatrix} + \mathcal{O}(n^{-9}).$$

For small values of k, we compute $h_k(\Gamma_{q,2})$ as follows:

$$h_1(\Gamma_{q,2}) = 1, \quad h_2(\Gamma_{q,2}) = \begin{cases} 8, & (q,2)=1 \\ 4, & (q,2)=2, \end{cases} \quad h_3(\Gamma_{q,2}) = \begin{cases} 72, & (q,6)=1 \\ 45, & (q,6)=2 \\ 63, & (q,6)=3 \\ 36, & (q,6)=6, \end{cases}$$

$$h_4(\Gamma_{q,2}) = \begin{cases} 1424, & (q,6)=1 \\ 720, & (q,6)=2 \\ 1280, & (q,6)=3 \\ 576, & (q,6)=6, \end{cases} \quad h_5(\Gamma_{q,2}) = \begin{cases} 37192, & (q,30)=1 \\ 21092, & (q,30)=2 \\ 36040, & (q,30)=3 \\ 35792, & (q,30)=5 \\ 20840, & (q,30)=6 \\ 19692, & (q,30)=10 \\ 34640, & (q,30)=15 \\ 19440, & (q,30)=30. \end{cases}$$

Proceeding as in Subsection 5.1, we obtain

$$s_n(\Gamma_{q,2}) = \delta n (n!)^2 R(n),$$

where δ is as in Theorem 5, and

$$R(n) = \begin{cases} 1-n^{-1}-7n^{-2}-56n^{-3}-1237n^{-4}-33573n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=1 \\ 1-n^{-1}-3n^{-2}-37n^{-3}-\ \ 623n^{-4}-19460n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=2 \\ 1-n^{-1}-7n^{-2}-47n^{-3}-1111n^{-4}-32826n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=3 \\ 1-n^{-1}-7n^{-2}-56n^{-3}-1237n^{-4}-32173n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=5 \\ 1-n^{-1}-3n^{-2}-28n^{-3}-\ \ 497n^{-4}-19541n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=6 \\ 1-n^{-1}-3n^{-2}-37n^{-3}-\ \ 623n^{-4}-18060n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=10 \\ 1-n^{-1}-7n^{-2}-47n^{-3}-1111n^{-4}-31426n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=15 \\ 1-n^{-1}-3n^{-2}-28n^{-3}-\ \ 497n^{-4}-18141n^{-5}+\mathcal{O}(n^{-6}), & (q,30)=30. \end{cases}$$

Note that the series for $s_n(\Gamma_{q,2})$ is far more dependent on q – and therefore on $\Gamma_{q,2}$ itself – than the series for $h_n(\Gamma_{q,2})$.

6. Finiteness Results

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

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

In [25, Theorem 3] a characterisation in terms of structural invariants is given for the equivalence relation $\sim$ on the class of groups Γ of the form

$$\Gamma = G_1 * G_2 * \cdots * G_s * F_r$$

with $r, s \geq 0$ and finite groups G_σ, and it is shown that each $\sim$-class decomposes into finitely many isomorphism classes. Here we are concerned with the analogous problems for Fuchsian groups.

Theorem 6. (i) *Let* $\Gamma = C_{a_1} * \cdots * C_{a_k} * F_r$ *and* $\Delta = C_{b_1} * \cdots * C_{b_l} * F_{r'}$ *be free products of cyclic groups such that* $s_n(\Gamma) \asymp s_n(\Delta)$. *Then* $r = r'$ *and* $\{a_1, \dots, a_k\} = \{b_1, \dots, b_l\}$ *as multi-sets.*

(ii) *Let*

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

and

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

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

(a) *The multi-sets* $\{a_i : 1 \leq i \leq r\}$ *and* $\{a'_i : 1 \leq i \leq r'\}$ *coincide,*

(b) $\mu(\Gamma) = \mu(\Delta)$,

(c) $\delta = \delta'$.

(iii) *Let*

$$\Gamma = \Big\langle y_1, \dots, y_s \,\Big|\, y_1^{e_1} y_2^{e_2} \cdots y_s^{e_s} = 1 \Big\rangle$$

and

$$\Delta = \Big\langle y_1, \dots, y_{s'} \,\Big|\, y_1^{e'_1} y_2^{e'_2} \cdots y_{s'}^{e'_{s'}} = 1 \Big\rangle$$

be two one-relator groups with $\alpha(\Gamma), \alpha(\Delta) < 0$. *Then the following assertions are equivalent:*

(a) $\Gamma \sim \Delta$.

(b) $s = s'$ *and* $\{e_1, \dots, e_s\} = \{e'_1, \dots, e'_{s'}\}$ *as multi-sets.*

(c) $\hat{\Gamma} \cong \hat{\Delta}$, *where the hat denotes pro-finite completion.*

The proof of Theorem 6 requires the following two auxiliary results.

Lemma 23. *Let $A = \{a_1, \dots, a_k\}$ and $B = \{b_1, \dots, b_l\}$ be multi-sets of integers, such that*

$$\sum_{d|a_i} \frac{1}{a_i} = \sum_{d|b_i} \frac{1}{b_i}$$

for all $d \geq 2$. Then $A = B$.

Proof. We argue by induction on $n = k + l$. For $n \leq 1$, there is nothing to show. Assume that our claim holds for all multi-sets A', B' with $|A'| + |B'| \leq n - 1$, and let A, B be multi-sets as above. Let d be the greatest integer, such that $\sum_{d|a_i} 1/a_i > 0$. Then $d = \max A$, and the value of the sum is $|\{i : a_i = \max A\}|/\max A$. The same holds for B, hence the greatest element of both multi-sets as well as the multiplicity of this maximum coincide. Deleting these elements in both multi-sets yields a pair of multi-sets A', B' of smaller cardinality, which are equal by the induction hypothesis. Hence we deduce $A = B$. □

Lemma 24. *Given positive integers k and l, disjoint tuples of variables $\vec{x}_i = (x_{i1}, \dots, x_{ia_i})$ for $1 \leq i \leq k$, words $w_1(\vec{x}_1), \dots, w_k(\vec{x}_k)$, and (possibly empty) words $v_{ij}(\vec{x}_i)$ for $1 \leq\ i \leq\ k$ and $1 \leq j \leq l$, and a permutation $\sigma \in S_k$, define*

$$\Gamma = \Big\langle \vec{x}_1, \dots, \vec{x}_k \,\Big|\, w_1(\vec{x}_1) \cdots w_k(\vec{x}_k) = v_{ij}(\vec{x}_i) = 1\, (1 \leq i \leq k,\, 1 \leq j \leq l) \Big\rangle$$

and

$$\Gamma_\sigma = \Big\langle \vec{x}_1, \dots, \vec{x}_k \,\Big|\, w_{\sigma(1)}(\vec{x}_{\sigma(1)}) \cdots w_{\sigma(k)}(\vec{x}_{\sigma(k)}) = v_{ij}(\vec{x}_i) = 1\, (1 \leq i \leq k,\, 1 \leq j \leq l) \Big\rangle.$$

Then Γ and Γ_σ have isomorphic pro-finite completions.

Proof. For $1 \leq i \leq k$ and a finite group G, let

$$N_i^{(G)}(g) := \Big|\Big\{\vec{x}_i \in G^{a_i} : w_i(\vec{x}_i) = g, v_{i1}(\vec{x}_i) = \cdots = v_{il}(\vec{x}_i) = 1\Big\}\Big|, \quad g \in G.$$

Since $N_i^{(G)}$ is a class function, we can introduce Fourier coefficients $\alpha_{\chi,i}$ via

$$N_i^{(G)}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \alpha_{\chi,i}\chi(g), \quad g \in G.$$

Then, using orthogonality, we have

$$\begin{aligned}
|\operatorname{Hom}(\Gamma, G)| &= \sum_{\substack{g_1,\dots,g_k \\ g_1g_2\cdots g_k = 1}} \prod_{1\leq i\leq k} N_i^{(G)}(g_i) \\
&= \sum_{\mathbf{c}_1,\dots,\mathbf{c}_k \subseteq G} \frac{|\mathbf{c}_1|\cdots|\mathbf{c}_k|}{|G|} \sum_{\chi} \sum_{\chi_1,\dots,\chi_k} \frac{\chi(\mathbf{c}_1)\cdots\chi(\mathbf{c}_k)}{(\chi(1))^{k-2}} \chi_1(\mathbf{c}_1)\alpha_{\chi_1,1}\cdots\chi_k(\mathbf{c}_k)\alpha_{\chi_k,k} \\
&= |G|^{k-1} \sum_{\chi} \frac{\alpha_{\overline{\chi},1}\cdots\alpha_{\overline{\chi},k}}{(\chi(1))^{k-2}}.
\end{aligned}$$

Since this computation leads to the same character formula when replacing Γ by Γ_σ, we deduce that, for each finite group G,

$$|\operatorname{Hom}(\Gamma, G)| = |\operatorname{Hom}(\Gamma_\sigma, G)|;$$

in particular, $s_n(\Gamma) = s_n(\Gamma_\sigma)$ for all n. Writing

$$|\operatorname{Hom}(\Gamma, G)| = \sum_{U \leq G} |\operatorname{Epi}(\Gamma, U)|$$

and using Möbius inversion in the subgroup lattice of G, this gives

$$|\operatorname{Epi}(\Gamma, G)| = \sum_{U \leq G} \mu(U, G) |\operatorname{Hom}(\Gamma, U)|,$$

thus also

$$|\operatorname{Epi}(\Gamma, G)| = |\operatorname{Epi}(\Gamma_\sigma, G)|. \tag{44}$$

For $n \in \mathbb{N}$, define finite groups G_n and G_n^σ via

$$G_n = \Gamma \Big/ \bigcap_{(\Gamma:\Delta) \leq n} \Delta, \quad G_n^\sigma = \Gamma_\sigma \Big/ \bigcap_{(\Gamma_\sigma:\Delta) \leq n} \Delta.$$

From (44) we know in particular, that G_n is a homomorphic image of Γ_σ. Let N be the kernel of such a projection map $\phi : \Gamma_\sigma \to G_n$. Since $s_\nu(\Gamma_\sigma) = s_\nu(G_n)$ for $\nu \leq n$, we have

$$N \leq \bigcap_{(\Gamma_\sigma:\Delta) \leq n} \Delta,$$

hence, G_n^σ is a homomorphic image of G_n. By symmetry, G_n and G_n^σ are isomorphic. By the universal properties of G_n and G_n^σ,

$$\hat{\Gamma} \cong \lim_{\leftarrow} G_n \cong \lim_{\leftarrow} G_n^\sigma \cong \hat{\Gamma}_\sigma,$$

as claimed. □

Proof of Theorem 6. (i) By [25, Theorem 1], the assumption $s_n(\Gamma) \asymp s_n(\Delta)$ is equivalent to the assertion that

$$(n!)^{-\chi(\Gamma)} \exp\left(\sum_{i=1}^{k} \sum_{d|a_i} \frac{n^{d/a_i}}{d} + \frac{r + \chi(\Gamma) + 1}{2} \log n\right) \asymp$$
$$(n!)^{-\chi(\Delta)} \exp\left(\sum_{i=1}^{l} \sum_{d|b_i} \frac{n^{d/b_i}}{d} + \frac{r' + \chi(\Delta) + 1}{2} \log n\right).$$

Comparing orders of magnitude as in the proof of [25, Theorem 3], we find first that $\chi(\Gamma) = \chi(\Delta)$, then, successively, that

$$\sum_{t|a_i} \frac{t}{a_i} = \sum_{t|b_i} \frac{t}{b_i}, \quad t \geq 2,$$

and, finally, that $r = r'$. Our claim follows now from Lemma 23.

(ii) By Theorem 3,for groups Γ, Δ satisfying $\alpha(\Gamma), \alpha(\Delta) > 0$, the assertion that $\Gamma \sim \Delta$ is equivalent to

$$\delta s_n(C_{a_1} * \cdots * C_{a_r} * F_{s+2t}) \sim \delta' s_n(C_{a'_1} * \cdots * C_{a'_{r'}} * F_{s'+2t'}), \quad (n \to \infty).$$

By part (i), the latter assertion is equivalent to the conjunction of

$$C_{a_1} * \cdots * C_{a_r} * F_{s+2t} \cong C_{a'_1} * \cdots * C_{a'_{r'}} * F_{s'+2t'}$$

and $\delta = \delta'$, whence our claim.

(iii) The equivalence of (a) and (b) follows from Theorem 4 and part (i). Since (c) obviously implies (a), it suffices to show that (b) implies (c); but this follows immediately from Lemma 24 upon setting $l = 0$ and $w_i(\vec{x}_i) = x_i^{e_i}$. □

Denote by $\mathcal{F}$ the class of all groups Γ having a presentation of the form (35) with $\alpha(\Gamma) > 0$, and by $\mathcal{FP}$ the class of all Fuchsian presentations in the sense of (1). We re-interpret $\sim$ as an equivalence relation on $\mathcal{FP}$ in the obvious way, and introduce three refinements of this equivalence relation $\sim$ on $\mathcal{FP}$: (i) the relation $\approx$ of strong equivalence defined via

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

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

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

in the Fuchsian presentation (35), denoted $\Gamma = \Delta$. Of course, $\approx$ and isomorphism are to be interpreted as equivalence relations on $\mathcal{FP}$ in the sense that two such presentations are isomorphic or $\approx$-equivalent if and only if their corresponding groups satisfy the respective relation. Clearly,

$$\Gamma = \Delta \Rightarrow \Gamma \cong \Delta \Rightarrow \Gamma \approx \Delta \Rightarrow \Gamma \sim \Delta. \tag{45}$$

All these implications are in fact strict. To see this, define

$$\Gamma_j = \Big\langle x, y, z, u \,\Big|\, R_j(x, y, z, u) = 1 \Big\rangle, \quad 1 \leq j \leq 3,$$

where

$$R_j := \begin{cases} [x, y][z, u], & j = 1 \\ [x, y]z^2u^2, & j = 2 \\ x^2y^2z^2u^2, & j = 3. \end{cases}$$

Then Γ_1 and Γ_2 are isospectral, that is, $s_n(\Gamma_1) = s_n(\Gamma_2)$ for all n (in particular, $\Gamma_1 \approx \Gamma_2$), but $\Gamma_1 \not\cong \Gamma_2$; and $\Gamma_2 \cong \Gamma_3$ but $\Gamma_2 \neq \Gamma_3$. Our next result implies that $\approx$ is a much finer equivalence relation than $\sim$. It appears that the asymptotic series carries most of the structural information on Fuchsian groups which can be detected via subgroup growth.

Theorem 7. *Each $\approx$-equivalence class of $\mathcal{FP}$ decomposes into finitely many classes with respect to $=$; that is, each group $\Gamma \in \mathcal{F}$ has only finitely many presentations of the form* (35), *and is $\approx$-equivalent to at most finitely many non-isomorphic $\mathcal{F}$-groups.*

Corollary 2. *Let $\Gamma \in \mathcal{F}$ be given by a representation as in* (35) *satisfying $\alpha(\Gamma) > 0$.*

(i) *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) $s = 1$, $t = 0$, $\sum_{i=1}^r \left(1 - \frac{1}{a_i}\right) < 2$,

(c) $s + 2t = 2$, $r = 1$.

(ii) *The set $\{\Delta \in \mathcal{F} : \Delta \sim \Gamma\}/\cong$ is infinite, but $\{\Delta \in \mathcal{F} : s_n(\Delta) = (1 + \mathcal{O}(n^{-2\mu(\Gamma)}))s_n(\Gamma)\}/\cong$ is finite, if and only if the following three conditions hold:*

(a) $s + 2t + \sum_{i=1}^r \left(1 - \frac{1}{a_i}\right) \geq 3$,

(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.*

Proof of Theorem 7. Let $(r, s, t; a_1, a_2 \dots, a_r, e_1, e_2, \dots, e_s)$ be a given set of parameters, let Γ be the corresponding group and assume that $\alpha(\Gamma) > 0$. We have to show that there are only finitely many tuples $(r', s', t'; a'_1, a'_2 \dots, a'_r, e'_1, e'_2, \dots, e'_s)$, such that for the corresponding group Δ we have $\Gamma \approx \Delta$. Before computing the coefficients of the asymptotic series for $s_n(\Gamma)$ and $s_n(\Delta)$, we show that we may assume without loss that $h_\nu(\Gamma) = h_\nu(\Delta)$ for $\nu = 2, 3$. In fact, from Theorem 6 (ii) we infer that $r + s + 2t = r'+s'+2t'$, hence, $|\operatorname{Hom}(\Delta, S_\nu)| \leq (\nu!)^{r+s+2t}$, that is, there are only finitely many choices for $h_\nu(\Delta)$ for each fixed ν. Hence, in the sequel we may assume that $d_\nu(\Gamma) = d_\nu(\Delta)$ for $\nu = 2, 3$, where the d_ν are given as in (39), and that $h_n(\Gamma) = \big(1 + \mathcal{O}(n^{-3\mu(\Gamma)})\big)h_n(\Delta)$. Theorem 6 (ii) already implies that the multi-sets $\{a_i : 1 \leq i \leq r\}$ and $\{a'_i : 1 \leq i \leq r'\}$ coincide. From Propositions 1 and 2 (i), and Equation (36), we see that

$$h_n(\Gamma) = (n!)^{s+2t-2} \prod_{i=1}^{r} |\operatorname{Hom}(C_{a_i}, S_n)| \left\{ \sum_{\substack{\lambda \vdash n \\ \Delta < 3\mu(\Gamma)/\alpha(\Gamma)}} \frac{\prod_{i=1}^{r} \alpha_{\chi_\lambda}^{(a_i)} \prod_{j=1}^{s} m_{\chi_\lambda}^{(e_j)}}{(\chi_\lambda(1))^{r+s+2t-2}} + \mathcal{O}(n^{-3\mu(\Gamma)}) \right\}. \tag{46}$$

In view of Proposition 2 (ii), the contribution of partitions λ with $3 \leq \Delta \leq 3\mu(\Gamma)/\alpha(\Gamma)$ is of lesser order than the error term, hence, we can compute $h_n(\Gamma)$ up to a relative error of order $n^{-3\mu(\Gamma)}$ using only coefficients already computed in the previous sections. Inserting the values for $\alpha_{\chi_\lambda}^{(q)}$ computed in Subsection 5.2, and the multiplicities as given in Proposition 2 (ii) into the right-hand side of (46), we obtain

$$\begin{aligned} h_n(\Gamma) \;=\; & \delta(n!)^{s+2t-2} \prod_{i=1}^{r} |\operatorname{Hom}(C_{a_i}, S_n)| \Bigg\{ 1 + (n-1)^{-(r+s+2t-2)} \prod_{i=1}^{r} H_{1,a_i}(n) \prod_{j=1}^{s} \big(\tau(e_j) - 1\big) \\ & + \left(\frac{n^2 - 3n + 2}{2}\right)^{-(r+s+2t)} \prod_{\substack{1 \leq i \leq r \\ 2 \mid a_i}} \frac{n}{n-1} H_{2,a_i}(n) \prod_{\substack{1 \leq i \leq r \\ 2 \nmid a_i}} (H_{2,a_i}(n) - 1) \\ & \quad \times \prod_{j=1}^{s} \frac{1}{2} \big(\sigma(e_j) + (\tau(e_j))^2 - 3\tau(e_j) + \tau_{\text{odd}}(e_j)\big) \\ & + \left(\frac{n^2 - 3n}{2}\right)^{-(r+s+2t)} \prod_{\substack{1 \leq i \leq r \\ 2 \mid a_i}} \left(\frac{n}{n-1} H_{2,a_i}(n) + 1\right) \prod_{\substack{1 \leq i \leq r \\ 2 \nmid a_i}} H_{2,a_i}(n) \\ & \quad \times \prod_{j=1}^{s} \frac{1}{2} \big(\sigma(e_j) + (\tau(e_j))^2 - 3\tau(e_j) - \tau_{\text{odd}}(e_j) + 2\big) \;+\; \mathcal{O}(n^{-3\mu(\Gamma)}) \Bigg\}, \end{aligned} \tag{47}$$

where

$$H_{i,q}(n) := \binom{n}{i} \frac{|\operatorname{Hom}(C_q, S_{n-i})|}{|\operatorname{Hom}(C_q, S_n)|}.$$

From [24, Theorem 6], we see that

$$(n-1)^{-(r+s+2t-2)}\prod_{i=1}^{r} H_{1,a_i}(n) \asymp n^{-\mu(\Gamma)},$$

and all other contributions to the asymptotic series in (47) are of lesser order, hence, expanding $h_n(\Delta)$ in the same way, we find that $\Gamma \approx \Delta$ implies

$$\prod_{j=1}^{s}\big(\tau(e_j)-1\big) = \prod_{j=1}^{s'}\big(\tau(e'_j)-1\big). \tag{48}$$

Moreover, the contribution of the character $\chi_{(n-1,1)}$ to $h_n(\Gamma)$ and $h_n(\Delta)$ are identical. Next we consider terms of order $n^{-2\mu(\Gamma)}$. Arguing as for terms of order $n^{-\mu(\Gamma)}$, we find that $h_n(\Gamma) = (1+o(n^{-2\mu(\Gamma)}))h_n(\Delta)$ is equivalent to (48) and

$$\begin{aligned}
&\prod_{j=1}^{s}\Big(\sigma(e_j)+(\tau(e_j))^2-3\tau(e_j)+\tau_{\text{odd}}(e_j)\Big)\\
&\qquad+\prod_{j=1}^{s}\Big(\sigma(e_j)+(\tau(e_j))^2-3\tau(e_j)-\tau_{\text{odd}}(e_j)+2\Big)\\
=\;&\prod_{j=1}^{s'}\Big(\sigma(e'_j)+(\tau(e'_j))^2-3\tau(e'_j)+\tau_{\text{odd}}(e'_j)\Big)\\
&\qquad+\prod_{j=1}^{s'}\Big(\sigma(e'_j)+(\tau(e'_j))^2-3\tau(e'_j)-\tau_{\text{odd}}(e'_j)+2\Big).
\end{aligned} \tag{49}$$

For a fixed tuple $(e_1,\dots,e_s)$, there are only finitely many tuples $(e'_1,\dots,e'_{s'})$ with $s' \leq s+2t$, solving (49). Indeed, the left-hand side is bounded by some constant, whereas the right-hand side is bounded below by its greatest factor, as all factors occurring in the last equation are ≥ 1; thus e'_j is bounded for all j. □

Proof of Corollary 2. (i) Using Theorem 3, one checks in each of these cases that $\{\Delta : \Delta \sim \Gamma\}$ is indeed finite. On the other hand, if none of the conditions (a)–(c) is satisfied, one easily computes that the groups

$$\Delta_e := \Big\langle x_1,\dots,x_r,y_1,\dots,y_{s+2t}\,\Big|\, x_1^{a_1}=\cdots=x_r^{a_r}=x_1\cdots x_r y_1^e y_2^2\cdots y_s^2 = 1\Big\rangle$$

satisfy $\alpha(\Delta_e) \geq \frac{2}{e}$, and, if necessary, adjusting the parity of e, we have $\Delta_e \sim \Gamma$ for infinitely many e. By Theorem 7, there is an infinite sequence $(e_\nu)_{\nu\geq 1}$, such that $\Delta_{e_\nu} \sim \Gamma$, while $\Delta_{e_\nu} \not\approx \Delta_{e_\mu}$ for $\nu \neq \mu$, which implies our claim.

(ii) In the proof of Theorem 7, we have seen that $s_n(\Delta) = (1+\mathcal{O}(n^{-2\mu(\Gamma)}))s_n(\Gamma)$ is equivalent to the conjunction of $\Delta \sim \Gamma$ and

$$\prod_{j=1}^{s}(\tau(e_j)-1) = \prod_{j=1}^{s'}(\tau(e'_j)-1).$$

From this equation and part (i) it is easy to see that for a group Γ satisfying (a)–(c) the described sets are of the claimed cardinality. Now assume that Γ is a group such that

$\{\Delta \in \mathcal{F} : \Delta \sim \Gamma\}$ is infinite, while $\{\Delta \in \mathcal{F} : s_n(\Delta) = (1 + \mathcal{O}(n^{-2\mu(\Gamma)}))s_n(\Gamma)\}$ is finite. If $\delta(\Gamma) = 1$, and $\{\Delta : \Delta \sim \Gamma\}$ is infinite, there are infinitely many integers e', such that $(e', 2, 2, \dots, 2)$ solves this equation, and $\delta(\Delta_{e'}) = \delta(\Gamma)$. Define the integer $q = q(\Gamma)$ via

$$q := \left(\prod_{j=1}^{s} \big(\tau(e_j) - 1\big)\right) + 1.$$

If q is not 1 or prime, say $q = a \cdot b$ with $a, b \geq 2$, then $s_n(\Delta_{2^a p^b}) = (1 + \mathcal{O}(n^{-2\mu(\Gamma)}))s_n(\Gamma)$ for all odd primes p, and, by Theorem 7, there are infinitely many non-isomorphic groups among the groups Δ defined in this way. Hence, we may assume that all e_j are even, $\tau(e_j) = 2$ for all j with at most one exception, and for the exceptional index j_0, we have that $\tau(e_{j_0})$ is either 2 or $p + 1$ for some prime p. This implies our claim. □

References

[1] G. E. Andrews, *The Theory of Partitions*, Cambridge University Press, New York, 1998.

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

[3] C. Curtis and I. Reiner, *Methods of Representation theory*, Wiley Interscience, New York, 1981.

[4] S. P. Demuškin, The group of the maximum p-extension of a local field, *Dokl. Akad. Nauk S.S.S.R.* **128** (1959), 657–660.

[5] S. P. Demuškin, On 2-extensions of a local field, *Math. Sibirisk.* **4** (1963), 951–955.

[6] S. P. Demuškin, Topological 2-groups with an even number of generators and a complete defining relation, *Izv. Akad. Nauk S.S.S.R.* **29** (1965), 3–10.

[7] P. Diaconis, *Group Representations in Probability and Statistics*, IMS Lecture Notes Vol. 11, Hayward, California, 1988.

[8] P. Diaconis, M. Shahshahani, Generating a random permutation with random transpositions, *Z. Wahrscheinlichkeitstheorie u. Verw. Gebiete* **57** (1981), 159–179.

[9] A. Dress and T. Müller, Decomposable functors and the exponential principle, *Adv. in Math.* **129** (1997), 188–221.

[10] P. D. T. A. Elliott, *Probabilistic number theory II. Central limit theorems.* Grundlehren der Mathematischen Wissenschaften 240, Springer-Verlag, Berlin-New York, 1980.

[11] S. V. Fomin and N. Lulov, On the number of Rim Hook Tableaux, *J. Math. Sciences* **87** (1997), 4118–4123

[12] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews, 2002, `http://www-gap.dcs.st-and.ac.uk/~gap`.

[13] F. Grunewald, D. Segal, and G. Smith, Subgroups of finite index in nilpotent groups, *invent. math.* **93**, 185–223.

[14] W. Hayman, A generalisation of Stirling's formula, *J. Reine Angew. Math.* **196** (1956), 67–95.

[15] G. James, A. Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its Applications, 16. Addison-Wesley Publishing Co., Reading, Mass., 1981.

[16] H. J. Kanold, Einige neuere Abschätzungen bei Stirlingschen Zahlen 2. Art, *J. Reine Angew. Math.* **238** (1969), 148–160.

[17] A. Kerber, *Algebraic combinatorics via finite group actions*, BI–Wiss.–Verl., Mannheim, 1991.

[18] E. Krätzel, *Zahlentheorie* VEB Deutscher Verlag der Wissenschaften, Berlin 1981.

[19] J. P. Labute, Classification of Demuškin groups, *Canad. J. Math.* **19** (1967), 106–132.

[20] R. C. Lyndon, P. E. Schupp, *Combinatorial Group Theory*, Springer, Berlin Heidelberg New York, 1977.

[21] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, second edition, Oxford University Press, Oxford, 1995.

[22] W. Magnus, *Noneuclidean Tesselations and Their Groups*, Academic Press, New York 1974.

[23] T. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Society* **44**, 75–94.

[24] T. Müller, Finite group actions and asymptotic expansion of $e^{P(z)}$, *Combinatorica* **17** (1997), 523–554.

[25] T. Müller, Subgroup growth of free products, *invent. math.* **126** (1996) 111–131.

[26] T. Müller, Enumerating representations in finite wreath products, *Adv. in Math.* **153** (2000), 118–154.

[27] T. Müller and J.-C. Puchta, Character theory of symmetric groups and subgroup growth of surface groups, *J. London Math. Soc.* (2) **66** (2002), 623–640.

[28] T. W. Müller and J.-C. Puchta, Some examples in the theory of subgroup growth, *Math. Monatshefte* **146** (2005), 49–76.

[29] Y. Roichman, Upper bound on the characters of the symmetric groups, *Invent. math.* **125** (1996), 451–485.

[30] T. Scharf, Die Wurzelanzahlfunktion in symmetrischen Gruppen, *J. Algebra* **139** (1991), 446–457.

[31] A. Terras, *Fourier analysis on finite groups and applications*, LMS Student Texts, 43. Cambridge University Press, Cambridge, 1999.

[32] E. M. Wright, A relationship between two sequences, *Proc. London Math. Soc.* **17** (1967), 296–304.

Thomas W. Müller, School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, E1 4NS London, UK (T.W.Muller@qmul.ac.uk)

Jan-Christoph Schlage-Puchta, Mathematisches Institut, Albert-Ludwigs-Universität, Eckerstr. 1, 79104 Freiburg, Germany (jcp@math.uni-freiburg.de)