Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ
England

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel

Abstract

Fuchsian groups (acting as isometries of the hyperbolic plane) occur naturally in geometry, combinatorial group theory, and other contexts. We use character-theoretic and probabilistic methods to study the spaces of homomorphisms from Fuchsian groups to symmetric groups. We obtain a wide variety of applications, ranging from counting branched coverings of Riemann surfaces, to subgroup growth and random finite quotients of Fuchsian groups, as well as random walks on symmetric groups.

In particular we show that, in some sense, almost all homomorphisms from a Fuchsian group to alternating groups A_n are surjective, and this implies Higman's conjecture that every Fuchsian group surjects onto all large enough alternating groups. As a very special case we obtain a random Hurwitz generation of A_n, namely random generation by two elements of orders 2 and 3 whose product has order 7. We also establish the analogue of Higman's conjecture for symmetric groups. We apply these results to branched coverings of Riemann surfaces, showing that under some assumptions on the ramification types, their monodromy group is almost always S_n or A_n.

Another application concerns subgroup growth. We show that a Fuchsian group Γ has $(n!)^{\mu+o(1)}$ index n subgroups, where μ is the measure of Γ, and derive similar estimates for so-called Eisenstein numbers of coverings of Riemann surfaces.

A final application concerns random walks on alternating and symmetric groups. We give necessary and sufficient conditions for a collection of 'almost homogeneous' conjugacy classes in A_n to have product equal to A_n almost uniformly pointwise.

Our methods involve some new asymptotic results for degrees and values of irreducible characters of symmetric groups.

Contents

1 Introduction

A *Fuchsian group* is a finitely generated non-elementary discrete group of isometries of the hyperbolic plane $\mathbb{H}^2$. By classical work of Fricke and Klein, the orientation-preserving such groups Γ have a presentation of the following form:

$$(1.1)\quad \text{generators:}\quad \begin{array}{ll} a_1, b_1, \ldots, a_g, b_g & \text{(hyperbolic)} \\ x_1, \ldots, x_d & \text{(elliptic)} \\ y_1, \ldots, y_s & \text{(parabolic)} \\ z_1, \ldots, z_t & \text{(hyperbolic boundary elements)} \end{array}$$

$$\text{relations:}\quad \begin{array}{l} x_1^{m_1} = \cdots = x_d^{m_d} = 1, \\ x_1 \cdots x_d \, y_1 \cdots y_s \, z_1 \cdots z_t \, [a_1, b_1] \cdots [a_g, b_g] = 1, \end{array}$$

where $g, d, s, t \geq 0$ and $m_i \geq 2$ for all i. The number g is referred to as the *genus* of Γ. The *measure* $\mu(\Gamma)$ of an orientation-preserving Fuchsian group Γ is defined by

$$\mu(\Gamma) = 2g - 2 + \sum_{i=1}^{d}(1 - \frac{1}{m_i}) + s + t.$$

It is well known that $\mu(\Gamma) > 0$. The groups with presentations as above, but having $\mu(\Gamma) = 0$ or $\mu(\Gamma) < 0$, are the so-called Euclidean and spherical groups, respectively.

The second author thanks EPSRC for its support and Imperial College for its hospitality while this work was carried out

We shall also study non-orientation-preserving Fuchsian groups; these have presentations as follows, with $g > 0$:

$$\text{(1.2)} \quad \begin{array}{ll} \text{generators:} & a_1, \ldots, a_g \\ & x_1, \ldots, x_d \\ & y_1, \ldots, y_s \\ & z_1, \ldots, z_t \\ & \\ \text{relations:} & x_1^{m_1} = \cdots = x_d^{m_d} = 1, \\ & x_1 \cdots x_d\, y_1 \cdots y_s\, z_1 \cdots z_t\, a_1^2 \cdots a_g^2 = 1. \end{array}$$

In this case the measure $\mu(\Gamma)$ is defined by

$$\mu(\Gamma) = g - 2 + \sum_{i=1}^{d} (1 - \frac{1}{m_i}) + s + t,$$

and again, $\mu(\Gamma) > 0$.

We call Fuchsian groups as in (1.1) *oriented*, and those as in (1.2) *non-oriented*. Note that $\mu(\Gamma)$ coincides with $-\chi(\Gamma)$, where $\chi(\Gamma)$ is the Euler characteristic of Γ.

If $s + t > 0$ then Γ is a free product of cyclic groups. In particular, non-abelian free groups are Fuchsian, as well as free products of finite cyclic groups, such as the modular group. Other examples are surface groups (where $d = s = t = 0$), and triangle groups

$$\Delta(m_1, m_2, m_3) = \langle x_1, x_2, x_3 \mid x_1^{m_1} = x_2^{m_2} = x_3^{m_3} = x_1 x_2 x_3 = 1 \rangle,$$

(where $g = s = t = 0$, $d = 3$ and $\sum \frac{1}{m_i} < 1$). Among triangle groups, the Hurwitz group $\Delta(2, 3, 7)$ has received particular attention, one reason being that its finite images are precisely those finite groups which occur as the automorphism group of a Riemann surface of genus $h \geq 2$ and have order achieving the Hurwitz bound $84(h - 1)$ (see [7, 21]).

We call Fuchsian groups with $s = t = 0$ *proper* (also termed *F-groups* in [33, iii.5]). Our main focus is on proper Fuchsian groups, since the improper ones are easier to handle, and some of our results are either known or easily derived for them.

In this paper we study the space of homomorphisms $\text{Hom}(\Gamma, S_n)$ from a Fuchsian group Γ to a symmetric group. The study of this space and various subspaces has a wide variety of applications, ranging from coverings of Riemann surfaces to subgroup growth and random finite quotients of Fuchsian groups, as well as random walks on symmetric groups. Two major by-products are estimates for Eisenstein numbers of coverings of Riemann surfaces in the hyperbolic case (Theorem 1.3), and a probabilistic proof of the well-known conjecture of Graham Higman that any Fuchsian group surjects onto all but finitely many alternating groups (Corollary 1.8). This conjecture has recently been proved by Everitt [16] for oriented Fuchsian groups using completely different methods. Our approach handles general Fuchsian groups, and we also prove an analogue of Higman's conjecture for symmetric quotients, determining precisely which Fuchsian groups surject to all but finitely many symmetric groups (Theorem 1.10). These results have applications to monodromy groups of branched coverings of Riemann surfaces (Theorem 1.13).

A major tool in our proofs is the character theory of symmetric groups, and we establish a number of new asymptotic results relating to degrees and values of such characters. For example, denoting by $Irr(S_n)$ the set of all irreducible characters of S_n, we prove

Theorem 1.1 *Fix a real number $s > 0$. Then*

$$\sum_{\chi \in Irr(S_n)} \chi(1)^{-s} \to 2 \textit{ as } n \to \infty.$$

Moreover, $\sum_{\chi \in Irr(S_n)} \chi(1)^{-s} = 2 + O(n^{-s})$.

For integers $s \geq 1$ this was originally proved by Lulov in his unpublished thesis [32]; this was reproved in [37], where more detailed estimates are obtained. The proof of Theorem 1.1 is fairly elementary, but it is important for many of our results, and we sometimes need it for rather small values of s, for example $s = \frac{1}{42}$. We also prove a version for alternating groups (see Corollary 2.7).

We now state our main results. The first deals with the number of homomorphisms from a Fuchsian group to a symmetric group, and forms the basis for the other results. In the statements below, $o(1)$ denotes a quantity which tends to 0 as $n \to \infty$.

Theorem 1.2 *For any Fuchsian group Γ, we have*

$$|\mathrm{Hom}(\Gamma, S_n)| = (n!)^{\mu(\Gamma)+1+o(1)}.$$

In fact our estimates for $|\mathrm{Hom}(\Gamma, S_n)|$ are more precise - see Theorem 1.12, Corollary 3.6 and Theorem 3.7 below. We also obtain similar results for $|\mathrm{Hom}(\Gamma, A_n)|$, which are important for some of the main applications.

A classical motivation behind the study of $|\mathrm{Hom}(\Gamma, S_n)|$ stems from the theory of branched coverings of Riemann surfaces. Let Y be a compact connected Riemann surface of genus g, and let $y_1, \ldots, y_d \in Y$ be fixed distinct points. Consider index n coverings $\pi : X \to Y$, unramified outside $\{y_1, \ldots, y_d\}$, and with monodromy elements $g_1, \ldots, g_d \in S_n$ around

$y_1, \dots, y_d$ respectively. As is standard, we identify geometrically equivalent coverings.

For conjugacy classes $C_1, \dots, C_d$ of S_n, and integers $m_1, \dots, m_d \geq 2$, set $\mathbf{C} = (C_1, \dots, C_d)$, $\mathbf{m} = (m_1, \dots, m_d)$ and define

$$P(\mathbf{C}, n) = \{\pi : X \to Y \ : \ g_i \in C_i \text{ for all } i\},$$

$$P(\mathbf{m}, n) = \{\pi : X \to Y \ : \ g_i^{m_i} = 1 \text{ for all } i\}.$$

Attempts to count such coverings go back to Hurwitz [22]. Define $\mathrm{Aut}\,\pi$ to be the centralizer in S_n of the monodromy group of π. Following [26] we call the sums $\sum 1/|\mathrm{Aut}\,\pi|$ over such sets of coverings $P(\mathbf{C}, n)$ the *Eisenstein numbers* of coverings, a term which the authors attribute to Serre. When all but one of the classes C_i consists of transpositions these numbers are called *Hurwitz numbers*, which have been the subject of recent intensive study in view of connections with geometry and physics - see for instance [46] and the references therein. See also [13], where asymptotic results are proved in the case where the C_i consist of cycles of bounded length, and used to study volumes of certain moduli spaces.

Eisenstein numbers are related to homomorphisms of Fuchsian groups in the following way. Let $C_i = g_i^{S_n}$ $(1 \leq i \leq d)$ be classes in S_n, and let m_i be the order of g_i. Define $\mathrm{sgn}(C_i) = \mathrm{sgn}(g_i)$, and write $\mathbf{C} = (C_1, \dots, C_d)$. For a group Γ having presentation as in (1.1) or (1.2), define

$$\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n) = \{\phi \in \mathrm{Hom}(\Gamma, S_n) \ : \ \phi(x_i) \in C_i \text{ for } 1 \leq i \leq d\}.$$

Note that if Γ is proper, and $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n) \neq \emptyset$, then $\prod_{i=1}^d \mathrm{sgn}(C_i) = 1$. When Γ is a proper oriented Fuchsian group (as in (1.1) with $s = t = 0$), a covering in $P(\mathbf{C}, n)$ corresponds to an S_n-class of homomorphisms in $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ (see Section 8 for details). If $\pi \in P(\mathbf{C}, n)$ corresponds to the class ϕ^{S_n} (where $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$), then $|\mathrm{Aut}\,\pi| = |C_{S_n}(\phi(\Gamma))|$.

The following formula, which essentially dates back to Hurwitz, connects Eisenstein numbers and $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|$ with characters of symmetric groups (see Proposition 3.2 and Section 8):

$$\sum_{\pi \in P(\mathbf{C}, n)} \frac{1}{|\mathrm{Aut}\,\pi|} = \frac{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|}{n!} = \frac{|C_1| \dots |C_d|}{(n!)^{2-2g}} \sum_{\chi \in Irr(S_n)} \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+2g}}. \tag{1.3}$$

This formula includes the case where $d = 0$; here Γ is a surface group, the coverings are unramified, $\mathrm{Hom}_{\mathbf{C}} = \mathrm{Hom}$, and empty products are taken to be 1. While the formula (1.3) has been around for a century or so, it has not been used extensively, partly due to the difficulty in dealing with the character-theoretic sum on the right hand side; rather, geometric and combinatorial methods have often been applied (see for instance [26, 46, 42]). See also [25] for a survey of some related material.

In this paper we are able to use character theory to estimate the sum in (1.3) for certain types of conjugacy classes C_i described below. This leads to estimates for Eisenstein numbers, as well as being a key ingredient for many of the other theorems in the paper. A key tool in our character-theoretic approach is a result of Fomin and Lulov [17] which bounds the values of irreducible characters of S_n on classes of cycle-shape (m^a), where $n = ma$. We call such classes *homogeneous*.

There is special interest in the case where the classes C_i are all homogeneous. Indeed, the Eisenstein numbers corresponding to such classes are studied in [26], mainly in the case where Γ is Euclidean or spherical, and formulae are obtained in [26, Section 3] using geometric methods. As stated in [26, p.414], the most interesting case is the hyperbolic one, in which the group Γ is Fuchsian. For this case, even allowing the permutations in C_i to have boundedly many fixed points, we prove the following result.

Theorem 1.3 *Fix integers $g \geq 0$ and $m_1, \ldots, m_d \geq 2$. Let $\mu = 2g - 2 + \sum_{i=1}^{d}(1 - \frac{1}{m_i})$ and suppose $\mu > 0$.*

(i) *For $1 \leq i \leq d$ let C_i be a conjugacy class in S_n having cycle-shape $(m_i^{a_i}, 1^{f_i})$, and assume $\prod_{i=1}^{d} \operatorname{sgn}(C_i) = 1$. Then for f_i bounded and $n \to \infty$, we have*

$$\begin{aligned} \textstyle\sum_{\pi \in P(\mathbf{C},n)} \frac{1}{|\mathrm{Aut}\,\pi|} &= (2 + O(n^{-\mu}))|C_1| \cdots |C_d| \cdot (n!)^{2g-2} \\ &\sim (n!)^{\mu} \cdot n^{\sum \frac{f_i}{m_i} - \frac{1}{2}(1 - \frac{1}{m_i})}. \end{aligned}$$

(ii) $\sum_{\pi \in P(\mathbf{m},n)} \frac{1}{|\mathrm{Aut}\,\pi|} = (n!)^{\mu + o(1)}$.

Here, and throughout the paper, for functions f_1, f_2, we write $f_1 \sim f_2$ if there are positive constants c_1, c_2 such that $c_1 f_2 \leq f_1 \leq c_2 f_2$. We call classes C_i as in (i) with f_i bounded *almost homogeneous* classes of S_n. We can show that most coverings in $P(\mathbf{C}, n)$ are connected (see Proposition 8.1), and so the estimates in 1.3 also hold for the numbers of connected coverings.

A different motivation behind the study of homomorphisms from Fuchsian groups to symmetric groups stems from the fast-growing theory of subgroup growth. For a finitely generated group Γ and a positive integer n, denote by $a_n(\Gamma)$ the number of index n subgroups of Γ. The relation between the function $a_n(\Gamma)$ and the structure of Γ has been the subject of intensive study over the past two decades (see the monograph [31]). The subgroup growth of the free group F_r of rank r was determined by M. Hall and M. Newman [19, 40]; extensions to the modular group as well as arbitrary free products of cyclic groups were subsequently given in [8, 40]. Recently Müller and Puchta [37], following the character-theoretic approach of Mednykh [34], determined the subgroup growth of surface groups. It follows from these results that $a_n(F_r) = (n!)^{r-1+o(1)}$, that $a_n(PSL_2(\mathbb{Z})) = (n!)^{\frac{1}{6}+o(1)}$, and for an oriented surface group Γ_g of genus $g \geq 2$, that $a_n(\Gamma_g) = (n!)^{2g-2+o(1)}$. We show that these results are particular cases of a general phenomenon:

Theorem 1.4 *For any Fuchsian group* Γ,

$$a_n(\Gamma) = (n!)^{\mu(\Gamma)+o(1)}.$$

This implies, for example, that the Hurwitz group $\Delta(2,3,7)$ has subgroup growth $(n!)^{\frac{1}{42}+o(1)}$. In fact this is the minimal subgroup growth of a Fuchsian group, since $\frac{1}{42}$ is easily seen to be the smallest possible value of $\mu(\Gamma)$. Note that Theorem 1.4 amounts to saying that

$$\frac{\log a_n(\Gamma)}{\log n!} \to \mu(\Gamma) = -\chi(\Gamma) \text{ as } n \to \infty.$$

Again, our results are more precise than stated in the theorem - see Theorems 1.12 and 4.6 below.

To explain the relation between $a_n(\Gamma)$ and homomorphisms of Γ, define

$$\mathrm{Hom}_{trans}(\Gamma, S_n) = \{\phi \in \mathrm{Hom}(\Gamma, S_n) : \phi(\Gamma) \text{ is transitive}\}.$$

It is well known that $a_n(\Gamma) = |\mathrm{Hom}_{trans}(\Gamma, S_n)|/(n-1)!$. Thus Theorem 1.2 immediately yields an upper bound for $a_n(\Gamma)$. To obtain a lower bound, we show that for almost homogeneous classes $C_1, \ldots, C_d$, almost all homomorphisms in $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ lie in $\mathrm{Hom}_{trans}(\Gamma, S_n)$ (see Theorem 4.4). Using the character formula (1.3) for $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|$ and our character-theoretic results in Section 2, we then complete the proof of Theorem 1.4.

For further applications it is important for us to estimate how many of the homomorphisms in $\mathrm{Hom}_{trans}(\Gamma, S_n)$ have primitive images in S_n. To do this we study the maximal subgroup growth of Fuchsian groups. Denote by $m_n(\Gamma)$ the number of maximal subgroups of index n in Γ. It turns out that most finite index subgroups of Fuchsian groups are maximal:

Theorem 1.5 *For any Fuchsian group* Γ, *we have*

$$\frac{m_n(\Gamma)}{a_n(\Gamma)} \to 1 \text{ as } n \to \infty.$$

Moreover, $\frac{m_n(\Gamma)}{a_n(\Gamma)} = 1 - O(c^{-n})$, *where* $c > 1$ *is a constant depending on* Γ.

This extends previously known results for free groups (see [12, Lemma 2]) and surface groups [37].

Theorem 1.5 amounts to saying that almost all transitive homomorphisms from a Fuchsian group to S_n have primitive images. The next theorem is the culmination of our results on homomorphisms from Fuchsian groups to symmetric groups, and shows that almost all of these homomorphisms have image containing A_n. In the statement, by H_Γ we mean the core of H, namely the largest normal subgroup of Γ contained in H.

Theorem 1.6 *Let Γ be a Fuchsian group, and let H be a randomly chosen index n subgroup of Γ. Then the probability that $\Gamma/H_\Gamma \cong A_n$ or S_n tends to 1 as $n \to \infty$; moreover, this probability is $1 - O(c^{-n})$ for some constant $c > 1$ depending on Γ. Equivalently, a random homomorphism $\phi \in \mathrm{Hom}_{trans}(\Gamma, S_n)$ satisfies $\phi(\Gamma) \supseteq A_n$ with probability $1 - O(c^{-n})$.*

The methods of proof of Theorem 1.6 also establish the following useful variant, dealing with maps to alternating groups.

Theorem 1.7 *Let Γ be a Fuchsian group. Then the probability that a random homomorphism in $\mathrm{Hom}_{trans}(\Gamma, A_n)$ is an epimorphism tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O(c^{-n})$ for some constant $c > 1$ depending on Γ.*

Our proofs show that in Theorems 1.5, 1.6 and 1.7, any constant c satisfying $1 < c < 2^{\mu(\Gamma)}$ will do.

Theorem 1.7 obviously implies the following.

Corollary 1.8 *Every Fuchsian group surjects to all but finitely many alternating groups. In other words, Higman's conjecture holds for all Fuchsian groups (including the non-oriented ones).*

Higman formulated his conjecture in the 1960s. Perhaps the first evidence in this direction was the result of Miller [35] that apart from A_6, A_7 and A_8, every alternating group A_n can be generated by two elements of orders 2 and 3, and hence is a quotient of the modular group. A much more telling contribution was that of Higman and Conder concerning *Hurwitz generation* of A_n - namely, generation by elements x, y satisfying $x^2 = y^3 = (xy)^7 = 1$. Using the method of coset diagrams, Higman (in unpublished work) proved that every sufficiently large alternating group can be generated in this way - in other words, is an image of the Hurwitz triangle group $\Delta(2,3,7)$. Conder [5] was able to find the precise values of n for which A_n is a quotient of $\Delta(2,3,7)$, and later in [6] showed that if $k \geq 7$ then every sufficiently large alternating group is a quotient of $\Delta(2,3,k)$. Further triangle groups were handled in [38, 39, 14, 15], and the full conjecture for oriented Fuchsian groups was finally proved by Everitt in [16].

The papers mentioned above all use extensions of the original Higman-Conder method of coset diagrams. Our approach to Higman's conjecture is completely different, and gives a uniform treatment of all Fuchsian groups. In particular we also establish the conjecture for non-oriented groups.

We also prove a more explicit result on random quotients of Fuchsian groups, dealing with homomorphisms sending the generators to elements in given almost homogeneous classes.

Theorem 1.9 *Let Γ be a Fuchsian group as in* (1.1) *or* (1.2)*, and let C_i $(1 \leq i \leq d)$ be conjugacy classes in S_n with cycle-shapes $(m_i^{a_i}, 1^{f_i})$, where f_i are bounded and $\prod_{i=1}^{d} \mathrm{sgn}(C_i) = 1$. Set $\mathbf{C} = (C_1, \ldots, C_d)$. Then the probability that a random homomorphism in $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ has image containing A_n tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O(n^{-\mu(\Gamma)})$.*

For example, applying this when Γ is the triangle group $\Delta(m_1, m_2, m_3)$ demonstrates that three elements, with product 1, from almost homogeneous classes C_1, C_2, C_3 of orders m_1, m_2, m_3, randomly generate A_n or S_n provided $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} < 1$. In particular, when $(m_1, m_2, m_3) = (2, 3, 7)$, this gives random Hurwitz generation of A_n.

Theorem 1.9 is instrumental in establishing the analogue of Higman's conjecture for symmetric quotients. Let Γ be as in (1.1) or (1.2), and define

$$d^* = |\{i : m_i \text{ even}\}|.$$

Note that if $s + t = g = 0$ and $d^* \leq 1$, or if $s + t = 1$ and $g = d^* = 0$, then Γ is generated by elements of odd order, so cannot have a symmetric group as a quotient. It turns out that these conditions form the only obstruction to Γ having symmetric quotients:

Theorem 1.10 *Let Γ be a Fuchsian group. If $s + t = 0$, assume $(g, d^*) \neq (0, 0), (0, 1)$; and if $s + t = 1$, assume $(g, d^*) \neq (0, 0)$. Then Γ surjects to all but finitely many symmetric groups. Equivalently, if a Fuchsian group has S_2 as a quotient, then it has S_n as a quotient for all sufficiently large n.*

Our proof of this result is probabilistic; to cover all possibilities for Γ we need to consider suitably chosen subspaces of $\mathrm{Hom}(\Gamma, S_n)$ as probability spaces (see Section 7 and Theorem 1.12(vi) below).

Theorem 1.10 is new even for triangle groups, where it takes the following form.

Corollary 1.11 *Let $m_1, m_2, m_3 \geq 2$ be integers such that $\sum \frac{1}{m_i} < 1$, and suppose at least two of the m_i are even. Then the triangle group $\Delta(m_1, m_2, m_3)$ surjects to all but finitely many symmetric groups.*

The special case of this where $(m_1, m_2, m_3) = (2, 3, k)$ with k even was established by Conder in [6].

The above results provide yet another demonstration of the power of probabilistic methods in group theory; see [44] for background.

When the genus g of the Fuchsian group Γ is at least 2 (at least 3 in the non-oriented case), we obtain below stronger versions of most of the above results, improving the asymptotics and replacing $\mathrm{Hom}_{trans}(\Gamma, S_n)$ and $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ by $\mathrm{Hom}(\Gamma, S_n)$.

To state this, we need some notation. For positive integers n, m define

$$E(n,m) = n^{-\frac{1}{2}(1-\frac{1}{m})} \cdot \exp(\sum_{a|m, a<m} \frac{n^{a/m}}{a}).$$

We also define $v = v(\Gamma)$ to be 2 if Γ is as in (1.1), and 1 if Γ is as in (1.2).

Theorem 1.12 *Let Γ be a Fuchsian group of genus g with presentation as in* (1.1) *or* (1.2) *above, and let $\mu = \mu(\Gamma)$. If $s + t = 0$, suppose that $g \geq 2$, and $g \geq 3$ in the non-oriented case. Then*

(i) $|\mathrm{Hom}(\Gamma, S_n)| \sim |\mathrm{Hom}(\Gamma, A_n)| \sim (n!)^{\mu+1} \cdot \prod_{i=1}^{d} E(n, m_i)$.

(ii) $\sum_{\pi \in P(\mathbf{m},n)} \frac{1}{|\mathrm{Aut}\pi|} \sim (n!)^{\mu} \cdot \prod_{i=1}^{d} E(n, m_i)$.

(iii) $a_n(\Gamma) \sim (n!)^{\mu} \cdot n \cdot \prod_{i=1}^{d} E(n, m_i)$.

(iv) *The probability that a random homomorphism $\phi \in \mathrm{Hom}(\Gamma, S_n)$ satisfies $\phi(\Gamma) \supseteq A_n$ tends to 1 as $n \to \infty$. This probability is $1 - O(n^{-\mu})$.*

(v) *The probability that a random homomorphism $\phi \in \mathrm{Hom}(\Gamma, A_n)$ is an epimorphism tends to 1 as $n \to \infty$. This probability is $1 - O(n^{-\mu})$.*

(vi) *The probability that a random homomorphism $\phi \in \mathrm{Hom}(\Gamma, S_n)$ satisfies $\phi(\Gamma) = S_n$ is equal to $1 - 2^{1-vg-d^*-s-t} + O(n^{-(vg-2)})$ if $d^* + s + t > 0$, and is equal to $1 - 2^{-vg} + O(n^{-(vg-2)})$ if $d^* + s + t = 0$.*

In parts (i), (ii) and (iii), the implied multiplicative constants can easily be found using our methods (see for example Theorem 3.8).

When $s + t > 0$, Γ is a free product of cyclic groups and some parts of this result are essentially known. Details will be given in the relevant sections.

In a subsequent paper [30] we extend various parts of Theorem 1.12 to all finite simple groups. More specifically, assuming that Γ is Fuchsian of genus $g \geq 2$ ($g \geq 3$ if Γ is non-oriented), we give precise estimates for $|\mathrm{Hom}(\Gamma, G)|$ where G is a finite simple group of Lie type, and prove that a random homomorphism in $\mathrm{Hom}(\Gamma, G)$ is surjective. We also apply these results to the study of representation varieties $\mathrm{Hom}(\Gamma, \bar{G})$, where $\bar{G}$ is $GL_n(K)$ or a simple algebraic group over K, an algebraically closed field of arbitrary characteristic.

Our results on random quotients of Fuchsian groups have implications for the monodromy groups of branched coverings of Riemann surfaces, under suitable assumptions on the ramification types around the branch points. Any finite set of index n coverings can be naturally viewed as a probability space, where the probability assigned to a covering π is proportional to $1/|\mathrm{Aut}\, \pi|$.

We adopt the notation of the preamble to Theorem 1.3.

Theorem 1.13 *Fix integers $g \geq 0$ and $m_1, \ldots, m_d \geq 2$. Let $\mu = 2g - 2 + \sum_{i=1}^{d}(1 - \frac{1}{m_i})$ and suppose $\mu > 0$.*

(i) *The probability that a randomly chosen connected covering $\pi \in P(\mathbf{m}, n)$ has monodromy group A_n or S_n tends to 1 as $n \to \infty$; moreover, this probability is $1 - O(c^{-n})$ for some constant $c > 1$.*

(ii) *For $1 \leq i \leq d$ let C_i be a conjugacy class in S_n having cycle-shape $(m_i^{a_i}, 1^{f_i})$ with f_i bounded, and assume $\prod_{i=1}^{d} \mathrm{sgn}(C_i) = 1$. Write $\mathbf{C} = (C_1, \ldots, C_d)$. If $\pi \in P(\mathbf{C}, n)$ is randomly chosen, then the probability that the monodromy group of π is A_n or S_n is $1 - O(n^{-\mu})$.*

Further results along these lines can be found in Section 8.

The ideas in this paper also have some bearing on certain random walks on symmetric groups. Let S be a subset of S_n generating A_n or S_n, and consider the random walk on the corresponding Cayley graph starting at the identity, and at each step moving from a vertex g to a neighbour gs, where $s \in S$ is chosen at random. Let $P^t(g)$ be the probability of reaching the vertex g after t steps. In recent years there has been much work on understanding the distribution P^t as t gets larger, and its relation to the uniform distribution. See Diaconis [9, 10] for background. The *mixing time* of the random walk is the smallest integer t such that

$$||P^t - U||_1 < \frac{1}{e}$$

where $||f||_1 = \sum |f(x)|$ is the l_1-norm. Much attention has focussed on the mixing time in the case where S is a conjugacy class of S_n. For example, [11] deals with transpositions, [32] with cycle-shapes (m^a) for fixed m, and [43] with arbitrary classes of permutations having at least ϵn fixed points (ϵ a positive constant). See also [18, 29] for some results on random walks on groups of Lie type.

In the next result we consider more general random walks, where the generating conjugacy class S may change with time. In the conclusion we arrive at a probability distribution which is close to the uniform distribution in the l_∞-norm, which is stronger than the l_1-norm condition in the definition of mixing time (and it also implies that the random walk hits all elements of the correct signature).

Theorem 1.14 *Let $m_1, \ldots, m_d \geq 2$ be integers satisfying $\sum_{i=1}^{d} \frac{1}{m_i} < d - 2$, and set $\mu = d - 2 - \sum_{i=1}^{d} \frac{1}{m_i}$. For $1 \leq i \leq d$ let C_i be a conjugacy class in S_n having cycle-shape $(m_i^{a_i}, 1^{f_i})$ with f_i bounded. Set $\alpha = \prod_{i=1}^{d} \mathrm{sgn}(C_i)$. Then for any $h \in S_n$ satisfying $\mathrm{sgn}(h) = \alpha$, and for randomly chosen $x_i \in C_i$, we have*

$$\mathit{Prob}(x_1 \cdots x_d = h) = \frac{2}{n!}(1 + O(n^{-\mu})).$$

In particular, if n is sufficiently large then, taking σ to be any permutation with $\operatorname{sgn}(\sigma) = \alpha$, *we have* $\prod_{i=1}^{d} C_i = A_n\sigma$ *almost uniformly pointwise.*

Taking $m_1 = \ldots = m_d = m$ and $C_1 = \ldots = C_d = C$, of cycle-shape $(m^a, 1^f)$ with f bounded, we see that a random walk on S_n with generating set C achieves an almost uniform distribution after t steps, where $t = 3$ if $m \geq 4$, $t = 4$ if $m = 3$ and $t = 5$ if $m = 2$. For the case where C is fixed point free (i.e. $f = 0$), Lulov [32] shows that the mixing time is 3 if $m = 2$ and 2 otherwise; while our number t of steps is slightly more than this, our distribution is arbitrarily close to uniform in the l_∞-norm, which is stronger than the mixing time condition. Moreover, our numbers t are best possible for this distribution (see below).

Another interesting case of Theorem 1.14 is that in which $d = 3$ and $(m_1, m_2, m_3) = (2, 3, 7)$. In particular it follows that if C_1, C_2, C_3 are conjugacy classes of elements in A_n of orders 2,3,7 respectively, with boundedly many fixed points, then $C_1C_2C_3 = A_n$ almost uniformly pointwise (the proof of this depends on an application of Theorem 1.1 with $s = \frac{1}{42}$).

Theorem 1.14 is best possible, in the sense that if $\sum \frac{1}{m_i} \geq d-2$ then the resulting distribution is not sufficiently close to uniform (in the l_∞-norm). We prove this in Proposition 9.1 using results on Eisenstein numbers in the Euclidean and spherical cases which are obtained in [26] by geometric methods.

We are grateful to Martin Bridson, Persi Diaconis, Brent Everitt and Paul Seidel for useful discussions on some of the background material in this paper, and to Walter Hayman for his help with the proof of Lemma 2.18.

Notation

Unless otherwise stated, Γ will denote a Fuchsian group as in (1.1) or (1.2). Define $v = v(\Gamma)$ to be 2 in the oriented case (1.1), and to be 1 in the non-oriented case (1.2). Define $\mu = \mu(\Gamma)$, so that

$$(1.4) \qquad \mu = vg - 2 + \sum_{i=1}^{d}(1 - \frac{1}{m_i}) + s + t.$$

For a positive integer n, denote by $p(n)$ the number of partitions of n. It is well known that $p(n) < c^{\sqrt{n}}$ for some constant c (see [1, 6.3]).

For a positive integer m and a finite group G, denote by $j_m(G)$ the number of solutions to the equation $x^m = 1$ in G.

Recall that for functions f_1, f_2, we write $f_1 \sim f_2$ if there are positive constants c_1, c_2 such that $c_1f_2 \leq f_1 \leq c_2f_2$.

We shall use $c, c_1, c_2, \ldots$ to denote constants, never depending on n, but often depending on various fixed parameters in a given context; this dependence will be clarified whenever necessary.

Layout

Section 2, which is the longest section in this paper, contains our results on characters of symmetric groups, which serve as a main tool in the rest of the paper. In Section 3 we count homomorphisms from Fuchsian groups to symmetric and alternating groups, proving Theorems 1.2 and 1.12(i). In Section 4 we study $\mathrm{Hom}_{trans}(\Gamma, S_n)$ and prove the subgroup growth results 1.4 and 1.12(iii). In Section 5 we prove Theorem 1.5, showing that almost all index n subgroups of a Fuchsian group are maximal. Section 6 contains our proofs of the random quotient theorems 1.6 and 1.7, together with Higman's conjecture 1.8. In Section 7 we prove our more explicit random quotient result 1.9 and use it to prove Theorem 1.10. Section 8 deals with applications to coverings of Riemann surfaces, and contains the proofs of Theorems 1.3 and 1.12(ii), as well as Theorem 1.13 and some related results. Finally, in Section 9 we discuss the random walk applications, proving Theorem 1.14 and also Proposition 9.1 showing the best possible nature of the theorem.

2 Characters of symmetric groups: asymptotic results

In this section we develop some of the machinery needed in the proofs of our main results. Most of this machinery consists of results, largely of an asymptotic nature, concerning the degrees and values of the irreducible characters of symmetric groups. The main such results are Theorems 2.6, 2.14 and 2.15 below. At the end of the section we discuss the numbers of elements of given order in symmetric and alternating groups.

We shall use [23] as our basic reference for the character theory of symmetric groups.

2.1 Results on character degrees

By a partition of a positive integer n, we mean a tuple $\lambda = (\lambda_1, \ldots, \lambda_r)$ with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r \geq 1$ and $\sum_{i=1}^{r} \lambda_i = n$. Denote by χ_λ the irreducible character of S_n corresponding to the partition λ.

We begin with an easy lower bound.

Lemma 2.1 *Write $\lambda_1 = n - k$, and assume that $n \geq 2k$. Then $\chi_\lambda(1) \geq \binom{n-k}{k}$.*

Proof Recall that $\chi_\lambda(1)$ is equal to the number of standard λ-tableaux, that is, the number of ways of filling in a λ-tableau with the numbers $1, \ldots, n$ in such a way that the numbers increase along the rows and down the columns.

Consider the following procedure. Write the numbers $1, \ldots, k$ in ascending order at the beginning of the first row of a λ-tableau. Then choose any k of the remaining $n - k$ numbers and arrange them in rows $2, \ldots, r$ of the λ-tableau, increasing along rows and down columns. Finally, write the remaining $n - 2k$ numbers in ascending order along the rest of the first row.

This procedure gives a standard λ-tableau, and can be carried out in at least $\binom{n-k}{k}$ ways, giving the result. ■

Lemma 2.2 *We have $\chi_\lambda(1) \geq \binom{n-\lambda_2}{n-\lambda_1}$.*

Proof The proof is virtually the same as the previous one. Write $1, \ldots, \lambda_2$ to start the first row of a λ-tableau, then choose $n - \lambda_1$ of the remaining $n - \lambda_2$ numbers to put in rows $2, \ldots, r$, and finally fill in the rest of the first row with the remaining numbers in ascending order. This gives at least $\binom{n-\lambda_2}{n-\lambda_1}$ standard λ-tableaux. ■

Lemma 2.3 *We have $\chi_\lambda(1) \geq 2^{\min(\lambda_2, \lambda_1 - 1)}$.*

Proof In a λ-tableau, place a 1 in the first entry of row 1, and for $1 \leq i \leq \min(\lambda_2, \lambda_1 - 1)$, place $i, i+1$ in either order in the i^{th} entry of row 2 and the $i + 1^{th}$ entry of row 1. This can be done in $2^{\min(\lambda_2, \lambda_1 - 1)}$ ways, each of which can be completed to a standard λ-tableau. ■

Denote by $\lambda' = (\lambda'_1, \ldots, \lambda'_s)$ the partition conjugate to λ (so that $\lambda'_1 = r$), and recall that $\chi_{\lambda'} = \chi_\lambda \otimes \text{sgn}$, where $\text{sgn} = \chi_{(1^n)}$ is the sign character of S_n.

Proposition 2.4 *Let $0 < \epsilon < 1$, and suppose that λ is a partition of n such that $\lambda'_1 \leq \lambda_1 \leq (1 - \epsilon)n$. Then $\chi_\lambda(1) > c^n$, where $c = c(\epsilon) > 1$.*

Proof If $\lambda_2 \geq \epsilon n$ this is immediate from the previous lemma, so assume $\lambda_2 < \epsilon n$. Moreover, if $\lambda_1 > \lambda_2 + \epsilon n$ the conclusion follows from Lemma 2.2, so assume also that $\lambda_1 \leq \lambda_2 + \epsilon n < 2\epsilon n$.

Without loss of generality we may assume that $\epsilon \leq \frac{1}{8e}$. Now for any i, j the ij-hook has length $h_{ij} = \lambda_i + \lambda'_j + 1 - i - j$ (see [23, p.73]), and so

$h_{ij} \leq \lambda_1 + \lambda_1' < 4\epsilon n$. Hence by the Hook Formula [23, 20.1],

$$\chi_\lambda(1) = \frac{n!}{\prod h_{ij}} > \frac{n!}{(4\epsilon n)^n} > \frac{(n/e)^n}{(4\epsilon n)^n} = (\frac{1}{4\epsilon e})^n \geq 2^n,$$

giving the result. ■

Proposition 2.5 *Fix a real number $s > 0$ and a positive integer k, and let Λ be the set of partitions λ of n such that $\lambda_1' \leq \lambda_1 \leq n-k$. Then*

$$\sum_{\lambda \in \Lambda} \chi_\lambda(1)^{-s} = O(n^{-sk})$$

(where the implied constant depends on k).

Proof Define $\Lambda_1 = \{\lambda \in \Lambda : \lambda_1 \geq \frac{2}{3}n\}$ and $\Lambda_2 = \{\lambda \in \Lambda : \lambda_1 < \frac{2}{3}n\}$, and let

$$\Sigma_1 = \sum_{\lambda \in \Lambda_1} \chi_\lambda(1)^{-s}, \; \Sigma_2 = \sum_{\lambda \in \Lambda_2} \chi_\lambda(1)^{-s}.$$

For $k \leq l \leq n/3$, the set Λ_1 contains at most $p(l)$ partitions λ with $\lambda_1 = n-l$ (where $p(l)$ denotes the partition function). Hence using Lemma 2.1, we have

$$\Sigma_1 \leq \sum_{k \leq l \leq n/3} \frac{p(l)}{\binom{n-l}{l}^s}.$$

We claim that

$$\Sigma_1 = O(n^{-sk}). \tag{1}$$

To see this, observe that for $1 \leq l \leq \frac{n}{3}$, we have

$$\binom{n-l}{l} \geq (\frac{n-l}{l})^l \geq (n-l)^{\sqrt{l}} \geq (\frac{2n}{3})^{\sqrt{l}}.$$

Set

$$\Sigma_1' = \sum_{k \leq l \leq k^2} \frac{p(l)}{\binom{n-l}{l}^s}, \quad \Sigma_1'' = \sum_{k^2 < l \leq n/3} \frac{p(l)}{\binom{n-l}{l}^s}.$$

Since k is fixed we obviously have $\Sigma_1' \leq cn^{-sk}$ (where c depends on k). Now consider Σ_1''. For $k^2 < l \leq n/3$, we have

$$\frac{p(l)}{\binom{n-l}{l}^s} \leq \frac{c_1^{\sqrt{l}}}{(2n/3)^{s\sqrt{l}}} \leq (\frac{c_2}{n^s})^{\sqrt{l}},$$

where c_1, c_2 are absolute constants. This yields

$$\Sigma_1'' \leq \sum_{l=k^2+1}^{\infty} (\frac{c_2}{n^s})^{\sqrt{l}},$$

which, letting q denote c_2/n^s, is bounded above by the integral

$$\int_{k^2}^{\infty} q^{\sqrt{x}} dx = \frac{2q^k}{\alpha}(k + \frac{1}{\alpha}),$$

where $\alpha = -\log q$. Hence $\Sigma_1'' \leq c_3 n^{-sk}$, where c_3 depends on k. This proves (1).

Next, by Proposition 2.4, there is a constant $c > 1$ such that

$$\Sigma_2 < p(n)c^{-ns}.$$

Since $p(n) < c_4^{\sqrt{n}}$ for some constant c_4, it follows that $\Sigma_2 \leq c_5^{-ns}$, and hence

$$\Sigma_1 + \Sigma_2 = O(n^{-sk}),$$

giving the result. ■

Observe that the 'dual' result $\sum_{\lambda \in \Lambda'} \chi_\lambda(1)^{-s} = O(n^{-sk})$ also holds, where $\Lambda' = \{\lambda \vdash n \ : \ \lambda_1 \leq \lambda_1' \leq n - k\}$, since $\chi_\lambda(1) = \chi_{\lambda'}(1)$.

From this we deduce one of our main character-theoretic results, stated as Theorem 1.1 in the Introduction:

Theorem 2.6 *Fix a real number $s > 0$. Then*

$$\sum_{\chi \in Irr(S_n)} \chi(1)^{-s} = 2 + O(n^{-s}).$$

Proof The number 2 on the right hand side comes from $\chi = \chi_{(n)}(= 1)$ and $\chi = \chi_{(1^n)}(= \text{sgn})$. Applying Proposition 2.5 and the remark following it for $k = 1$, we see that the remaining characters contribute $O(n^{-s})$ to the sum on the right hand side, giving the result. ■

We shall need the following easy consequence for A_n.

Corollary 2.7 *Fix a real number $s > 0$. Then*

$$\sum_{\chi \in Irr(A_n)} \chi(1)^{-s} = 1 + O(n^{-s}).$$

Proof For each irreducible character χ of S_n, either $\chi \downarrow A_n$ is irreducible, or $\chi \downarrow A_n = \chi_1 + \chi_2$, a sum of two irreducible characters of degree $\chi(1)/2$. All irreducible characters of A_n occur in this way. Hence

$$\sum_{1 \neq \chi \in Irr(A_n)} \chi(1)^{-s} \leq 2 \cdot 2^s \cdot \sum_{\chi \in Irr(S_n), \chi(1) > 1} \chi(1)^{-s} = O(n^{-s}).$$

The result follows. ■

2.2 Results on character values

We begin by stating a result of Fomin and Lulov [17] which plays a key role in this paper.

Theorem 2.8 (Fomin-Lulov [17]) *Fix an integer $m \geq 2$. Suppose n is divisible by m, say $n = am$, and let $\pi \in S_n$ be a permutation of cycle-shape (m^a). Then for any irreducible character χ of S_n, we have*

$$|\chi(\pi)| \leq \frac{a!\, m^a}{(n!)^{1/m}} \cdot \chi(1)^{1/m} \leq c \cdot n^{\frac{1}{2}(1-\frac{1}{m})} \cdot \chi(1)^{1/m},$$

where c depends only on m.

We shall also frequently use the Murnaghan-Nakayama Rule [23, 21.1]. By a *rim r-hook* ν in a λ-tableau, we mean a connected part of the rim containing r nodes, which can be removed to leave a proper tableau, denoted by $\lambda \backslash \nu$. If, moving from right to left, the rim hook ν starts in row i and finishes in column j, then the *leg-length* $l(\nu)$ is defined to be $\lambda'_j - i$ (the number of nodes below the ij-node in the λ-tableau).

Theorem 2.9 (Murnaghan-Nakayama Rule) *Let $\rho\sigma \in S_n$, where ρ is an r-cycle and σ is a permutation of the remaining $n - r$ points. Then*

$$\chi_\lambda(\rho\sigma) = \sum_\nu (-1)^{l(\nu)} \chi_{\lambda\backslash\nu}(\sigma),$$

where the sum is over all rim r-hooks ν in a λ-tableau.

An easy consequence is the following.

Lemma 2.10 *Let $\rho \in S_n$ be an $(n-c)$-cycle, and let σ be a permutation of the remaining c points. Then for any partition λ of n,*

$$|\chi_\lambda(\rho\sigma)| \leq f(c),$$

where $f(c)$ depends only on c, and $f(0) = 1, f(1) = 2$.

Proof Apply Theorem 2.9 with $r = n - c$. Observe that λ has at most $c + 1$ rim $(n-c)$-hooks ν, and for each such ν we have

$$|\chi_{\lambda\backslash\nu}(\sigma)| \leq \chi_{\lambda\backslash\nu}(1) \leq (c!)^{1/2},$$

so $f(c) = (c+1) \cdot (c!)^{1/2}$ will do. ■

In order to apply the Murnaghan-Nakayama rule it is useful to estimate the number of rim r-hooks in a tableau. We prove the following.

Lemma 2.11 *For any positive integer r, and any partition λ of n, the number of rim r-hooks in a λ-tableau is at most $\sqrt{2n}$.*

Proof A rim r-hook ν is uniquely determined by the topmost row it intersects, say row t_ν, and also by the leftmost column it intersects, say column l_ν. Let R be the set of all rim r-hooks, and denote by $P_2(R)$ the set of all 2-subsets of R. Define a map from $R \cup P_2(R)$ to the set consisting of the n nodes of the λ-tableau as follows:

$$\begin{aligned} \nu \to &\quad \text{node } (t_\nu, l_\nu) \ \ (\nu \in R), \\ \{\nu_1, \nu_2\} \to &\quad \text{node } (t_{\nu_1}, l_{\nu_2}) \ \ (\nu_1, \nu_2 \in R, t_{\nu_1} < t_{\nu_2}). \end{aligned}$$

This map is injective, showing that

$$|R| + \binom{|R|}{2} \leq n,$$

which gives the result. ■

Proposition 2.12 (i) *Let $\pi \in S_n$ and let $C(\pi)$ be the total number of cycles in π. Then for any $\chi \in Irr(S_n)$, we have*

$$|\chi(\pi)| \leq (2n)^{C(\pi)/2}.$$

(ii) *Let $\pi = \rho\sigma \in S_n$ be a permutation of order m, where ρ has cycle-shape (m^a) and σ permutes the remaining $n - ma$ points. Let $C(\sigma)$ be the number of cycles in σ. Then for any $\chi \in Irr(S_n)$ we have*

$$|\chi(\pi)| \leq c \cdot (2n)^{\frac{1}{2}C(\sigma)(1-\frac{1}{m})} \chi(1)^{1/m} n^{1/2},$$

where c depends only on m.

(iii) *Let $\pi \in S_n$ have cycle-shape $(m^a, 1^f)$. Then for any $\chi \in Irr(S_n)$ we have*

$$|\chi(\pi)| \leq c \cdot (2n)^{\frac{1}{2}(f+1)} \chi(1)^{1/m},$$

where c depends only on m.

Proof (i) This follows by repeated application of the Murnaghan-Nakayama Rule, using Lemma 2.11.

(ii) Applying the Murnaghan-Nakayama Rule and Lemma 2.11 we see that

$$|\chi(\pi)| \leq \sum |\chi_i(\rho)|,$$

where $\chi_i \in Irr(S_{ma})$, the sum has at most $(2n)^{C(\sigma)/2}$ terms, and $\sum \chi_i(1) \leq \chi(1)$. By Theorem 2.8, $|\chi_i(\rho)| \leq c \cdot \chi_i(1)^{1/m} n^{1/2}$, where $c = c(m)$. It is easy to see that the maximum of $\sum_{i=1}^N X_i^{1/m}$ subject to $\sum_{i=1}^N X_i \leq X$ (where

X, X_i are positive real numbers) is $N^{1-1/m}X^{1/m}$ (obtained when the X_i are all equal). This implies

$$|\chi(\pi)| \leq c \cdot (2n)^{(C(\sigma)/2)(1-1/m)}\chi(1)^{1/m}n^{1/2},$$

as required.

(iii) This is immediate from (ii). ■

Lemma 2.13 *Let $\pi \in S_n$ have cycle-shape $(m^a, 1^f)$, let λ be a partition of n, and write $\lambda_1 = n - k$. Then there exists $c = c(m, k, f)$ such that $|\chi_\lambda(\pi)| \leq cn^{[k/m]}$.*

Proof Write $\pi = \pi'1$ where $\pi' \in S_{n-f}$ has cycle-shape (m^a). The number of sequences of f rim 1-hooks we can successively remove from a λ-tableau is bounded in terms of f and k, so we have

$$|\chi_\lambda(\pi)| \leq \sum |\chi_{\mu_i}(\pi')|$$

where each μ_i is a partition of $n - f$ obtained by removing f nodes from λ, and there are $c_1(k, f)$ terms in the sum.

Now fix i, and consider the set $\mathcal{S}_i$ of sequences of a rim m-hooks which we can successively remove from μ_i. Given the positions in the sequence in which m-hooks having all nodes below the first row appear, the number of such sequences is bounded in terms of m and k (apart from these positions, one is forced to remove hooks from the first row until an m, k-bounded shape is reached). Clearly the number of positions for m-hooks having all nodes below the first row is at most $[k/m]$. Hence

$$|\mathcal{S}_i| \leq c_2(m, k) \cdot \sum_{i=1}^{[k/m]} \binom{n}{i} \leq c_3(m, k)\binom{n}{[k/m]}.$$

The Murnaghan-Nakayama Rule implies that $|\chi_{\mu_i}(\pi')| \leq |\mathcal{S}_i|$, and hence

$$|\chi_\lambda(\pi)| \leq c_1(k, f)c_3(m, k)\binom{n}{[k/m]} \leq c(k, f, m)n^{[k/m]},$$

as required. ■

The next theorem is our second main result on character values for S_n.

Theorem 2.14 *Let $m \geq 2$ be an integer. There is a constant $c = c(m)$ such that for any $\pi \in S_n$ of order m and any $\chi \in Irr(S_n)$, we have*

$$|\pi^{S_n}| \cdot |\chi(\pi)| < (n!)^{1-\frac{1}{m}} \cdot \chi(1)^{1/m} \cdot c^{n^{1-\frac{1}{2m}}}.$$

Proof In this proof we use constants c_i ($i = 0, 1, 2, \ldots$), all of which depend only on m. Let π have cycle-shape $(m_1^{a_1}, \ldots, m_k^{a_k})$, where $\sum m_i a_i = n$, $m_1 > m_2 > \ldots > m_k$ and $m_1 = m$ (allowing the possibility that $a_1 = 0$). Set $A = \sum_{i=2}^k a_i$. Since

$$|\pi^{S_n}| = \frac{n!}{\prod_{i=1}^k m_i^{a_i} \prod_{i=1}^k a_i!},$$

Proposition 2.12(ii) implies that

$$|\pi^{S_n}| \cdot |\chi(\pi)| \leq c_0 \cdot \frac{n!}{\prod_{i=1}^k m_i^{a_i} \prod_{i=1}^k a_i!} (2n)^{\frac{1}{2}A(1-\frac{1}{m})} \chi(1)^{1/m} n^{1/2}. \tag{2}$$

Hence, setting

$$\gamma = 1 - \frac{1}{2m}, \quad T = \frac{n!}{\prod_{i=1}^k m_i^{a_i} \prod_{i=1}^k a_i!} (2n)^{\frac{1}{2}A(1-\frac{1}{m})},$$

it suffices to prove

$$T \leq (n!)^{1-\frac{1}{m}} c_1^{n^\gamma} \tag{3}$$

for some constant c_1 (since $c_0 c_1^{n^\gamma} n^{1/2} \leq c^{n^\gamma}$).

Assume first that $A > n/m$. Since $\frac{n^a}{a!} < e^a$ for any positive integer a, we have $\frac{n^{\sum a_i}}{\prod a_i!} < e^{\sum a_i}$, and hence

$$\frac{n!}{\prod_{i=1}^k a_i!} < \frac{n^n}{\prod_{i=1}^k a_i!} < e^{\sum_1^k a_i} n^{n - \sum_1^k a_i}.$$

This implies

$$T < c_2^n \cdot n^{n - \sum_1^k a_i} \cdot n^{\frac{1}{2}A(1-\frac{1}{m})} = c_2^n \cdot n^{n - a_1 - \frac{1}{2}A(1+\frac{1}{m})}.$$

Recall that $A = \sum_{i=2}^k a_i$, and that for $i \geq 2$, m_i is a proper divisor of m. It follows that $a_1 m + Am/2 \geq n$, whence

$$a_1 + \frac{1}{2}A(1 + \frac{1}{m}) \geq a_1 + \frac{1}{2}A + \frac{n}{2m^2} \geq n(\frac{1}{m} + \frac{1}{2m^2}).$$

It follows that

$$T < c_2^n \cdot n^{n(1-\frac{1}{m}-\frac{1}{2m^2})} < (n!)^{1-\frac{1}{m}}$$

for large n, which implies (3) in this case.

Now assume that $A \leq n/m$. By Stirling's formula,

$$T < c_3 n^{1/2} (\frac{n}{e})^n \cdot \frac{(2n)^{\frac{1}{2}A(1-\frac{1}{m})}}{m^{a_1} (a_1/e)^{a_1} \prod_{i=2}^k a_i!}. \tag{4}$$

Since $a_1 \geq \frac{n}{m} - \frac{1}{2}A$, we have

$$\begin{aligned} a_1^{a_1} &\geq (\frac{n}{m} - \frac{1}{2}A)^{a_1} = (\frac{n}{m})^{a_1}(1 - \frac{mA}{2n})^{a_1} \\ &= (\frac{n}{m})^{a_1}(1 - \frac{mA}{2n})^{\frac{2n}{mA} \cdot \frac{a_1 mA}{2n}}. \end{aligned}$$

Since $A \leq n/m$, we have $\frac{mA}{2n} \leq \frac{1}{2}$, which implies $(1 - \frac{mA}{2n})^{\frac{2n}{mA}} \geq e^{-2}$. This yields

$$a_1^{a_1} \geq (\frac{n}{m})^{a_1} e^{\frac{-a_1 mA}{n}} \geq (\frac{n}{m})^{a_1} e^{-A}$$

(since $a_1 \leq n/m$). Substituting in (4), this gives

$$\begin{aligned} T &< c_3 n^{1/2} (\frac{n}{e})^n \cdot \frac{(2n)^{\frac{1}{2}A(1-\frac{1}{m})} e^{a_1}}{m^{a_1} (n/m)^{a_1} e^{-A} \prod_{i=2}^k a_i!} \\ &= c_3 n^{1/2} (\frac{n}{e})^n \cdot \frac{(2n)^{\frac{1}{2}A(1-\frac{1}{m})} e^{a_1 + A}}{n^{a_1} \prod_{i=2}^k a_i!} \\ &\leq c_3 c_4^A n^{1/2} \cdot (\frac{n}{e})^{n - a_1} \cdot \frac{n^{\frac{1}{2}A(1-\frac{1}{m})}}{\prod_{i=2}^k a_i!}. \end{aligned}$$

Now $n - a_1 \leq n(1 - \frac{1}{m}) + \frac{1}{2}A$. So

$$\begin{aligned} T < c_3 c_4^A n^{1/2} \cdot (\frac{n}{e})^{n(1-\frac{1}{m}) + \frac{1}{2}A} \cdot \frac{n^{\frac{1}{2}A(1-\frac{1}{m})}}{\prod_{i=2}^k a_i!} &\leq c_3 c_5^A n^{1/2} \cdot (\frac{n}{e})^{n(1-\frac{1}{m})} \cdot \frac{n^{A - \frac{A}{2m}}}{\prod_{i=2}^k a_i!} \\ &= c_3 n^{1/2} (\frac{n}{e})^{n(1-\frac{1}{m})} \cdot \prod_{i=2}^k \frac{(c_5 n^{1-\frac{1}{2m}})^{a_i}}{a_i!} \\ &< c_3 n^{1/2} (\frac{n}{e})^{n(1-\frac{1}{m})} \cdot \prod_{i=2}^k e^{c_5 n^{1-\frac{1}{2m}}} < (n!)^{1-\frac{1}{m}} e^{c_6 n^\gamma}, \end{aligned}$$

whence (3). ■

Theorem 2.14 is our main tool for bounding the right hand side in the formula (1.3), for general classes C_i of elements of order m_i. In the case of almost homogeneous classes, we are able to establish the following precise estimate, which will be used frequently in later sections.

Theorem 2.15 *For $1 \leq i \leq d$ fix integers $m_i \geq 2$ and $f_i \geq 0$, and let $\pi_i \in S_n$ have cycle-shape $(m_i^{a_i}, 1^{f_i})$. Let $l \geq 0$ and set $\mu = l + d - 2 - \sum_{i=1}^d \frac{1}{m_i}$. Assume that $\mu > 0$. Then*

$$\sum_{\chi \in Irr(S_n), \chi(1) > 1} \frac{|\chi(\pi_1) \cdots \chi(\pi_d)|}{\chi(1)^{l+d-2}} = O(n^{-\mu}).$$

In particular, if $\prod_{i=1}^{d} \operatorname{sgn}(\pi_i) = 1$, *then*

$$\sum_{\chi \in Irr(S_n)} \frac{\chi(\pi_1)\cdots\chi(\pi_d)}{\chi(1)^{l+d-2}} = 2 + O(n^{-\mu}).$$

Proof In this proof we use $c_1, \ldots, c_6$ to denote constants depending only on the m_i and f_i. To prove the first statement, we may restrict attention to characters $\chi = \chi_\lambda$ with $\lambda_1' \leq \lambda_1$ (since the other characters are products of these with the sign character). We subdivide these non-linear irreducible characters of S_n as follows. Define $C = \frac{1}{\mu}\sum_{i=1}^{d} \frac{f_i+1}{2}$, and write

$$\begin{aligned} \Lambda_1 &= \{\lambda \vdash n : \lambda_1' \leq \lambda_1 \leq n - C - 1\}, \\ \Lambda_2 &= \{\lambda \vdash n : \lambda_1' \leq \lambda_1, n > \lambda_1 > n - C - 1\}. \end{aligned}$$

For $\lambda \in \Lambda_1$, Proposition 2.12(iii) gives $|\chi_\lambda(\pi_i)| \leq c_1(2n)^{\frac{f_i+1}{2}}\chi_\lambda(1)^{1/m_i}$, and hence

$$\frac{|\chi_\lambda(\pi_1)\cdots\chi_\lambda(\pi_d)|}{\chi_\lambda(1)^{l+d-2}} \leq c_1^d n^{\sum(f_i+1)/2}\chi_\lambda(1)^{(\sum\frac{1}{m_i})-(l+d-2)} = c_2 n^{\sum(f_i+1)/2}\chi_\lambda(1)^{-\mu}.$$

Therefore

$$\sum_{\lambda\in\Lambda_1} \frac{|\chi_\lambda(\pi_1)\cdots\chi_\lambda(\pi_d)|}{\chi_\lambda(1)^{l+d-2}} \leq c_2 \cdot n^{\sum(f_i+1)/2} \sum_{\lambda\in\Lambda_1}\chi_\lambda(1)^{-\mu}.$$

Hence by Theorem 2.5,

$$\sum_{\lambda\in\Lambda_1} \frac{|\chi_\lambda(\pi_1)\cdots\chi_\lambda(\pi_d)|}{\chi_\lambda(1)^{l+d-2}} \leq c_3 \cdot n^{\sum(f_i+1)/2}\cdot n^{-\mu(C+1)} = O(n^{-\mu}). \qquad (5)$$

For $\lambda \in \Lambda_2$ we have $\lambda_1 = n - k$ with $k < C + 1$, and Lemmas 2.13 and 2.1 give

$$|\chi_\lambda(\pi_i)| < c_4 n^{[k/m_i]},\ \chi_\lambda(1) > c_5 n^k.$$

Hence

$$\frac{|\chi_\lambda(\pi_1)\cdots\chi_\lambda(\pi_d)|}{\chi_\lambda(1)^{l+d-2}} < c_6 n^{\sum[k/m_i]-k(l+d-2)} \leq c_6 n^{-k\mu},$$

and it follows that

$$\sum_{\lambda\in\Lambda_2} \frac{|\chi_\lambda(\pi_1)\cdots\chi_\lambda(\pi_d)|}{\chi_\lambda(1)^{l+d-2}} \leq \sum_{k=1}^{[C+1]} c_6 n^{-k\mu} = O(n^{-\mu}). \qquad (6)$$

The first conclusion now follows from (5) and (6).

The last part follows, noting that the number 2 on the right hand side comes from the trivial and sign characters of S_n. ■

We shall also need a version of Theorem 2.15 with A_n replacing S_n. We rely on the following information about the irreducible characters of A_n (see [24]). For partitions $\lambda \neq \lambda'$ of n, we have $\chi_\lambda \downarrow A_n = \chi_{\lambda'} \downarrow A_n$, and these are irreducible. And for $\lambda = \lambda'$, $\chi_\lambda \downarrow A_n = \chi_\lambda^{(1)} + \chi_\lambda^{(2)}$, a sum of two irreducible characters of A_n; moreover, for $\sigma \in A_n$, if $\sigma^{S_n} = \sigma^{A_n}$ then

$$\chi_\lambda^{(j)}(\sigma) = \frac{1}{2}\chi_\lambda(\sigma) \quad (j = 1, 2).$$

In particular this holds when σ is of cycle-shape $(m^a, 1^f)$ with $a \geq 2$.

Corollary 2.16 *Assume the hypotheses of Theorem* 2.15, *with* $\pi_i \in A_n$. *Then*

$$\sum_{1 \neq \chi \in Irr(A_n)} \frac{|\chi(\pi_1) \cdots \chi(\pi_d)|}{\chi(1)^{l+d-2}} = O(n^{-\mu}),$$

and

$$\sum_{\chi \in Irr(A_n)} \frac{\chi(\pi_1) \cdots \chi(\pi_d)}{\chi(1)^{l+d-2}} = 1 + O(n^{-\mu}).$$

Proof Write

$$T(A_n) = \sum_{1 \neq \chi \in Irr(A_n)} \frac{|\chi(\pi_1) \cdots \chi(\pi_d)|}{\chi(1)^{l+d-2}},$$

$$T(S_n) = \sum_{\chi \in Irr(S_n), \chi(1) > 1} \frac{|\chi(\pi_1) \cdots \chi(\pi_d)|}{\chi(1)^{l+d-2}}.$$

We claim that $T(A_n) \leq 2^{l-1} T(S_n)$.

To see this, consider a term $\frac{|\chi(\pi_1) \cdots \chi(\pi_d)|}{\chi(1)^{l+d-2}}$ of $T(A_n)$. If $\chi = \chi_\lambda \downarrow A_n$ $(\lambda \neq \lambda')$ then this term appears twice in $T(S_n)$. If not, then $\chi = \chi_\lambda^{(j)}$ with $\lambda = \lambda'$, $j \in \{1, 2\}$, and by the above remarks (noting that we make take n large, so that $a_i \geq 2$ for all i), $\chi(\pi_i) = \frac{1}{2}\chi_\lambda(\pi_i)$ and $\chi(1) = \frac{1}{2}\chi_\lambda(1)$. Hence

$$\frac{|\chi(\pi_1) \cdots \chi(\pi_d)|}{\chi(1)^{l+d-2}} = 2^{l-2} \cdot \frac{|\chi_\lambda(\pi_1) \cdots \chi_\lambda(\pi_d)|}{\chi_\lambda(1)^{l+d-2}}.$$

The claim follows, and the conclusion is now a consequence of Theorem 2.15. ■

2.3 Elements of given order in S_n and A_n

We conclude the section with some results on the numbers of elements of given order in symmetric and alternating groups. These will be useful in later sections.

Recall from the Introduction that for a finite group G and a positive integer m, we write

$$j_m(G) = |\{x \in G \,:\, x^m = 1\}|,$$

and also that for positive integers m, n,

$$E(n,m) = n^{-\frac{1}{2}(1-\frac{1}{m})} \cdot \exp(\sum_{a|m, a<m} \frac{n^{a/m}}{a}).$$

Lemma 2.17 *Let $m \geq 2$ be an integer. Then $j_m(S_n) \sim (n!)^{1-1/m} E(n,m)$.*

Proof The asymptotics of the numbers $j_m(S_n)$ were determined by Wilf [47]. The convenient formula in the conclusion is a special case of Müller's more general result [36, Theorem 5]. ■

In fact the results in [36, 47] are more precise, providing a constant c depending on m such that $j_m(S_n) = (c + o(1)) \cdot (n!)^{1-1/m} E(n,m)$.

We shall also need a version of this result for $j_m(A_n)$. Obviously if m is odd then $j_m(A_n) = j_m(S_n)$, so it is only necessary to consider the case where m is even.

We are very grateful to Walter Hayman for supplying most of the details of the proof of the following lemma.

Lemma 2.18 *Let $m \geq 2$ be an even integer. Then*

$$\frac{j_m(A_n)}{j_m(S_n)} \to \frac{1}{2} \text{ as } n \to \infty.$$

Moreover there is a constant $c = c(m) > 0$ such that $\frac{j_m(A_n)}{j_m(S_n)} = \frac{1}{2} + O(e^{-cn^{1/m}})$.

Proof It is possible to prove this directly, but we choose to give an elegant proof using generating functions, along similar lines to part of Wilf's proof in [47]. Write $a_n = j_m(S_n)$, $b_n = j_m(A_n)$, and for $z \in \mathbb{C}$ define the generating functions

$$f(z) = \sum_{n=1}^{\infty} a_n z^n, \quad g(z) = 2\sum_{n=1}^{\infty} b_n z^n.$$

An old result of Chowla, Herstein and Scott [3] states that

$$f(z) = \exp(\sum_{k|m} \frac{z^k}{k}),$$

while it follows from [4, Theorem 4] that

$$g(z) = \exp(\sum_{k|m} \frac{z^k}{k}) + \exp(\sum_{k|m} \frac{(-1)^{k-1}z^k}{k}).$$

Write

$$h(z) = g(z) - f(z) = \exp(\sum_{k|m} \frac{(-1)^{k-1}z^k}{k}).$$

At the heart of the proofs of Lemma 2.17 in [36, 47] is a result of Hayman [20], which provides an asymptotic estimate for a_n as follows. Write $P(z) = \sum_{k|m} \frac{z^k}{k}$ and set $r = |z|$. Define $a(r) = rP'(r)$ and $b(r) = ra'(r)$, so $a(r) \sim mP(r)$ and $b(r) \sim m^2P(r)$. (Here and in the rest of this proof only, we are using $\sim$ in a stronger sense than elsewehere, writing $\alpha(r) \sim \beta(r)$ to mean that $\alpha(r)/\beta(r) \to 1$ as $r \to \infty$.) Then by [20, Corollary II], if we define r_n by $a(r_n) = n$, we have

$$a_n \sim \frac{f(r_n)}{(r_n)^n\sqrt{2\pi b(r_n)}} \sim \frac{f(r_n)}{(r_n)^n\sqrt{2\pi m^2 P(r_n)}}. \tag{7}$$

We shall establish that if $M(r,h) = \sup_{|z|=r}|h(z)|$, then there is a positive constant ϵ_1 such that for large r,

$$\frac{M(r,h)}{M(r,f)} \leq e^{-\epsilon_1 r}. \tag{8}$$

Given (8), the lemma follows quickly: letting $h(z) = \sum c_n z^n$ (so $c_n = 2b_n - a_n$), Cauchy's inequality and (8) yield, for large n,

$$|c_n| \leq \frac{M(r_n,h)}{(r_n)^n} \leq \frac{e^{-\epsilon_1 r_n}M(r_n,f)}{(r_n)^n} \leq \frac{e^{-\epsilon_1 r_n}f(r_n)}{(r_n)^n}$$

(the last inequality holds since $|f(z)| \leq f(|z|)$). Hence by (7) we have $\frac{|c_n|}{a_n} \leq e^{-\epsilon_2 r_n}$ for some constant $\epsilon_2 > 0$. By definition of r_n we have $P(r_n) \sim n/m$. Therefore $\frac{|c_n|}{a_n} \leq e^{-\epsilon_3 n^{1/m}}$ for some constant $\epsilon_3 > 0$. As $\frac{b_n}{a_n} = \frac{1}{2} + \frac{c_n}{a_n}$, the lemma follows.

It remains to establish (8). Write $z = re^{i\theta}$, so $Re(z^n) = r^n \cos n\theta$, and define $Q(z) = \sum_{k|m} \frac{(-1)^{k-1}z^k}{k}$. As m is even, z^m appears with a negative coefficient in $Q(z)$.

If $|\theta| < \frac{\pi}{4m}$, then $\cos m\theta > \cos(\pi/4) = 1/\sqrt{2}$, and so

$$\log|\frac{h(z)}{f(z)}| \leq -\frac{2}{m}r^m \cos m\theta < \frac{-\sqrt{2}r^m}{m}.$$

And if $|\theta| \geq \frac{\pi}{4m}$, consideration of the $k=1$ terms in the expressions $f(z) = \exp(\sum_{k|m} \frac{z^k}{k})$ and $h(z) = \exp(\sum_{k|m} \frac{(-1)^{k-1}z^k}{k})$ shows that

$$\log |\frac{h(re^{i\theta})}{f(r)}| \leq r\cos\theta - r \leq -r(1-\cos(\pi/4m)).$$

Thus for large r and all θ, we deduce that

$$\log \frac{|h(re^{i\theta})|}{M(r,f)} \leq -\epsilon r,$$

where ϵ is a positive constant. This yields (8), and hence completes the proof. ■

3 Homomorphisms from Fuchsian groups to symmetric groups

In this section we prove Theorems 1.2 and 1.12(i).

First, for completeness, we give a proof of Theorems 1.2 and 1.12(i) in the easier (essentially known) case where Γ is improper (i.e. $s+t>0$ in (1.1) or (1.2)). In this case

$$\Gamma \cong Z_{m_1} * \cdots * Z_{m_d} * F_r, \tag{9}$$

where F_r is a free group of rank $r = vg+s+t-1$ and Z_m denotes a cyclic group of order m. It then follows immediately that for any finite group G,

$$|\mathrm{Hom}(\Gamma, G)| = |G|^r \prod_{i=1}^{d} j_{m_i}(G), \tag{10}$$

and hence Lemma 2.17 and Lemma 2.18 yield

$$|\mathrm{Hom}(\Gamma, S_n)| \sim |\mathrm{Hom}(\Gamma, A_n)| \sim (n!)^{r+\sum_1^d 1-\frac{1}{m_i}} \cdot \prod_{i=1}^{d} E(n, m_i). \tag{11}$$

Since $r + \sum(1-\frac{1}{m_i}) = \mu+1$, this proves Theorem 1.12(i) for the case $s+t>0$. Note that $\prod_{i=1}^{d} E(n,m_i)$ is at most $c^{\sqrt{n}}$, and at least n^b, for any b and sufficiently large n. Hence Theorem 1.2 and the remarks following it also follow in this case. The constant c can be taken to be $c_0(m)^{d+1}$, where $m = \max(1, m_1, \ldots, m_d)$.

Next, observe that by (10) we have

$$\frac{|\mathrm{Hom}(\Gamma, A_n)|}{|\mathrm{Hom}(\Gamma, S_n)|} \leq \frac{|A_n|^r}{|S_n|^r} \cdot \prod_{i=1}^{d} \frac{j_{m_i}(A_n)}{j_{m_i}(S_n)}.$$

Applying Lemma 2.18, this yields

$$\frac{|\mathrm{Hom}(\Gamma, A_n)|}{|\mathrm{Hom}(\Gamma, S_n)|} = 2^{-r-d^*} + o(1), \tag{12}$$

where r is as above and d^* is the number of m_i which are even. The $o(1)$ term is zero if $d^* = 0$; otherwise, using the error term in 2.18, we see that the $o(1)$ term is $O(e^{-cn^{1/m^*}})$, where $m^* = \max(m_i : i \text{ even})$. In other words, the probability that a random homomorphism in $\mathrm{Hom}(\Gamma, S_n)$ has image contained in A_n is $2^{-vg-s-t-d^*+1} + O(e^{-n^\delta})$ for some $\delta > 0$. This will be used in Section 6 in the proof of Theorem 1.12(vi) for the improper case.

Before continuing, we record a well known result on the number of solutions to certain equations in finite groups. In the statement $\iota(\chi)$ denotes the Schur indicator of an irreducible character χ of G. Recall that $\iota(\chi)$ is ± 1 if χ is a real character, and 0 otherwise.

Lemma 3.1 *Let G be a finite group and let d, g be positive integers. Fix an element $z \in G$.*

(i) *For $1 \leq i \leq d$ let C_i be a conjugacy class in G with representative g_i. Then the number of solutions to the equation $x_1 \cdots x_d = z$ with $x_i \in C_i$ $(1 \leq i \leq d)$ is equal to*

$$\frac{|C_1| \cdots |C_d|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(g_1) \cdots \chi(g_d)\chi(z^{-1})}{\chi(1)^{d-1}}.$$

(ii) *The number of solutions to the equation $[a_1, b_1] \cdots [a_g, b_g] = z$ with $a_i, b_i \in G$ is equal to*

$$|G|^{2g-1} \sum_{\chi \in Irr(G)} \frac{\chi(z)}{\chi(1)^{2g-1}}.$$

(iii) *The number of solutions to $a_1^2 \cdots a_g^2 = z$ with $a_i \in G$ is equal to*

$$|G|^{g-1} \sum_{\chi \in Irr(G)} \iota(\chi)^g \frac{\chi(z)}{\chi(1)^{g-1}}.$$

Proof All parts are well known. Part (i) can be found in [2, 10.1,p.43], and parts (ii),(iii) in [31, Chapter 14]. ■

In estimating $|\mathrm{Hom}(\Gamma, G)|$ it is often useful to focus on a certain subspace of special homomorphisms, defined as follows. Let $\mathbf{C} = (C_1, \ldots, C_d)$ be a d-tuple of conjugacy classes C_i of the finite group G. Set

$$\mathrm{Hom}_{\mathbf{C}}(\Gamma, G) = \{\phi \in \mathrm{Hom}(\Gamma, G) : \phi(x_i) \in C_i \ \ i = 1, \ldots, d\}.$$

Clearly (9) gives

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{vg-1+s+t}|C_1| \cdots |C_d| \quad \text{for } \Gamma \text{ improper}. \tag{13}$$

It turns out that under some extra conditions, a similar estimate holds for proper Fuchsian groups Γ (see Theorem 3.3 below).

So let us now turn to the main case, estimating $|\mathrm{Hom}(\Gamma, S_n)|$ when Γ is a proper Fuchsian group (as in (1.1), (1.2) with $s = t = 0$).

Our starting point is the following.

Proposition 3.2 (i) *Let Γ be a group with presentation as in* (1.1) *with $s = t = 0$ (but $\mu(\Gamma)$ not necessarily positive). Let G be a finite group, and for $1 \leq i \leq d$ let C_i be a conjugacy class in G with representative g_i of order m_i. Define $\mathbf{C} = (C_1, \ldots, C_d)$. Then*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{2g-1}|C_1| \cdots |C_d| \sum_{\chi \in Irr(G)} \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+2g}}.$$

(ii) *Let Γ be a group with presentation as in* (1.2) *with $s = t = 0$ (but $\mu(\Gamma)$ not necessarily positive), and let G, C_i, g_i be as in* (i). *Then*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{g-1}|C_1| \cdots |C_d| \sum_{\chi \in Irr(G)} \iota(\chi)^g \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+g}}.$$

Proof (i) This essentially goes back to Hurwitz [22]. For completeness we provide a proof. Observe first that $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)|$ is equal to the number of solutions to the equation $x_1 \cdots x_d \, [a_1, b_1] \cdots [a_g, b_g] = 1$ $(a_i, b_i \in G, x_i \in C_i)$. By Lemma 3.1(i), given $z \in G$, the number of solutions to $x_1 \cdots x_d = z$ with $x_i \in C_i$ is

$$|G|^{-1}|C_1| \cdots |C_d| \sum_{\chi \in Irr(G)} \frac{\chi(g_1) \cdots \chi(g_d)\chi(z^{-1})}{\chi(1)^{d-1}}.$$

Moreover, Lemma 3.1(ii) shows that the number of solutions to the equation $[a_1, b_1] \cdots [a_g, b_g] = z^{-1}$ is

$$|G|^{2g-1} \sum_{\chi \in Irr(G)} \frac{\chi(z)}{\chi(1)^{2g-1}}.$$

Hence $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{2g-2}|C_1|\cdots|C_d|\Lambda$, where

$$\Lambda = \sum_{z\in G}\sum_{\chi_1\in Irr(G)} \frac{\chi_1(g_1)\cdots\chi_1(g_d)\chi_1(z^{-1})}{\chi_1(1)^{d-1}} \sum_{\chi_2\in Irr(G)} \frac{\chi_2(z)}{\chi_2(1)^{2g-1}}$$

$$= \sum_{\chi_1,\chi_2,z} \frac{\chi_1(g_1)\cdots\chi_1(g_d)\chi_1(z^{-1})\chi_2(z)}{\chi_1(1)^{d-1}\chi_2(1)^{2g-1}}.$$

By the orthogonality relations, $\sum_{z\in G}\chi_1(z^{-1})\chi_2(z)$ is equal to 0 if $\chi_1 \neq \chi_2$, and is equal to $|G|$ if $\chi_1 = \chi_2$. Consequently

$$\Lambda = |G| \sum_{\chi\in Irr(G)} \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+2g}}.$$

Part (i) follows.

(ii) The argument is similar to (i). Here $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)|$ is equal to the number of solutions to the equation $x_1\cdots x_d\, a_1^2\cdots a_g^2 = 1$ $(a_i, b_i \in G, x_i \in C_i)$. Now argue as above, using Lemma 3.1(iii). ■

The next result determines the precise behaviour of $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|$ when Γ is Fuchsian and the classes C_i are almost homogeneous.

Theorem 3.3 *Let Γ be a proper Fuchsian group, and let $\mu = \mu(\Gamma) > 0$. For $1 \le i \le d$ let C_i be a conjugacy class in S_n with cycle-shape $(m_i^{a_i}, 1^{f_i})$, where the f_i are bounded and $\prod \mathrm{sgn}(C_i) = 1$. Then*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| = (n!)^{vg-1}|C_1|\cdots|C_d|\cdot(2 + O(n^{-\mu})).$$

Moreover, if all the classes C_i lie in A_n then

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, A_n)| = (n!/2)^{vg-1}|C_1|\cdots|C_d|\cdot(1 + O(n^{-\mu})).$$

Proof This follows by combining Proposition 3.2 with Theorem 2.15 for S_n, and Corollary 2.16 for A_n. (In both cases we take $l = vg$.) ■

To derive the asymptotics of the expressions in Theorem 3.3, we need the following lemma on the size of an almost homogeneous class in S_n.

Lemma 3.4 *Let $m \ge 2$ and $f \ge 0$ be fixed integers, and let $\pi \in S_n$ have cycle-shape $(m^a, 1^f)$. Then*

$$|\pi^{S_n}| \sim (n!)^{1-\frac{1}{m}} \cdot n^{\frac{f}{m}-\frac{1}{2}(1-\frac{1}{m})}.$$

Proof Using Stirling's formula we have

$$|\pi^{S_n}| = \frac{n!}{m^a a! f!} \sim \frac{n^{1/2}(n/e)^n}{m^a a^{1/2}(a/e)^a} = \frac{n^{1/2}(n/e)^n}{a^{1/2}(\frac{n-f}{e})^{\frac{n-f}{m}}}.$$

Now $(\frac{n}{n-f})^{n-f} = (1+\frac{f}{n-f})^{n-f} < e^f$, hence $(\frac{n-f}{e})^{\frac{n-f}{m}} \sim (n/e)^{\frac{n-f}{m}}$, and

$$|\pi^{S_n}| \sim \frac{n^{1/2}(n/e)^n}{((n-f)/m)^{1/2}(n/e)^{\frac{n-f}{m}}} \sim (\frac{n}{e})^{n(1-\frac{1}{m})+\frac{f}{m}} \sim (n!)^{1-\frac{1}{m}} \cdot n^{\frac{f}{m}-\frac{1}{2}(1-\frac{1}{m})},$$

as required. ■

We can now deduce

Theorem 3.5 *In the notation of Theorem* 3.3, *we have*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| \sim (n!)^{\mu+1} \cdot n^{\sum \frac{f_i}{m_i} - \frac{1}{2}(1-\frac{1}{m_i})}.$$

The same holds for $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, A_n)|$ *provided all the classes* C_i *lie in* A_n.

Proof Combining Theorem 3.3 with Lemma 3.4, we obtain

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| \sim (n!)^{vg-1+\sum(1-\frac{1}{m_i})} \cdot n^{\sum \frac{f_i}{m_i} - \frac{1}{2}(1-\frac{1}{m_i})}.$$

The result follows for S_n. The argument for A_n is similar. ■

Corollary 3.6 *Let* Γ *be a Fuchsian group, and let* b *be any fixed real number. Then for sufficently large* n *we have*

$$|\mathrm{Hom}(\Gamma, S_n)| \geq |\mathrm{Hom}(\Gamma, A_n)| \geq (n!)^{\mu+1} \cdot n^b.$$

Proof The proof for Γ improper was already given in (11) and the remarks following it. For Γ proper, the result follows from Theorem 3.5, taking the f_i fixed, but as large as we want. ■

We now turn to proving upper bounds for $|\mathrm{Hom}(\Gamma, S_n)|$.

Theorem 3.7 *Let* Γ *be a Fuchsian group. Let* $m = max(1, m_1, \ldots, m_d)$, *and set* $\gamma = 1 - \frac{1}{2m}$. *Then there is a constant* c *depending on* Γ *such that*

(i) $|\mathrm{Hom}(\Gamma, S_n)| \leq (n!)^{\mu+1} c^{n^\gamma}$ *for all* n;

(ii) *if* $g \geq 1$ *(*$g \geq 2$ *in the non-oriented case), then*

$$|\mathrm{Hom}(\Gamma, S_n)| \leq (n!)^{\mu+1} c^{\sqrt{n}} \text{ for all } n.$$

Moreover, in both cases we may take $c = c_0^{d+1}$, *where* $c_0 = c_0(m)$ *depends only on* m.

Proof The case where Γ is improper is covered by (11) and the remarks following it.

Now assume Γ is proper. We start with the oriented case; so suppose Γ is as in (1.1). Obviously, $|\mathrm{Hom}(\Gamma, S_n)| = \sum_{\mathbf{C}} |\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|$, where the sum is over all $\mathbf{C} = (C_1, \ldots, C_d)$ such that each C_i is a conjugacy class in S_n of elements of order dividing m_i. By Proposition 3.2(i) this yields

$$|\mathrm{Hom}(\Gamma, S_n)| = \sum_{\mathbf{C}} (n!)^{2g-1} |C_1| \cdots |C_d| \sum_{\chi \in Irr(S_n)} \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+2g}}. \qquad (14)$$

By Theorem 2.14, for all i and $\chi \in Irr(S_n)$ we have

$$|C_i| \cdot |\chi(g_i)| < (n!)^{1-\frac{1}{m_i}} \cdot \chi(1)^{1/m_i} \cdot c_i^{n^{1-\frac{1}{2m_i}}},$$

where $c_i = c_i(m_i)$. Hence

$$|\mathrm{Hom}(\Gamma, S_n)| \leq (n!)^{2g-1} \sum_{\mathbf{C},\chi} \frac{\prod_1^d ((n!)^{1-\frac{1}{m_i}} \cdot \chi(1)^{1/m_i} \cdot c_i^{n^{1-\frac{1}{2m_i}}})}{\chi(1)^{d-2+2g}}$$

$$\leq (n!)^{\mu+1} c_0^{dn^{\gamma}} \sum_{\mathbf{C}} \sum_{\chi} \chi(1)^{-\mu},$$

where $c_0 = \max c_i$ depends only on m. Observe that since the orders m_i are given, the number of possiblities for $\mathbf{C}$ is at most n^a, where $a = a(m)$. Also by Theorem 2.6, $\sum_{\chi} \chi(1)^{-\mu} = 2 + O(n^{-\mu})$. Therefore, replacing c_0 by a larger constant (still depending only on m), we have

$$|\mathrm{Hom}(\Gamma, S_n)| \leq (n!)^{\mu+1} c_0^{(d+1)n^{\gamma}}$$

(the $d+1$ factor replacing d to accomodate the case where $d = 0$). This proves part (i) in the oriented case.

Now assume $g \geq 1$ (still in the oriented case). Observe that

$$\sum_{\chi \in Irr(S_n)} \frac{|\chi(g_1) \cdots \chi(g_d)|}{\chi(1)^{d-2+2g}} \leq \sum_{\chi} \chi(1)^{-2+2g}. \qquad (15)$$

Since $g \geq 1$ the last sum is at most $p(n)$. We clearly have

$$\sum_{\mathbf{C}} |C_1| \cdots |C_d| = \prod_1^d j_{m_i}(S_n).$$

Hence by (14),

$$|\mathrm{Hom}(\Gamma, S_n)| \leq p(n)(n!)^{2g-1} \sum_{\mathbf{C}} |C_1| \cdots |C_d|$$

$$= p(n)(n!)^{2g-1}\prod_{i=1}^{d} j_{m_i}(S_n).$$

Since by Lemma 2.17 we have $j_{m_i}(S_n) \sim (n!)^{1-\frac{1}{m_i}} \cdot E(n,m_i)$, and both $p(n)$ and $E(n,m_i)$ are bounded by $c_0^{\sqrt{n}}$, where $c_0 = c_0(m)$, this gives

$$|\mathrm{Hom}(\Gamma, S_n)| \leq (n!)^{\mu+1} c_0^{(d+1)\sqrt{n}},$$

proving (ii).

The non-oriented case is very similar, using Proposition 3.2(ii), and is left to the reader. ■

When the genus is at least 2, we can prove a much more precise result. Recall from the Introduction that d^* is the number of m_i which are even.

Theorem 3.8 *Let Γ be a proper Fuchsian group, and suppose that $g \geq 2$ ($g \geq 3$ in the non-oriented case). Then*

(i) $|\mathrm{Hom}(\Gamma, A_n)| = (1 + O(n^{-(vg-2)}) \cdot (\frac{n!}{2})^{vg-1} \prod_{i=1}^{d} j_{m_i}(A_n)$.

(ii) $|\mathrm{Hom}(\Gamma, S_n)| = (h + O(n^{-(vg-2)}) \cdot (n!)^{vg-1} \prod_{i=1}^{d} j_{m_i}(S_n)$*, where* $h = 1$ *if* $d^* > 0$*, and* $h = 2$ *if* $d^* = 0$.

(iii) $|\mathrm{Hom}(\Gamma, S_n)| \sim |\mathrm{Hom}(\Gamma, A_n)| \sim (n!)^{\mu+1} \cdot \prod_{i=1}^{d} E(n, m_i)$.

Proof We shall give the proof only for the case where Γ is oriented. The non-oriented case is similar and is left to the reader.

As before, $|\mathrm{Hom}(\Gamma, A_n)| = \sum_{\mathbf{C}} |\mathrm{Hom}_{\mathbf{C}}(\Gamma, A_n)|$, where the sum is over all $\mathbf{C} = (C_1, \ldots, C_d)$ such that each C_i is a conjugacy class in A_n of elements of order dividing m_i. Hence by Proposition 3.2(i),

$$|\mathrm{Hom}(\Gamma, A_n)| = \sum_{\mathbf{C}} (\frac{n!}{2})^{2g-1} |C_1| \cdots |C_d| \sum_{\chi \in Irr(A_n)} \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+2g}}. \qquad (16)$$

Each term $\frac{|\chi(g_1)\cdots\chi(g_d)|}{\chi(1)^{d-2+2g}} \leq \chi(1)^{-(2g-2)}$. Since $g \geq 2$ we have $2g-2 \geq 2$, and hence by Corollary 2.7,

$$\sum_{\chi \in Irr(A_n)} \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+2g}} = 1 + O(n^{-(2g-2)}).$$

It follows that

$$|\mathrm{Hom}(\Gamma, A_n)| = (1 + O(n^{-(2g-2)})) \cdot (\frac{n!}{2})^{2g-1} \cdot \sum_{\mathbf{C}} |C_1| \cdots |C_d|$$

$$= (1 + O(n^{-(2g-2)})) \cdot (\frac{n!}{2})^{2g-1} \cdot \prod_{i=1}^{d} j_{m_i}(A_n),$$

giving (i).

For part (ii), assume first that $d^* = 0$; in other words, all m_i are odd. Then by Theorem 2.6 and the assumption $g \geq 2$, we have

$$\sum_{\chi \in Irr(S_n)} \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+2g}} = 2 + O(n^{-(2g-2)}),$$

and so (14) gives the conclusion as above.

Now assume $d^* > 0$. Then $\sum_{\chi \in Irr(S_n)} \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+2g}}$ is $2 + O(n^{-(2g-2)})$ if $g_1 \cdots g_d \in A_n$, and is $O(n^{-(2g-2)})$ if $g_1 \cdots g_d \notin A_n$. By Lemma 2.18, given $g_i^{m_i} = 1$, the probability that $g_1 \cdots g_d$ lies in A_n is $\frac{1}{2} + O(e^{-n^\delta})$ for some $\delta > 0$, and the conclusion follows from (14) again.

Finally, (iii) follows from (i) and (ii), together with 2.17 and 2.18. ■

The proofs of Theorems 1.2 and 1.12(i) are now complete.

It is now easy to deduce the following result, which will be used in the proof of Theorem 1.12(vi).

Corollary 3.9 *Under the hypotheses of Theorem* 3.8*, the probability that a random homomorphism in* $\mathrm{Hom}(\Gamma, S_n)$ *has image contained in* A_n *is equal to* $2^{-(vg+d^*-1)} + O(n^{-(vg-2)})$ *if* $d^* > 0$*, and is equal to* $2^{-vg} + O(n^{-(vg-2)})$ *if* $d^* = 0$.

Proof The probability in question is $\frac{|\mathrm{Hom}(\Gamma,A_n)|}{|\mathrm{Hom}(\Gamma,S_n)|}$. Hence the result follows from Theorem 3.8 and Lemma 2.18. ■

4 Subgroup growth

In this section we prove Theorems 1.4 and 1.12(iii). Let Γ be a Fuchsian group. If Γ is improper then it is a free product of cyclic groups, and precise estimates on the subgroup growth of Γ are known by [40, 36] and imply Theorem 1.4 and also the conclusion of 1.12(iii).

For completeness and for use in later sections, we include improper groups in our results, although most of the work is taken up with the main case, where Γ is proper.

Recall from the Introduction that $a_n(\Gamma) = |\mathrm{Hom}_{trans}(\Gamma, S_n)|/(n-1)!$. Using Theorem 3.7(i) we have

$$|\mathrm{Hom}_{trans}(\Gamma, S_n)| \leq |\mathrm{Hom}(\Gamma, S_n)| \leq (n!)^{\mu+1} \cdot c^{n^\gamma}$$

where $\gamma < 1$ and c are constants, and so

$$a_n(\Gamma) \leq (n!)^{\mu} \cdot c_1^{n^\gamma}. \tag{17}$$

Moreover, we may take c_1 to be of the form $c_0(m)^{d+1}$.

The idea for proving the lower bound is probabilistic: we show that for almost homogeneous classes $C_1, \ldots, C_d$ with elements of orders $m_1, \ldots, m_d$, almost all homomorphisms in $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ lie in $\mathrm{Hom}_{trans}(\Gamma, S_n)$ (where $\mathbf{C} = (C_1, \ldots, C_d)$). To do this we need some preparations.

Lemma 4.1 *Let $M = S_k \times S_{n-k} < S_n$ $(1 \leq k \leq n/2)$, and fix an integer $m \geq 2$. Then there is a constant c such that for all n we have*

$$\frac{j_m(M)}{j_m(S_n)} \leq \binom{n}{k}^{-(1-\frac{1}{m})} c^{\sqrt{k}}.$$

Proof Write $l = n-k$, so that $j_m(M) = j_m(S_k)j_m(S_l)$. Using Lemma 2.17, we have

$$\begin{aligned}\frac{j_m(M)}{j_m(S_n)} &\sim \frac{(k!\,l!)^{1-1/m}E(k,m)E(l,m)}{(n!)^{1-1/m}E(n,m)} \\ &\leq \binom{n}{k}^{-(1-\frac{1}{m})} \cdot E(k,m).\end{aligned}$$

Note that $E(k,m) < c^{\sqrt{k}}$. The result follows. ■

Lemma 4.2 *Let $M = S_k \times S_{n-k} < S_n$ $(1 \leq k \leq n/2)$, and fix integers $m \geq 2$, $f \geq 0$. Let C be a conjugacy class of S_n with cycle-shape $(m^a, 1^f)$. Then there is a constant c such that*

$$\frac{|C \cap M|}{|C|} \leq c \binom{n}{k}^{-(1-\frac{1}{m})}.$$

Proof Write $l = n-k$. By Lemma 3.4, $|C| \sim (n!)^{1-\frac{1}{m}} \cdot n^{\frac{f}{m} - \frac{1}{2}(1-\frac{1}{m})}$. Writing $C = C(n,m,f)$, we have

$$|C \cap M| = \sum_{f_1+f_2=f} |C(k,m,f_1)| \cdot |C(l,m,f_2)|$$

$$\leq \sum_{f_1+f_2=f} (k!)^{1-\frac{1}{m}} k^{\frac{f_1}{m}-\frac{1}{2}(1-\frac{1}{m})} \cdot (l!)^{1-\frac{1}{m}} l^{\frac{f_2}{m}-\frac{1}{2}(1-\frac{1}{m})}$$

$$\leq (f+1)(k!\,l!)^{1-\frac{1}{m}} n^{\frac{f}{m}} (kl)^{-\frac{1}{2}(1-\frac{1}{m})}.$$

Hence

$$\frac{|C\cap M|}{|C|} \leq (f+1)\binom{n}{k}^{-(1-\frac{1}{m})} (\frac{n}{kl})^{\frac{1}{2}(1-\frac{1}{m})} \leq c\binom{n}{k}^{-(1-\frac{1}{m})},$$

where $c = 2(f+1)$. ■

For $1 \leq i \leq d$ let C_i be a conjugacy class in S_n with cycle-shape $(m_i^{a_i}, 1^{f_i})$, where the f_i are bounded and $\prod_{i=1}^d \mathrm{sgn}(C_i) = 1$. Write $\mathbf{C} = (C_1, \ldots, C_d)$. For a subgroup M of S_n, we let $\mathrm{Hom}_{\mathbf{C}}(\Gamma, M)$ denote the set of those $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ satisfying $\phi(\Gamma) \subseteq M$.

Lemma 4.3 *There is a constant c such that for every k with $1 \leq k \leq n/2$, and any k-subset stabilizer $M \cong S_k \times S_{n-k}$, we have*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, M)| < c|M|^{vg-1+s+t} \prod_{i=1}^d |C_i \cap M|.$$

Proof Writing $l = n-k$ and $C_i = C_i(n, m_i, f_i)$, we have

$$C_i \cap M = \bigcup_{f_{i1}+f_{i2}=f_i} C(k, m_i, f_{i1}) \times C(l, m_i, f_{i2}).$$

This enables us to present $\mathrm{Hom}_{\mathbf{C}}(\Gamma, M)$ as a disjoint union of direct products $\mathrm{Hom}_{\mathbf{K}}(\Gamma, S_k) \times \mathrm{Hom}_{\mathbf{L}}(\Gamma, S_l)$, where $\mathbf{K}, \mathbf{L}$ range over a bounded number of d-tuples of almost homogeneous classes in S_k and S_l respectively.

It follows from Theorem 3.3 if $s+t=0$, and from (13) if $s+t>0$, that for a suitable constant c we have

$$|\mathrm{Hom}_{\mathbf{K}}(\Gamma, S_k)| \leq c(k!)^{vg-1+s+t} \prod_{i=1}^d |K_i|,$$

and

$$|\mathrm{Hom}_{\mathbf{L}}(\Gamma, S_l)| \leq c(l!)^{vg-1+s+t} \prod_{i=1}^d |L_i|.$$

Applying this and the above decomposition of $\mathrm{Hom}_{\mathbf{C}}(\Gamma, M)$ we easily see that, for some constant c_1 we have

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, M)| \leq c_1(k!\,l!)^{vg-1+s+t} \prod_{i=1}^d |C_i \cap M|.$$

The result follows. ■

Theorem 4.4 *With* $\mathbf{C}$ *as above, the probability that a random homomorphism* $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ *has a transitive image tends to* 1 *as* $n \to \infty$*. Moreover, this probability is of the form* $1 - O(n^{-\mu})$*, where* $\mu = \mu(\Gamma)$*. The same holds for* $\mathrm{Hom}_{\mathbf{C}}(\Gamma, A_n)$*, assuming that the classes* C_i *all lie in* A_n*.*

Proof For $1 \leq k \leq n/2$, let $M \cong S_k \times S_l < S_n$ be the stabilizer of a k-subset, where $l = n - k$. If Q is the probability that a random $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ has intransitive image, then

$$Q \leq \sum_M \frac{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, M)|}{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|},$$

where M ranges over all stabilizers of subsets of size between 1 and $n/2$.

Now, combining Theorem 3.3 and (13) with the preceding lemma, we obtain

$$\frac{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, M)|}{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|} \leq c_1 |G : M|^{-(vg-1+s+t)} \prod_{i=1}^{d} \frac{|C_i \cap M|}{|C_i|}$$

$$\leq c_2 |G : M|^{-(vg-1+s+t)} \prod_{i=1}^{d} \binom{n}{k}^{-(1-\frac{1}{m_i})} = c_2 \binom{n}{k}^{-(\mu+1)}.$$

Summing over k, noting that there are $\binom{n}{k}$ stabilizers of k-subsets, we see that

$$Q \leq c_2 \sum_{1 \leq k \leq n/2} \binom{n}{k}^{-\mu} = O(n^{-\mu}).$$

This completes the proof for S_n. The argument for A_n is entirely similar. ■

Corollary 4.5 *For any constant* b *and for all sufficiently large* n *we have*

$$|\mathrm{Hom}_{trans}(\Gamma, S_n)| \geq |\mathrm{Hom}_{trans}(\Gamma, A_n)| \geq (n!)^{\mu+1} \cdot n^b.$$

Proof By Theorem 4.4, it follows that

$$|\mathrm{Hom}_{trans}(\Gamma, S_n)| \geq (1 - O(n^{-\mu})) |\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|, \tag{18}$$

where $\mathbf{C}$ is as above. Applying Theorem 3.5 with the f_i fixed, but arbitrarily large, the result follows for S_n. The same argument works for A_n. ■

This, combined with the upper bound (17), proves our main result on subgroup growth:

Theorem 4.6 (i) *For every constant* b *and for all sufficiently large* n *we have* $a_n(\Gamma) \geq (n!)^{\mu} \cdot n^b$*.*

(ii) *There is a constant* c *such that for all* n *we have* $a_n(\Gamma) \leq (n!)^{\mu} \cdot c^{n^{\gamma}}$*, where* $\gamma = 1 - \frac{1}{2m}$ *(*$m = max(1, m_1, \ldots, m_d)$*). We can take* $c = c_0(m)^{d+1}$*.*

In particular it follows that $a_n(\Gamma) = (n!)^{\mu+o(1)}$, proving Theorem 1.4.

To prove Theorem 1.12(iii), we need the following.

Theorem 4.7 *Let Γ be a Fuchsian group. If Γ is proper, assume that $g \geq 2$ ($g \geq 3$ in the non-oriented case). Then the probability that a random homomorphism $\phi \in \mathrm{Hom}(\Gamma, S_n)$ has transitive image tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O(n^{-\mu})$.*

Proof By Theorem 3.8(ii) for Γ proper, and using (10) for Γ improper, we have $|\mathrm{Hom}(\Gamma, S_n)| \sim (n!)^{vg+s+t-1} \prod_{i=1}^d j_{m_i}(S_n)$. Hence for $1 \leq k \leq n/2$, letting $M \cong S_k \times S_{n-k}$ be the stabilizer of a k-subset, we have

$$|\mathrm{Hom}(\Gamma, M)| \leq c|M|^{vg+s+t-1} \prod_{i=1}^{d} j_{m_i}(M).$$

Thus if Q is the probability that a random $\phi \in \mathrm{Hom}(\Gamma, S_n)$ has intransitive image, then

$$Q \leq \sum_M \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, S_n)|} \leq \sum_{k=1}^{n/2} \binom{n}{k} \frac{|\mathrm{Hom}(\Gamma, S_k \times S_{n-k})|}{|\mathrm{Hom}(\Gamma, S_n)|}$$

$$\leq \sum_{k=1}^{n/2} \binom{n}{k}^{-(vg+s+t-2)} \prod_{i=1}^{d} \frac{j_{m_i}(S_k \times S_{n-k})}{j_{m_i}(S_n)}.$$

Applying Lemma 4.1, this gives

$$Q \leq \sum_{k=1}^{n/2} \binom{n}{k}^{-(vg+s+t-2)-\sum(1-\frac{1}{m_i})} \cdot c^{\sqrt{k}} = O(n^{-\mu}),$$

completing the proof. ∎

It follows that $|\mathrm{Hom}_{trans}(\Gamma, S_n)| \sim |\mathrm{Hom}(\Gamma, S_n)|$ under the hypotheses of Theorem 1.12, and hence Theorem 1.12(iii) follows from 1.12(i).

We shall also need the following slight variant of Theorem 4.7.

Theorem 4.8 *Assume the hypotheses of Theorem 4.7. Then the probability that a random homomorphism $\phi \in \mathrm{Hom}(\Gamma, A_n)$ has transitive image tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O(n^{-\mu})$.*

Proof By 3.8 and (12), there is a constant $c > 0$ such that $|\mathrm{Hom}(\Gamma, A_n)| > c|\mathrm{Hom}(\Gamma, S_n)|$ for all n. Hence the result follows from Theorem 4.7. ∎

5 Maximal subgroup growth

In this section we prove Theorem 1.5, showing that almost all index n subgroups of a Fuchsian group are maximal. It is interesting to note that our proof of this for a given Fuchsian group requires our subgroup growth results for all Fuchsian groups.

For a group Γ as in (1.1) or (1.2) write $\gamma(\Gamma) = 1 - \frac{1}{2m}$ where $m = m(\Gamma) = \max(1, m_1, \ldots, m_d)$. Set also $d(\Gamma) = d$ (the number of elliptic generators).

We shall need the following result.

Proposition 5.1 *Let Γ be a Fuchsian group, and let Γ_0 be a subgroup of finite index in Γ. Then*

(i) Γ_0 *is also a Fuchsian group,*

(ii) $\mu(\Gamma_0) = |\Gamma : \Gamma_0| \cdot \mu(\Gamma)$,

(iii) $m(\Gamma_0) \leq m(\Gamma)$ *and* $\gamma(\Gamma_0) \leq \gamma(\Gamma)$,

(iv) $d(\Gamma_0) \leq |\Gamma : \Gamma_0| \cdot d(\Gamma)$.

Proof Part (i) is obvious from the geometric definition of Fuchsian groups. Part (ii) for proper Fuchsian groups is [33, III.7.9, p.140]; the improper case is covered by the remarks following that result. Next, (iii) follows from the well known fact that every non-identity torsion element of Γ is conjugate to a power of one of the elliptic generators x_i (so m above is equal to the maximal order of a torsion element of Γ). Finally, part (iv) follows from the description of possible signatures of subgroups of given index in Γ in [45, Theorem 1]. ■

We shall also need the following easy observation concerning indices of wreath product subgroups.

Lemma 5.2 *Let k, n be positive integers such that $k|n$ and $1 < k < n$. Set* $i(n,k) = \frac{n!}{k!((n/k)!)^k}$.

(i) $i(n,k) \geq 2^n \cdot cn^{-1/2}$, *where $c > 0$ is an absolute constant.*

(ii) *Fix ϵ with $0 < \epsilon < 1$. If $k \geq n^\epsilon$ then $i(n,k) \geq (n!)^{\epsilon/2}$ for all sufficiently large n.*

Proof Part (i) is well known and easy. For (ii), observe that by Stirling's formula we have

$$i(n,k) \sim \frac{(n/k)^{\frac{1}{2}(1+k)} e^k k^n}{n^k} \geq \frac{k^n}{n^k}.$$

Set $j(n,k) = \frac{k^n}{n^k}$. The function x^n/n^x increases for $2 \leq x \leq \frac{n}{\log n}$ and decreases for $\frac{n}{\log n} < x \leq n/2$. Hence, for $k \geq n^\epsilon$ we have $j(n,k) \geq$

$\min\{j(n,n^\epsilon), j(n,n/2)\}$, which is easily seen to be at least $(n!)^{\epsilon/2}$ for large n. ■

We now prove Theorem 1.5.

Recall that $m_n(\Gamma)$ denotes the number of index n maximal subgroups of Γ. We estimate below the number $a_n(\Gamma) - m_n(\Gamma)$ of non-maximal index n subgroups. If H is such a subgroup, then there exists $k|n$ with $1 < k < n$ and an index k subgroup K of Γ such that $H < K$. Given such k, the number of choices for K is $a_k(\Gamma)$, which is bounded above by $(k!)^{\mu(\Gamma)} c^{(d(\Gamma)+1)k^{\gamma(\Gamma)}}$ by Theorem 4.6, where $c = c(m(\Gamma))$. Given K, the number of choices for our subgroup H is $a_{n/k}(K)$, which is bounded above by $((n/k)!)^{\mu(K)} c_1^{(d(K)+1)(n/k)^{\gamma(K)}}$, where $c_1 = c_1(m(K))$. By Proposition 5.1 we have $m(K) \leq m(\Gamma)$, so we may take $c_1 = c$. The same proposition also gives $\mu(K) = k\mu(\Gamma)$, $\gamma(K) \leq \gamma(\Gamma)$ and $d(K) \leq kd(\Gamma)$. Hence, setting $\mu = \mu(\Gamma)$, $\gamma = \gamma(\Gamma)$ and $d = d(\Gamma)$, we obtain

$$a_n(\Gamma) - m_n(\Gamma) \leq \sum_{k|n, 1<k<n} (k!(n/k)!^k)^\mu \cdot c^{(d+1)k^\gamma + (kd+1)(n/k)^\gamma}.$$

Using the lower bound $a_n(\Gamma) \geq (n!)^\mu$ which holds for all large n by Theorem 4.6, and letting $i(n,k)$ be as in Lemma 5.2 this gives

$$\frac{a_n(\Gamma) - m_n(\Gamma)}{a_n(\Gamma)} \leq \sum_{k|n, 1<k<n} i(n,k)^{-\mu} \cdot c^{(d+1)k^\gamma + (kd+1)(n/k)^\gamma}.$$

Let $\epsilon = 1 - \gamma$. We divide the sum above into two parts Σ_1, Σ_2, over $k < n^\epsilon$ and $k \geq n^\epsilon$ respectively. Note that for $k < n^\epsilon$ we have

$$(d+1)k^\gamma + (kd+1)(n/k)^\gamma \leq (d+1)(n^\gamma + n^{1-\gamma+\gamma^2}) \leq c_2 n^{\gamma'},$$

where $\gamma' = 1 - \gamma + \gamma^2 < 1$ and $c_2 = 2(d+1)$. Using part (i) of Lemma 5.2 this yields

$$\Sigma_1 \leq c^{c_2 n^{\gamma'}} \sum_{1<k<n^\epsilon} (2^n c_3 n^{-1/2})^{-\mu} \leq \frac{1}{2} c_4^{-n},$$

for any constant c_4 satisfying $1 < c_4 < 2^\mu$ and sufficiently large n.

To bound Σ_2 note that, for all k we have

$$(d+1)k^\gamma + (kd+1)(n/k)^\gamma \leq c_2 n$$

with c_2 as above. Now part (ii) of Lemma 5.2 yields

$$\Sigma_2 \leq c^{c_2 n} \sum_{n^\epsilon \leq k < n} ((n!)^{\epsilon/2})^{-\mu} \leq \frac{1}{2} c_4^{-n},$$

for all sufficiently large n (where c_4 is as above).

Altogether it follows that if n is large enough, then

$$\frac{a_n(\Gamma) - m_n(\Gamma)}{a_n(\Gamma)} \leq \Sigma_1 + \Sigma_2 \leq c_4^{-n}.$$

This completes the proof of Theorem 1.5.

The following is an equivalent version of Theorem 1.5, which we shall use in the sequel.

Corollary 5.3 *If Γ is a Fuchsian group, then the probability that a randomly chosen $\phi \in \mathrm{Hom}_{trans}(\Gamma, S_n)$ has primitive image tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O(c^{-n})$ for some constant $c > 1$.*

We shall also need the corresponding statement for A_n:

Corollary 5.4 *If Γ is a Fuchsian group, then the probability that a randomly chosen $\phi \in \mathrm{Hom}_{trans}(\Gamma, A_n)$ has primitive image is $1 - O(c^{-n})$, where $c > 1$.*

Proof The proof is very similar to that of Theorem 1.5. Define $a'_n(\Gamma)$ to be the number of index n subgroups H of Γ such that the permutation representation of Γ on Γ/H maps Γ into A_n, and let $m'_n(\Gamma)$ denote the number of maximal such subgroups. It is enough to show that $\frac{a'_n(\Gamma)-m'_n(\Gamma)}{a'_n(\Gamma)} \leq c^{-n}$ for some $c > 1$. Note that $a'_n(\Gamma) - m'_n(\Gamma) \leq a_n(\Gamma) - m_n(\Gamma)$ (since the left hand side is the number of non-maximal index n subgroups with an etxra property). Also

$$a'_n(\Gamma) \geq |\mathrm{Hom}_{trans}(\Gamma, A_n)|/(n-1)! \geq (n!)^{\mu} \cdot n$$

for sufficiently large n, by 4.5. Hence the proof above carries over to show that

$$\frac{a'_n(\Gamma) - m'_n(\Gamma)}{a'_n(\Gamma)} \leq c^{-n},$$

yielding the conclusion. ■

Note that in 5.3 and 5.4, any constant c with $1 < c < 2^{\mu}$ will do.

Define $\mathrm{Hom}_{prim}(\Gamma, S_n)$ to be the set of homomorphisms $\phi : \Gamma \to S_n$ such that $\phi(\Gamma)$ is primitive, and define $\mathrm{Hom}_{prim}(\Gamma, A_n)$ similarly.

Corollary 5.5 *If Γ is a Fuchsian group, then for any b and for sufficiently large n,*

$$|\mathrm{Hom}_{prim}(\Gamma, S_n)| \geq |\mathrm{Hom}_{prim}(\Gamma, A_n)| \geq (n!)^{\mu+1} \cdot n^b.$$

Proof This follows from the previous result, combined with Corollary 4.5. ■

6 Random quotients I: Higman's conjecture

In this section we prove Theorems 1.6, 1.7 and deduce Higman's conjecture (Corllary 1.8). Unlike all previous proofs, we make use of the classification of finite simple groups through Lemma 6.1(ii) below.

While our proof works equally well for proper and improper Fuchsian groups, these results for improper groups (i.e. free products of cyclic groups) are essentially known - see [12] for the case of free groups, and [28, 2.4,5.1] for $Z_p * Z_q$ with p, q primes not both 2 (and the same proof applies for any free product of finite cyclic groups). Extensions of this to free products of arbitrary finite groups have been announced by Müller and Pyber.

We begin with Theorem 1.6. We shall need the following known result about primitive subgroups of S_n.

Lemma 6.1 (i) *If M is a primitive subgroup of S_n not containing A_n, then $|M| < 4^n$.*

(ii) *The number of conjugacy classes of primitive maximal subgroups in A_n or S_n is at most $n^{6/11+o(1)}$.*

Proof Part (i) follows from [41], and part (ii) from [27, 4.3], together with the proof of [27, 4.4] (taking into account maximal subgroups of A_n as well as S_n). ■

Lemma 6.2 *If Γ is a Fuchsian group, then the probability that a randomly chosen $\phi \in \mathrm{Hom}_{prim}(\Gamma, S_n)$ has image A_n or S_n tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O((n!)^{-\mu'})$ for any $\mu' < \mu$.*

Proof Denote by $\mathcal{M}_{prim}$ a set of conjugacy classes representatives of maximal primitive subgroups of A_n or S_n, not including A_n itself. Let Q be the probability that a randomly chosen $\phi \in \mathrm{Hom}_{prim}(\Gamma, S_n)$ has $\phi(\Gamma) \not\supseteq A_n$. Since each $M \in \mathcal{M}_{prim}$ has $|S_n : M|$ conjugates, we obtain

$$Q \leq \sum_{M \in \mathcal{M}_{prim}} |S_n : M| \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}_{prim}(\Gamma, S_n)|}.$$

By Corollary 5.5, we have, for large n,

$$|\mathrm{Hom}_{prim}(\Gamma, S_n)| \geq (n!)^{\mu+1}.$$

Noting that Γ can be generated by $r = d + vg + s + t$ elements, and using Lemma 6.1(i), we see that

$$Q \leq \sum_{M \in \mathcal{M}_{prim}} \frac{|S_n : M| \cdot |M|^r}{(n!)^{\mu+1}} \leq \sum_{M \in \mathcal{M}_{prim}} \frac{|M|^{r-1}}{(n!)^{\mu}} \leq |\mathcal{M}_{prim}| \cdot \frac{4^{n(r-1)}}{(n!)^{\mu}}.$$

Now $|\mathcal{M}_{prim}| < n$ for large n by Lemma 6.1(ii), and so it follows that $Q = O((n!)^{-\mu'}$ for any $\mu' < \mu$, proving the result. ■

It now follows from Corollary 5.3 and Lemma 6.2 that the probability that a random homomorphism in $\mathrm{Hom}_{trans}(\Gamma, S_n)$ has image A_n or S_n is $(1 - O(c^{-n})) \cdot (1 - O((n!)^{-\mu'}))$ for any $\mu' < \mu$, and taking $\mu' > 0$, this is $1 - O(c^{-n})$. This completes the proof of Theorem 1.6.

The following corollary is immediate.

Corollary 6.3 *If Γ is a Fuchsian group, and n is sufficiently large, then Γ surjects onto either A_n or S_n.*

We now deduce Theorem 1.7, and hence Higman's conjecture (Corollary 1.8).

Lemma 6.4 *If Γ is a Fuchsian group, then the probability that a randomly chosen $\phi \in \mathrm{Hom}_{prim}(\Gamma, A_n)$ is an epimorphism tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O((n!)^{-\mu'})$ for any $\mu' < \mu$.*

Proof Denote by $\mathcal{M}'_{prim}$ a set of conjugacy classes representatives of maximal primitive subgroups of A_n, and let Q' be the probability that a randomly chosen $\phi \in \mathrm{Hom}_{prim}(\Gamma, A_n)$ satisfies $\phi(\Gamma) \neq A_n$. Then

$$Q' \leq \sum_{M \in \mathcal{M}'_{prim}} |A_n : M| \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}_{prim}(\Gamma, A_n)|}.$$

It now follows exactly as in the proof of Lemma 6.2 that $Q' = O((n!)^{-\mu'})$ for any $\mu' < \mu$. ■

Combining Lemma 6.4 with Corollary 5.4 completes the proof of Theorem 1.7 and of Higman's conjecture.

Now we prove parts (iv), (v) and (vi) of Theorem 1.12. Assume Γ is a Fuchsian group, and if Γ is proper assume $g \geq 2$ ($g \geq 3$ in the non-oriented case). In this case Theorem 4.7 shows that the probability that a random $\phi \in \mathrm{Hom}(\Gamma, S_n)$ have transitive image is $1 - O(n^{-\mu})$. Combining this with Theorem 1.6 yields part (iv) of Theorem 1.12. Likewise, part (v) follows from Theorems 4.8 and 1.7. Finally, Theorem 1.12(vi) follows from part (iv) together with Corollary 3.9 (for the proper case) and from (12) and the remarks following it (for the improper case).

7 Random quotients II: symmetric quotients

In this section we prove Theorems 1.9 and 1.10.

Let Γ be a Fuchsian group as in (1.1), (1.2). For $1 \leq i \leq d$ let C_i be a conjugacy class in S_n with cycle-shape $(m_i^{a_i}, 1^{f_i})$, where the f_i are bounded and $\prod_{i=1}^{d} \mathrm{sgn}(C_i) = 1$. Set $\mathbf{C} = (C_1, \ldots, C_d)$.

We already know by Theorem 4.4 that a randomly chosen $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ has transitive image with probability $1 - O(n^{-\mu})$. The main step in the proof of Theorem 1.9 is to show that the probability that ϕ has primitive image has the same form.

We need some notation. Define

$$\mathrm{Hom}_{\mathbf{C},trans}(\Gamma, S_n) = \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n) \cap \mathrm{Hom}_{trans}(\Gamma, S_n),$$

$$\mathrm{Hom}_{\mathbf{C},prim}(\Gamma, S_n) = \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n) \cap \mathrm{Hom}_{prim}(\Gamma, S_n),$$

$$\mathrm{Hom}_{trans,imp}(\Gamma, S_n) = \{\phi \in \mathrm{Hom}_{trans}(\Gamma, S_n) \ : \ \phi(\Gamma) \text{ imprimitive}\},$$

$$\mathrm{Hom}_{\mathbf{C},trans,imp}(\Gamma, S_n) = \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n) \cap \mathrm{Hom}_{trans,imp}(\Gamma, S_n).$$

Proposition 7.1 *The probability that a randomly chosen homomorphism in* $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ *has primitive image is* $1 - O(n^{-\mu})$.

Proof By Corollary 5.3, there is a constant $c_1 > 1$ such that

$$|\mathrm{Hom}_{trans,imp}(\Gamma, S_n)| \leq c_1^{-n} \cdot |\mathrm{Hom}_{trans}(\Gamma, S_n)|.$$

Theorem 3.7 then gives

$$|\mathrm{Hom}_{trans,imp}(\Gamma, S_n)| \leq c_1^{-n} \cdot |\mathrm{Hom}(\Gamma, S_n)| \leq c_1^{-n} \cdot c_2^{n^{\gamma}} \cdot (n!)^{\mu+1}, \qquad (19)$$

where $\gamma < 1$. Combining Theorems 4.4 and 3.5, we obtain

$$|\mathrm{Hom}_{\mathbf{C},trans}(\Gamma, S_n)| \geq (1 - o(1)) \cdot |\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| \geq n^{-c_3} \cdot (n!)^{\mu+1}, \quad (20)$$

for some constant c_3.

By (19) and (20), we have

$$\frac{|\mathrm{Hom}_{\mathbf{C},trans,imp}(\Gamma, S_n)|}{|\mathrm{Hom}_{\mathbf{C},trans}(\Gamma, S_n)|} \leq \frac{|\mathrm{Hom}_{trans,imp}(\Gamma, S_n)|}{|\mathrm{Hom}_{\mathbf{C},trans}(\Gamma, S_n)|} \leq c_1^{-n} \cdot c_2^{n^\gamma} \cdot n^{c_3} \leq c_4^{-n},$$

for some constant $c_4 > 1$. In other words, the probability that a random homomorphism in $\mathrm{Hom}_{\mathbf{C},trans}(\Gamma, S_n)$ has a primitive image is at least $1 - c_4^{-n}$. Combining this with Theorem 4.4 we obtain

$$\frac{|\mathrm{Hom}_{\mathbf{C},prim}(\Gamma, S_n)|}{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|} = \frac{|\mathrm{Hom}_{\mathbf{C},prim}(\Gamma, S_n)|}{|\mathrm{Hom}_{\mathbf{C},trans}(\Gamma, S_n)|} \cdot \frac{|\mathrm{Hom}_{\mathbf{C},trans}(\Gamma, S_n)|}{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|}$$

$$\geq (1 - c_4^{-n})(1 - O(n^{-\mu})) = 1 - O(n^{-\mu}).$$

The result follows. ■

Lemma 7.2 *The probability that a randomly chosen $\phi \in \mathrm{Hom}_{\mathbf{C},prim}(\Gamma, S_n)$ has image A_n or S_n tends to 1 as $n \to \infty$. Moreover, this probability is $1 - O((n!)^{-\mu'})$ for any $\mu' < \mu$.*

Proof The argument is similar to the proof of Lemma 6.2. Let $\mathcal{M}_{prim}$ be a set of conjugacy class representatives of maximal primitive subgroups of A_n or S_n. By Proposition 7.1 and Theorem 3.5 we have $|\mathrm{Hom}_{\mathbf{C},prim}(\Gamma, S_n)| \geq (n!)^{\mu+1} \cdot n^{-c}$ for some constant c. Hence, setting $r = d + vg + s + t$ and denoting by Q the probability that a random $\phi \in \mathrm{Hom}_{\mathbf{C},prim}(\Gamma, S_n)$ does not have image containing A_n, then

$$Q \leq \sum_{M \in \mathcal{M}_{prim}} |S_n : M| \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}_{\mathbf{C},prim}(\Gamma, S_n)|} \leq \sum_{M \in \mathcal{M}_{prim}} \frac{|S_n : M| \cdot |M|^r \cdot n^c}{(n!)^{\mu+1}}$$

$$= \sum_{M \in \mathcal{M}_{prim}} \frac{|M|^{r-1} \cdot n^c}{(n!)^\mu} = O((n!)^{-\mu'})$$

by Lemma 6.1, where μ' is any fixed number satisfying $0 < \mu' < \mu$. The result follows. ■

Combining this with Proposition 7.1 it follows that the probability that a random homomorphism $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ has image containing A_n is $(1 - O(n^{-\mu}))(1 - O((n!)^{-\mu'})) = 1 - O(n^{-\mu})$.

This completes the proof of Theorem 1.9.

We now turn to the proof of Theorem 1.10. Let Γ be as in the hypothesis of the theorem: so if $s+t=0$, then $(g,d^*) \neq (0,0),(0,1)$, and if $s+t=1$ then $(g,d^*) \neq (0,0)$. We divide the analysis into three cases:

Case 1 Γ is improper.

Case 2 Γ is proper and $d^* \geq 2$.

Case 3 Γ is proper and $d^* \leq 1$.

In each case we consider a suitable subspace X of $\mathrm{Hom}(\Gamma, S_n)$, and show that, for large n, a random homomorphism $\phi \in X$ has image S_n with positive probability.

Case 1 For this case the space X is $\mathrm{Hom}(\Gamma, S_n)$ itself. By Theorem 1.12(vi), the probability that a random homomorphism $\phi \in \mathrm{Hom}(\Gamma, S_n)$ satisfies $\phi(\Gamma) = S_n$ is equal to $1 - 2^{1-vg-d^*-s-t} + o(1)$. Note that, by our assumptions on Γ, $s+t \geq 1$, and if $s+t=1$ then $vg + d^* > 0$. Therefore this probability is at least $\frac{1}{2} - o(1)$, which is positive for large n.

Case 2 Since $d^* \geq 2$ there are distinct indices j,k such that m_j and m_k are even. Choose almost homogeneous classes C_i $(1 \leq i \leq d)$ in such a way that C_j and C_k are odd classes, and the rest of the classes are all contained in A_n. We may assume n is large, so that for $i \neq j,k$, the class C_i is also a conjugacy class in A_n. In this case our space X will be $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$, where $\mathbf{C} = (C_1, \ldots, C_d)$.

By the definition of X we have $\phi(\Gamma) \not\subseteq A_n$ for all $\phi \in X$. Theorem 1.9 now shows that $\phi(\Gamma) = S_n$ with probability tending to 1 as $n \to \infty$.

Case 3 Here $d^* \leq 1$ and so by our assumption on Γ we have $g > 0$. Choose C_i $(1 \leq i \leq d)$ to be almost homogeneous classes in A_n. Again we take our space $X = \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$.

Observe that by Theorem 3.3, we have

$$\frac{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, A_n)|}{|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|} = (\frac{1}{2})^{vg} + O(n^{-\mu}) \leq \frac{1}{2} + O(n^{-\mu}).$$

Combining this with Theorem 1.9, it follows that the probability that a random homomorphism $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ has image equal to S_n is at least $\frac{1}{2} + O(n^{-\mu})$, which implies Theorem 1.10.

This completes the proof of Theorem 1.10 (and hence of Corollary 1.11 as well).

8 Branched coverings of Riemann surfaces

In this section we prove Theorems 1.3 and 1.12(ii), as well as Theorem 1.13 and further related results.

We begin by expanding a little on the discussion in the preamble to Theorem 1.3 in the Introduction. Let Y be a compact connected Riemann surface of genus g, and let $y_1, \dots, y_d \in Y$ be fixed distinct points. The fundamental group $\Pi = \pi_1(Y \backslash \{y_1, \dots, y_d\})$ has presentation

$$\Pi = \langle x_i, a_j, b_j \, (1 \leq i \leq d, \, 1 \leq j \leq g) \mid x_1 \cdots x_d \, [a_1, b_1] \cdots [a_g, b_g] = 1 \rangle.$$

Topologically, index n coverings $X \to Y$ unramified outside $\{y_1, \dots, y_d\}$ are classified by conjugacy classes of homomorphisms $\Pi \to S_n$. Now, fixing the S_n-conjugacy classes $C_1, \dots, C_d$ of the monodromy elements around $y_1, \dots, y_d$ respectively, we see that the number of index n coverings with monodromy elements in these classes is equal to the number of solutions up to conjugacy of the equation

$$x_1 \cdots x_d \, [a_1, b_1] \cdots [a_g, b_g] = 1 \quad (x_i \in C_i, a_j, b_j \in S_n). \tag{21}$$

Let m_i be the order of the elements in C_i, and consider the group Γ as in (1.1) with $s = t = 0$. Then there is a bijection between solutions to (21) and homomorphisms $\phi \in \mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$.

Now, since a solution to (21) which corresponds to a covering $\pi : X \to Y$ has $n!/|\mathrm{Aut}\,\pi|$ conjugates it follows that

$$\sum_{\pi \in P(\mathbf{C}, n)} \frac{n!}{|\mathrm{Aut}\,\pi|} = |\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|.$$

This gives rise to the following formula for the Eisenstein number of coverings:

$$\sum_{\pi \in P(\mathbf{C}, n)} \frac{1}{|\mathrm{Aut}\,\pi|} = \frac{1}{n!} \cdot |\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|,$$

as stated in (1.3) of the Introduction.

Now part (i) of Theorem 1.3 (where the classes C_i are almost homogeneous) follows from Theorems 3.3 and 3.5.

To prove 1.3(ii), we sum over all $\mathbf{C} = (C_1, \dots, C_d)$ with C_i classes in S_n of elements of order dividing m_i, and obtain

$$\sum_{\pi \in P(\mathbf{m}, n)} \frac{1}{|\mathrm{Aut}\,\pi|} = \frac{1}{n!} \cdot |\mathrm{Hom}(\Gamma, S_n)|.$$

Now Theorem 1.3(ii) follows from Theorem 1.2, while Theorem 1.12(ii) follows from Theorem 3.8(iii).

We now turn to Theorem 1.13 and other probabilistic results on coverings. Let m_i, C_i be as above, and assume that $\mu = 2g-2+\sum(1-\frac{1}{m_i}) > 0$ (the hyperbolic case), and also that the classes C_i have cycle-shape $(m_i^{a_i}, 1^{f_i})$ with f_i bounded. Recall that we are viewing $P(\mathbf{m}, n)$ and $P(\mathbf{C}, n)$ as probability spaces, where the probability assigned to a covering π is proportional to $1/|\mathrm{Aut}\,\pi|$. This is the natural measure geometrically, and corresponds to the uniform distribution on $\mathrm{Hom}(\Gamma, S_n)$ and $\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)$ respectively. Note that the monodromy group $\mathrm{Mon}(\pi)$ of $\pi \in P(\mathbf{m}, n)$ is the image of ϕ, where $\phi \in \mathrm{Hom}(\Gamma, S_n)$ is in the S_n-class of homomorphisms corresponding to π. It is well known that $\mathrm{Mon}(\pi)$ is transitive if and only if π is a connected covering. Note also that $\mathrm{Aut}\,\pi = C_{S_n}(\mathrm{Mon}(\pi))$; in particular, if $\mathrm{Mon}(\pi)$ is primitive and not regular of prime degree, then $\mathrm{Aut}\,\pi = 1$.

Several of our results on $\mathrm{Hom}(\Gamma, S_n)$ and its subspaces can now be translated into the language of coverings. The first result shows that most of our coverings are connected and have trivial automorphism group.

Proposition 8.1 *Let π be a randomly chosen covering in $P(\mathbf{C}, n)$.*

(i) *The probability that π is connected is $1 - O(n^{-\mu})$.*

(ii) *The probability that $\mathrm{Aut}\,\pi = 1$ is $1 - O(n^{-\mu})$.*

Proof Part (i) follows from Theorem 4.4. Part (ii) follows from Proposition 7.1 (noting that the probability that $\mathrm{Mon}(\pi)$ is regular is sufficiently small). ■

While Proposition 8.1 is classification-free, stronger results can be deduced from our later theorems which apply the classification. Indeed, Theorem 1.9 shows that the probability that a random covering in $P(\mathbf{C}, n)$ has monodromy group A_n or S_n is $1 - O(n^{-\mu})$, proving Theorem 1.13(ii).

Next, Theorem 1.6 shows that almost all connected coverings in $P(\mathbf{m}, n)$ have monodromy group A_n or S_n, and proves part (i) of Theorem 1.13.

Finally, in some situations it is possible to compute the limit probability of having the full symmetric group as a monodromy group. Indeed, Theorem 1.12(vi) yields

Proposition 8.2 *Assume $g \geq 2$ and let d^* be the number of i such that m_i is even. Then for a random $\pi \in P(\mathbf{m}, n)$, the probability that $\mathrm{Mon}(\pi) = S_n$ is equal to $1 - 2^{1-2g-d^*} + O(n^{-(2g-2)})$ if $d^* > 0$, and is $1 - 2^{-2g} + O(n^{-(2g-2)})$ if $d^* = 0$.*

9 Random walks on symmetric groups

In this section we prove Theorem 1.14. Assume the hypothesis of the theorem. For $h \in S_n$ with $\mathrm{sgn}(h) = \prod_{i=1}^{d} \mathrm{sgn}(g_i)$, let $P(h)$ denote the probability that $x_1 \cdots x_d = h$ for randomly chosen $x_i \in C_i$. Then $P(h) = N/(|C_1| \cdots |C_d|)$, where N is the number of ways of writing $h = x_1 \cdots x_d$ with $x_i \in C_i$. By Lemma 3.1(i),

$$N = \frac{|C_1| \cdots |C_d|}{n!} \sum_{\chi \in Irr(S_n)} \frac{\chi(g_1) \cdots \chi(g_d)\chi(h^{-1})}{\chi(1)^{d-1}}.$$

It follows that

$$P(h) = \frac{1}{n!} \sum_{\chi \in Irr(S_n)} \frac{\chi(g_1) \cdots \chi(g_d)\chi(h^{-1})}{\chi(1)^{d-1}}.$$

Since $|\chi(h^{-1})| \leq \chi(1)$, we have

$$|\sum_{\chi \in Irr(S_n), \chi(1)>1} \frac{\chi(g_1) \cdots \chi(g_d)\chi(h^{-1})}{\chi(1)^{d-1}}| \leq \sum_{\chi \in Irr(S_n), \chi(1)>1} \frac{|\chi(g_1) \cdots \chi(g_d)|}{\chi(1)^{d-2}}$$

and since $\mu = d-2-\sum \frac{1}{m_i} > 0$ by hypothesis, Theorem 2.15(i) (with $l = 0$) shows that the last sum is $O(n^{-\mu})$. Therefore

$$P(h) = \frac{1}{n!}(2 + O(n^{-\mu})),$$

completing the proof of Theorem 1.14.

To conclude, we show that Theorem 1.14 is best possible, in the sense that the condition $\mu > 0$ is essential. Indeed, as is shown below, once this condition is removed, the resulting distribution is not sufficiently close to uniform in the l_∞-norm.

Proposition 9.1 *Let $d \geq 2$, let $m_1, \ldots, m_d \geq 2$ be integers and set $\mu = d - 2 - \sum \frac{1}{m_i}$. For $1 \leq i \leq d$, assume $g_i \in S_n$ has cycle-shape $(m_i^{a_i})$ (so $m_i|n$), and let $C_i = g_i^{S_n}$. Assume also that $\prod_{i=1}^{d} \mathrm{sgn}(g_i) = 1$, and for $h \in A_n$ define $P(h)$ as above.*

(i) *If $\mu < 0$ then for sufficiently large n we have $P(1) \geq \frac{2}{n!} \cdot (n!)^{|\mu|/2}$, except when $d = 2$ and $m_1 \neq m_2$, in which case $P(1) = 0$.*

(ii) *If $\mu = 0$ then $P(1) \geq \frac{2}{n!} \cdot c^{\sqrt{n}}$ for some fixed $c > 1$.*

Proof First note that

$$P(1) = \frac{1}{n!} \sum_{\chi \in Irr(S_n)} \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2}}.$$

For $\mu \leq 0$, formulae for these character sums are obtained in [26, 3.3,3.9].

Assume now that $\mu < 0$ (the *elliptic* case). If $d = 2$ we assume that $m_1 = m_2$, since otherwise clearly $P(1) = 0$. Writing $\mathbf{m} = (m_1, \ldots, m_d)$, the possibilities for $\mathbf{m}$ and the corresponding character formulae in the elliptic case are as follows:

(1) $\mathbf{m} = (m, m)$, and

$$\sum_\chi \chi(g_1)^2 = (\frac{n}{m})!\, m^{n/m}$$

(2) $\mathbf{m} = (2, 2, m)$, and

$$\sum_\chi \frac{\chi(g_1)^2\chi(g_3)}{\chi(1)} = \frac{[(n/2)!\, 2^{n/2}]^2 (n/m)!\, m^{n/m}}{n!\, (2m)^{n/m}(n/2m)!}$$

(3) $\mathbf{m} = (2, 3, 3)$, and

$$\sum_\chi \frac{\chi(g_1)\chi(g_3)^2}{\chi(1)} = \frac{[(n/3)!\, 3^{n/3}]^2 (n/2)!\, 2^{n/2}}{n!\, (12)^{n/12}(n/12)!}$$

(4) $\mathbf{m} = (2, 3, 4)$, and

$$\sum_\chi \frac{\chi(g_1)\chi(g_2)\chi(g_3)}{\chi(1)} = \frac{(n/2)!\, 2^{n/2}(n/3)!\, 3^{n/3}(n/4)!\, 4^{n/4}}{n!\, (24)^{n/24}(n/24)!}$$

(5) $\mathbf{m} = (2, 3, 5)$, and

$$\sum_\chi \frac{\chi(g_1)\chi(g_2)\chi(g_3)}{\chi(1)} = \frac{(n/2)!\, 2^{n/2}(n/3)!\, 3^{n/3}(n/5)!\, 5^{n/5}}{n!\, (60)^{n/60}(n/60)!}.$$

Using Stirling's formula, it follows that in all cases these are asymptotically of the form $(n/e)^{n|\mu|/2}\sqrt{n}$, which for large n is at least $2(n!)^{|\mu|/2}$ (since $|\mu| < 2$). Part (i) follows.

Now suppose $\mu = 0$ (the *parabolic* case). Given positive integers n, u, define $C(n, u)$ to be the coefficient of q^n in the infinite product $\prod_{k=1}^\infty (1 - q^k)^{-1/u}$. An asymptotic expression for $C(n, u)$ is given in [26, (3.6)], and in particular it follows from this that there are constants $c_1, c_2 > 1$ depending on u such that

$$c_1^{\sqrt{n}} < C(n, u) < c_2^{\sqrt{n}}.$$

By [26, 3.9], the possibilities in the parabolic cases are as follows:

(6) $\mathbf{m} = (2, 2, 2, 2)$, and

$$\sum_\chi \frac{\chi(g_1)^4}{\chi(1)^2} = \frac{2^{2n}((n/2)!)^4}{(n!)^2} \cdot C(\frac{n}{2}, 2)$$

(7) $\mathbf{m} = (2,4,4)$, and

$$\sum_{\chi} \frac{\chi(g_1)\chi(g_2)^4}{\chi(1)} = \frac{2^{3n/2}(n/2)!((n/4)!)^2}{n!} \cdot C(\frac{n}{4}, 4)$$

(8) $\mathbf{m} = (2,3,6)$, and

$$\sum_{\chi} \frac{\chi(g_1)\chi(g_2)\chi(g_3)}{\chi(1)} = \frac{2^{2n/3}3^{n/2}(n/2)!(n/3)!(n/6)!}{n!} \cdot C(\frac{n}{6}, 6)$$

(9) $\mathbf{m} = (3,3,3)$, and

$$\sum_{\chi} \frac{\chi(g_1)^3}{\chi(1)} = \frac{3^n((n/3)!)^3}{n!} \cdot C(\frac{n}{3}, 3).$$

By Stirling's formula these expressions are all asymptotically of the form $n \cdot C(\frac{n}{m}, m)$, where $m = \max(m_i)$. Part (ii) follows. ■

Observe that when $\mu < 0$, the number $|\mu|/2$ is equal to $1/|H|$, where H is the finite triangle group $\Delta(m_1, m_2, m_3)$ in cases (2)-(5) above and $H = Z_m$ in case (1).

Theorem 1.14 and Proposition 9.1 imply, for example, that if C_1, C_2, C_3 are classes in A_n of cycle-shape $(m_1^{a_1}), (m_2^{a_2}), (m_3^{a_3})$ respectively, then $C_1C_2C_3 = A_n$ almost uniformly pointwise if and only if $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} < 1$.

It is interesting to note that, while in this paper character-theoretic results are proved and used to obtain geometric results on coverings of Riemann surfaces, the proofs in [26] of the character formulae above are geometric, and thus Proposition 9.1 uses geometric insights on coverings in order to prove a probabilistic statement.

References

[1] G.E. Andrews, *The theory of partitions*, Encyclopedia of Mathematics, Addison-Wesley, 1976.

[2] Z. Arad and M. Herzog (eds.), *Products of Conjugacy Classes in Groups*, Springer Lecture Notes **1112**, Springer-Verlag, Berlin, 1985.

[3] S. Chowla, I.N. Herstein and W.R. Scott, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Slesk.* **25** (1952), 29-31.

[4] N. Chigira, The solutions of $x^d = 1$ in finite groups, *J. Algebra* **180** (1996), 653-661.

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

[6] M.D.E. Conder, More on generators for alternating and symmetric groups, *Quart. J. Math. Oxford Ser.* **32** (1981), 137-163.

[7] M.D.E. Conder, Hurwitz groups: a brief survey, *Bull. Amer. Math. Soc.* **23** (1990), 359-370.

[8] I.M.S. Dey, Schreier systems in free products, *Proc. Glasgow Math. Soc.* **7** (1965), 61-79.

[9] P. Diaconis, *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics Lecture Notes - Monograph Series, Vol. 11, 1988.

[10] P. Diaconis, Random walks on groups: characters and geometry, in *Groups St Andrews 2001 in Oxford*, London Math. Soc. Lecture Note Series, Cambridge Univ. Press, to appear.

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

[12] J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199-205.

[13] A. Eskin and A. Okounkov, Asymptotics of numbers of branched coverings of a torus and volumes of moduli spaces of holomorphic differentials, *Invent. Math.* **145** (2001), 59-103.

[14] B. Everitt, Permutation representations of the $(2, 4, r)$ triangle groups, *Bull. Austral. Math. Soc.* **49** (1994), 499-511.

[15] B. Everitt, Alternating quotients of the $(3, q, r)$ triangle groups, *Comm. Algebra* **25** (1997), 1817-1832.

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

[17] S.V. Fomin and N. Lulov, On the number of rim hook tableaux, *J. Math. Sci. (New York)* **87** (1997), 4118-4123.

[18] D. Gluck, Characters and random walks on finite classical groups, *Adv. Math.* **129** (1997), 46-72.

[19] M. Hall, Subgroups of finite index in free groups, *Canad. J. Math.* **1** (1949), 187-190.

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

[21] A. Hurwitz, Über algebraische Gebilde mit eindeutigen Transformationen in sich, *Math. Ann.* **41** (1893), 408-442.

[22] A. Hurwitz, Über die Anzahl der Riemannschen Flächen mit gegebener Verzweigungspunkten, *Math. Ann.* **55** (1902), 53-66.

[23] G.D. James, *The representation theory of the symmetric groups*, Lecture Notes in Math. **682**, Springer-Verlag, Berlin, 1978.

[24] G.D. James and A. Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its Applications, **16**, Addison-Wesley, 1981.

[25] G.A. Jones, Characters and surfaces, in *The atlas of finite groups: ten years on* (eds. R. Curtis and R. Wilson), London Math. Soc. Lecture Note Series **249**, Cambridge Univ. Press, 1998, pp.90-118.

[26] A. Klyachko and E. Kurtaran, Some identities and asymptotics for characters of the symmetric group, *J. Algebra* **206** (1998), 413-437.

[27] M.W. Liebeck and A. Shalev, Maximal subgroups of symmetric groups, *J. Comb. Theory, Series A* **75** (1996), 341-352.

[28] M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods and the $(2,3)$-generation problem, *Annals of Math.* **144** (1996), 77-125.

[29] M.W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383-406

[30] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties, to appear.

[31] A. Lubotzky and D. Segal, *Subgroup growth*, Birkhauser, 2003.

[32] N. Lulov, Random walks on symmetric groups generated by conjugacy classes, Ph.D. Thesis, Harvard University, 1996.

[33] R.C. Lyndon and P.E. Schupp, *Combinatorial Group Theory*, Ergebnisse der Math. und ihrer Grenzgebiete **89**, Springer-Verlag, 1977.

[34] A.D. Mednykh, On the number of subgroups in the fundamental group of a closed surface, *Commun. in Alg.* **16** (1988), 2137-2148.

[35] G.A. Miller, On the groups generated by two operators, *Bull. Amer. Math. Soc.* **7** (1901), 424-426.

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

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

[38] Q. Mushtaq and G-C. Rota, Alternating groups as quotients of two generator groups, *Adv. Math.* **96** (1992), 113-121.

[39] Q. Mushtaq and H. Servatius, Permutation representations of the symmetry groups of regular hyperbolic tessellations, *J. London Math. Soc.* **48** (1993), 77-86.

[40] M. Newman, Asymptotic formulas related to free products of cyclic groups, *Math. Comp.* **30** (1976), 838-846.

[41] C.E. Praeger and J.Saxl, On the orders of primitive permutation groups, *Bull. London Math. Soc.* **12** (1980), 303-307.

[42] H. Röhrl, Unbounded coverings of Riemann surfaces and extensions of rings of meromorphic functions, *Trans. Amer. Math. Soc.* **107** (1963), 320-346.

[43] Y. Roichman, Upper bound on the characters of the symmetric groups, *Invent. Math.* **125** (1996), 451-485.

[44] A. Shalev, Probabilistic group theory, in *Groups St Andrews 1997 in Bath, II*, London Math. Soc. Lecture Note Series **261**, Cambridge University Press, Cambridge, 1999, pp. 648-678.

[45] D. Singerman, Subgroups of Fuchsian groups and finite permutation groups, *Bull. London Math. Soc.* **2** (1970), 319-323.

[46] R. Vakil, Genus 0 and 1 Hurwitz numbers: recursions, formulas, and graph-theoretic interpretations, *Trans. Amer. Math. Soc.* **353** (2001), 4025-4038.

[47] H.S. Wilf, The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n, *Bull. Amer. Math. Soc.* **15** (1986), 228-232.