APPLICATIONS OF CHARACTER THEORY OF FINITE SIMPLE GROUPS

MARTIN W. LIEBECK

1. Introduction

There is a vast literature on the theory of representations and characters of finite simple groups. This theory has many diverse applications, and in this article we shall present a selection of such applications. The choice is heavily skewed by the author's own research directions, and the article is by no means a complete survey of all areas of application.

In this introductory section we shall give the background to three general areas where the character theory of simple groups can be applied. Section 2 contains applications to these areas in the case where the simple groups in question are alternating groups; and Section 3 does likewise for the simple groups of Lie type. The sporadic groups do not play any role in our discussions.

Throughout the article we shall ignore abelian simple groups – so that by a finite simple group we shall mean a finite non-abelian simple group.

1.1. Application 1: Random generation and representation varieties.

The story begins with a well-known result of Steinberg [55]:

Theorem 1.1. *Every finite simple group is* 2*-generated (i.e. can be generated by* 2 *elements).*

For alternating groups A_n ($n \geq 5$), it is easy to see that a 3-cycle and a suitable n- or $(n-1)$-cycle form a pair of generators. Steinberg produced a short, elegant proof for the simple groups of Lie type. Here are his two generators for $SL_n(q)$ with $n \geq 3$, $q > 3$. Let λ be a primitive element of $\mathbb{F}_q$, and let E_{ij} denote the $n \times n$ matrix with 1 in the ij-entry and 0's elsewhere. For $\alpha \in \mathbb{F}_q$ define $x_1(\alpha) = I + \alpha E_{12}$, and let $w = E_{12} + E_{23} + \cdots + E_{n-1,n} \pm E_{n1}$, a monomial matrix of determinant 1 corresponding to an n-cycle in the Weyl group. Then $SL_n(q) = \langle x, h \rangle$ where

$$x = x_1(\lambda)w, \ h = \mathrm{diag}(\lambda^{-1}, \lambda, 1 \ldots, 1).$$

To see this, observe that $y := xhx^{-1} = x_1(\lambda - 1)h_1$ with h_1 diagonal, and then check that $[y, h] = x_1(\beta)$ with $\beta \neq 0$. This shows that $\langle x, h \rangle$ contains root elements $x_1(\beta)$, and now further conjugations produce many more root elements which are easily seen to generate $SL_n(q)$. For other groups of Lie type, Steinberg's argument is a general version of this one, taking h and $x_1(\lambda)$ as diagonal and root elements in an SL_2 subgroup, and w a Coxeter element in the Weyl group. The proof of Theorem 1.1 was actually completed by Aschbacher and Guralnick in [1], where they checked that all the sporadic groups are 2-generated.

An equivalent way of stating Theorem 1.1 is to say that for any finite simple group G, there is an epimorphism $F_2 \to G$, where F_2 denotes the free group of rank 2.

In [10], Dixon showed that not only is the alternating group A_n 2-generated, it is *randomly* 2-generated – that is, if for a finite group G we define $P(G)$ to be the probability

Date: October 2, 2017.

that two elements chosen uniformly at random generate G, then

$$P(A_n) \to 1 \text{ as } n \to \infty.$$

Dixon conjectured that this should hold for all finite simple groups, and his conjecture was proved in [27, 36]:

Theorem 1.2. *Finite simple groups are randomly 2-generated: that is, for finite simple groups G, we have $P(G) \to 1$ as $|G| \to \infty$.*

Again, we can express this equivalently by saying that for simple groups G,

$$\text{Prob}\,(\text{random } \phi \in \text{Hom}(F_2, G) \text{ is surjective}) \to 1 \text{ as } |G| \to \infty.$$

There are many refinements of these questions. A very classical one asks: which finite simple groups are $(2,3)$-generated – that is, generated by two elements, of orders 2 and 3? Equivalently: which simple groups are images of the modular group $C_2 * C_3 \cong PSL_2(\mathbb{Z})$? There is a great deal of literature on this (for example [49, 43, 57]), but it is far from completely solved. On the other hand, there is a complete solution of the probabilistic version of the question. Denote by $P_{2,3}(G)$ the probability that randomly chosen elements of orders 2 and 3 generate G– that is,

$$P_{2,3}(G) = \text{Prob}\,(\text{random } \phi \in \text{Hom}(C_2 * C_3, G) \text{ is surjective})\,.$$

Theorem 1.3. *For G simple, as $|G| \to \infty$,*

$$P_{2,3}(G) \to \begin{cases} 0, \ G = {}^2B_2(2^a),\ PSp_4(2^a),\ PSp_4(3^a) \\ \frac{1}{2}, \ G = PSp_4(p^a),\ p \neq 2,3, p \text{ prime} \\ 1, \ \text{otherwise.} \end{cases}$$

This was proved in [37] for alternating and classical groups, and in [17] for exceptional groups of Lie type.

Another classical refinement asks: which finite simple groups are $(2,3,7)$-generated, i.e. images of the Hurwitz triangle group

$$T_{237} = \langle x, y, z \,:\, x^2 = y^3 = z^7 = xyz = 1 \rangle.$$

Conder [5] showed that A_n is $(2,3,7)$-generated for $n \geq 168$, and there is a substantial literature on the question for groups of Lie type (see [56]). Again, one can pose the probabilistic version of the question.

We now introduce a definition that encompasses all the above probabilistic questions. For a finitely generated group Γ and a finite group G, let

$$P_\Gamma(G) = \text{Prob}\,(\text{random } \phi \in \text{Hom}(\Gamma, G) \text{ is surjective})\,.$$

Thus $P(G) = P_{F_2}(G)$, $P_{2,3}(G) = P_{C_2 * C_3}(G)$, and so on. We aim to study the behaviour of $P_\Gamma(G)$ for simple groups G, for various classes of finitely generated groups Γ. To do this, we need to study *representation varieties*, which we shall loosely define as spaces of the form

$$\text{Hom}(\Gamma, GL_n(K)),\ \text{Hom}(\Gamma, G(q)),\ \text{Hom}(\Gamma, S_n),$$

where K is an algebraically closed field, and $G(q)$ denotes a finite group of Lie type over $\mathbb{F}_q$.

The first step is to estimate the size of the representation variety, and it is here that character theory becomes a vital tool.

Example: Surface groups Suppose Γ is a 1-relator group:

$$\Gamma = \langle x_1, \ldots, x_d \,:\, w(x_1, \ldots, x_d) = 1 \rangle.$$

Then for a finite group G we have $|\mathrm{Hom}(\Gamma, G)| = N_w(1)$, where $N_w : G \to \mathbb{Z}$ is defined as follows, for $z \in G$:

$$N_w(z) = |\{(g_1, \ldots, g_d) \in G^d \,:\, w(g_1, \ldots, g_d) = z\}|.$$

Notice that N_w is a class function on G, hence can be expressed as a linear combination of irreducible characters. For some particularly nice words w, one can work out this expression explicitly.

For example, consider a *surface group* of genus $g \geq 2$:

$$\Gamma_g = \langle x_1, y_1, \ldots, x_g, y_g \,:\, \prod_1^g [x_i, y_i] = 1 \rangle. \tag{1.1}$$

Let G be a finite group, and denote by $\mathrm{Irr}(G)$ the set of irreducible characters of G.

Proposition 1.4. *For $z \in G$, the number of solutions to the equation $\prod_1^g [x_i, y_i] = z$ is*

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

In particular,

$$|\mathrm{Hom}(\Gamma_g, G)| = |G|^{2g-1} \sum_{\chi \in Irr(G)} \frac{1}{\chi(1)^{2g-2}}.$$

This result goes back to Frobenius. We shall give a proof, based on the following basic result (see [26, 30.4]):

Lemma 1.5. *Let C_1, C_2 be conjugacy classes of G, with representatives c_1, c_2. Then for $z \in G$, the number of solutions to the equation $x_1 x_2 = z$ with $x_i \in C_i$ for $i = 1, 2$, is*

$$\frac{|C_1|\,|C_2|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(c_1)\chi(c_2)\chi(z^{-1})}{\chi(1)}.$$

Corollary 1.6. *For $z \in G$, the number of solutions $(x, y) \in G \times G$ to the equation $[x, y] = z$ is*

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

Proof. Observe that $[x, y] = x^{-1}x^y$. For a conjugacy class $C = c^G$, Lemma 1.5 shows that the number of solutions to $x^{-1}u = z$ with $x \in C, u \in C^{-1}$ is

$$\frac{|C|\,|C^{-1}|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(c)\chi(c^{-1})\chi(z^{-1})}{\chi(1)}.$$

For a solution (x, u), there are $|C_G(x)|$ elements y such that $x^y = u$. Hence the number of solutions to $[x, y] = z$ with $x \in C$ is

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

Now sum over C and use the orthogonality relations: the total number of solutions to $[x, y] = z$ is

$$\sum_\chi \left(\sum_{g \in G} \chi(g)\chi(g^{-1}) \right) \frac{\chi(z^{-1})}{\chi(1)} = |G| \sum_\chi \frac{\chi(z^{-1})}{\chi(1)}.$$

The result follows, since the answer must be real, and $\chi(z^{-1})$ is the complex conjugate of $\chi(z)$. □

Proof of Proposition 1.4 Let $w_i = [x_i, y_i]$ and let $N_{w_i}(z)$ be the number of solutions to $[x_i, y_i] = z$. Then

$$N_{w_1 w_2}(z) = \sum_{y \in G} N_{w_1}(y) N_{w_2}(y^{-1}z) = N_{w_1} * N_{w_2}(z),$$

the convolution of N_{w_1} and N_{w_2}. Hence $N_{w_1 \cdots w_g} = N_{w_1} * \cdots * N_{w_g}$. The value of $N_{w_1}(z)$ is given by Corollary 1.6. Now the result follows by induction. □

In Sections 2 and 3 we shall use Proposition 1.4 to estimate $|\mathrm{Hom}(\Gamma, G)|$ for simple groups G, for surface groups $\Gamma = \Gamma_g$ and other finitely generated groups Γ, and see how this can be used to study random generation questions.

1.2. **Application 2: Random walks.** Let G be a finite group with a generating set S. A random walk on G based on S is defined as follows: start at 1, and at each step move from g to gs, for $s \in S$ chosen according to some probability distribution P on S. For $k \in \mathbb{N}$, let P_k be the probability distribution on G after k steps – that is, for $z \in G$, $P_k(z)$ is the probability of reaching z after k steps.

The basic question we wish to address is: how quickly (if at all) does P_k become close to the uniform distribution U on G (where $U(g) = \frac{1}{|G|}$ for all $g \in G$)? The standard way to measure this is using the l_1-norm

$$||P_k - U|| = \sum_{x \in G} |P_k(x) - U(x)|.$$

Examples Here are a couple of well-known examples, taken from [7], one of the pioneering works on the subject.

(a) The "drunkard's walk" on the circle $\mathbb{Z}_p$: let p be a large odd positive integer, and let $\mathbb{Z}_p$ denote the cyclic group of integers modulo p, with generating set $S = \{\pm 1\}$. Start at $X_0 = 0$, and at each step move from X_k to $X_k + 1$ or $X_k - 1$, both with probability $\frac{1}{2}$. So the question here is: how many steps are required until we know that X_k is close to being a random number (between 0 and p)?

(b) A card shuffle: suppose we want to shuffle a pack of n cards according to the following rule. For each shuffle, swap cards i and j, where i, j are chosen uniformly at random from $\{1, \ldots, n\}$ (possibly $i = j$). We can regard this as a random walk on the symmetric group S_n based on the generating set $S = \{e, (ij) : i \neq j\}$ (here e is the identity), where the initial probability distribution P is

$$P(e) = \frac{1}{n},\ P(ij) = \frac{2}{n^2} \text{ for all } i \neq j.$$

Here the question is: how many shuffles are required to mix the pack?

Character theory is a powerful tool for analysing such random walks, particularly in the case where the generating set S consists of a single conjugacy class, or union of classes, of G (as is the case in the above examples). This is usually applied via the following result, commonly known as the "Upper Bound Lemma" of Diaconis and Shahshahani [8].

Proposition 1.7. *Suppose G is generated by a conjugacy class $S = x^G$, and let the initial probability distribution P on S be uniform. Then for $k \geq 1$,*

$$||P_k - U||^2 \leq \sum_{1 \neq \chi \in Irr(G)} \left(\frac{|\chi(x)|}{\chi(1)} \right)^{2k} \chi(1)^2.$$

We shall give a proof of this. The proof requires the following elementary generalisation of Lemma 1.5 and Corollary 1.6.

Lemma 1.8. *Let $C_1, \ldots, C_d$ be conjugacy classes of G, with representatives $c_1, \ldots, c_d$.*

(i) *For $z \in G$, the number of solutions $(x_1, \ldots, x_d) \in C_1 \times \cdots \times C_d$ to the equation $x_1 \cdots x_d = z$ is*

$$\frac{\prod |C_i|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(c_1) \cdots \chi(c_d)\chi(z^{-1})}{\chi(1)^{d-1}}.$$

(ii) *Let $g \in \mathbb{N}$. The number of solutions to the equation*

$$x_1 \cdots x_d\,[a_1, b_1] \cdots [a_g, b_g] = 1 \quad (x_i \in C_i,\ a_i, b_i \in G)$$

is

$$|G|^{2g-1} \prod |C_i| \sum_{\chi \in Irr(G)} \frac{\chi(c_1) \cdots \chi(c_d)}{\chi(1)^{d-2+2g}}.$$

Proof of Proposition 1.7 Suppose G is generated by $S = x^G$. By definition, $P_k(z)$ is the probability that $x_1 \cdots x_k = z$, for $x_i \in S$ chosen uniformly at random. Applying Lemma 1.8(i) with $C_i = S$ for all i, it follows that

$$P_k(z) = \frac{1}{|G|}\left(1 + \sum_{1 \neq \chi \in Irr(G)} \frac{\chi(x)^k \chi(z^{-1})}{\chi(1)^{k-1}}\right). \tag{1.2}$$

Hence

$$\begin{aligned}
||P_k - U||^2 &= \left(\textstyle\sum_{z \in G} |P_k(z) - U(z)|\right)^2 \\
&\leq |G| \textstyle\sum_z |P_k(z) - U(z)|^2 \ \text{(by Cauchy-Schwarz)} \\
&= \tfrac{1}{|G|} \textstyle\sum_z \left|\sum_{\chi \neq 1} \frac{\chi(x)^k \chi(z^{-1})}{\chi(1)^{k-1}}\right|^2 \ \text{(by (1.2))} \\
&\leq \tfrac{1}{|G|} \textstyle\sum_{\chi \neq 1} \frac{|\chi(x)|^{2k}}{\chi(1)^{2k-2}} \sum_z |\chi(z)|^2 \ \text{(using orthogonality relations)} \\
&= \textstyle\sum_{\chi \neq 1} \frac{|\chi(x)|^{2k}}{\chi(1)^{2k-2}}. \quad \square
\end{aligned}$$

Examples Here are a few examples illustrating how Proposition 1.7 can be applied. We will see many more in later sections.

(1) Let $n \geq 5$ be odd, let $G = A_n$ and let x be the n-cycle $(12 \ldots n) \in G$. Take $S = x^G$, a generating set for G. Using the usual notation χ^λ for irreducible characters of S_n (where λ is a partition of n), we have

$$\chi^\lambda(x) = \begin{cases} (-1)^t, \text{ if } \lambda = (n-t, 1^t), \\ 0, \text{ otherwise} \end{cases}$$

(see [24, 21.4]). Moreover, $\chi^{(n-t,1^t)}(1) = \binom{n-1}{t}$. Therefore, if we ignore details about restricting characters to A_n, taking $k = 2$ in Proposition 1.7 gives

$$||P_2 - U||^2 \leq \sum_{t=1}^{n-2} \frac{1}{\binom{n-1}{t}^2} \to 0 \text{ as } n \to \infty.$$

(For this argument to be made rigorous we need to work with irreducible characters of A_n rather than S_n; for this example, the above can easily be adjusted using [25, p.67].) Hence for large n, the distribution P_2 is close to uniform; in other words, this random walk is close to uniform after 2 steps. We say the *mixing time* of the random walk is 2.

(2) Consider the drunkard's walk on $\mathbb{Z}_p$ based on the generating set $\{\pm 1\}$, as introduced above. The nontrivial irreducible characters of $\mathbb{Z}_p$ are $\chi_j : \pm 1 \to e^{\pm 2\pi i j/p}$,

for $1 \leq j \leq p-1$. In this example the generating set consists of two conjugacy classes of $\mathbb{Z}_p$, so we require an "averaged" version of Proposition 1.7. This gives

$$||P_k - U||^2 \leq \sum_{j=1}^{p-1} \left(\frac{1}{2}(\chi_j(1) + \chi_j(-1))\right)^{2k} = \sum_{j=1}^{p-1} \left(\cos\frac{2\pi j}{p}\right)^{2k}.$$

It is shown in [7, p.26] that the right hand side is less than $e^{-\pi^2 k/2p^2}$. Hence P_k is close to uniform when k is of the order of p^2. Further analysis in [7] shows that the mixing time of this random walk is in fact of the order of p^2 – that is, p^2 steps are required to generate a random number by this method.

1.3. **Application 3: Width questions.** Suppose G is a finite group with a generating set S. For $g \in G$, let $l(g) = \min(k : g = s_1 \dots s_k,\ s_i \in S)$, and define

$$\text{width}(G, S) = \max(l(g) : g \in G).$$

This is just the diameter of the (directed) Cayley graph of G with respect to S.

There are many interesting questions concerning the width of finite simple groups. The most famous conjecture in the area is Babai's conjecture: this states that there is a constant c such that $\text{width}(G, S) < (\log|G|)^c$ for all non-abelian simple groups G and generating sets S. There has been spectacular progress on this conjecture (for example [20, 21, 3, 53]), but character theory does not have much impact, so we shall not go into this.

The width questions to which character theory can be applied profitably (often via Lemma 1.8) are those in which the generating set S is a union of conjugacy classes of G. Below we mention several highlights, which will be considered in more detail in later sections.

First, the most famous conjecture in this area:

Conjecture 1.9. (Thompson's Conjecture) *Every finite non-abelian simple group G has a conjugacy class C such that $G = C^2$.*

While this has been proved for many simple groups (alternating and sporadic groups, groups of Lie type over sufficiently large fields [11]), it has remained open for a long time. A useful substitute, proved in [47, 18], is the following. Denote by $G^\sharp$ the set of non-identity elements of G.

Theorem 1.10. *Every finite non-abelian simple group G has conjugacy classes C_1, C_2 such that $G^\sharp \subseteq C_1C_2$.*

Other generating sets of particular interest that have been considered in the literature include:

(a) the set S of commutators of a simple group
(b) the set S of involutions.

For both of these, the width is known:

Theorem 1.11. (The Ore Conjecture, [42]) *Every element of every finite non-abelian simple group is a commutator (i.e. the commutator width is 1).*

Theorem 1.12. ([45]) *Every element of every finite non-abelian simple group is a product of at most 4 involutions (i.e. the involution width is at most 4).*

Interestingly, 4 is a sharp upper bound in this result, as there are infinitely many simple groups of involution width equal to 4 (see [28]).

2. Alternating and symmetric groups

In this section we present some applications of character theory to the alternating and symmetric groups.

2.1. **Character degrees.** Motivated by the formula in Proposition 1.4, we define a character theoretic zeta function as follows. For a finite group G, and a real number s, let

$$\zeta^G(s) = \sum_{\chi \in Irr(G)} \chi(1)^{-s}.$$

For example, $\zeta^G(-2) = |G|$ and $\zeta^G(0) = k(G)$, the number of conjugacy classes of G.

The next result is [38, 2.6,2.7].

Theorem 2.1. *Fix a real number $s > 0$.*

(i) *For $G = S_n$, we have $\zeta^G(s) = 2 + O(n^{-s}) \to 2$ (as $n \to \infty$).*
(ii) *For $G = A_n$, we have $\zeta^G(s) = 1 + O(n^{-s})$.*

The dominant term 2 in part (i) of course comes form the trivial and sign characters of S_n.

We shall sketch a proof of part (i) of the theorem. As already mentioned we label the irreducible characters of S_n as χ^λ for $\lambda = (\lambda_1, \lambda_2, \ldots)$ a partition of n. We shall need the following very standard facts about these characters (see [25] for example):

(a) If $\lambda' = (\lambda'_1, \lambda'_2, \ldots)$ is the partition conjugate to λ, then $\chi^{\lambda'}(1) = \chi^\lambda(1)$.
(b) The degree $\chi^\lambda(1)$ is equal to the number of standard λ-tableaux, i.e. the number of ways of filling in a λ-tableau with $1, \ldots, n$ so that the numbers increase along all rows and columns.
(c) The Hook Formula:
$$\chi^\lambda(1) = \frac{n!}{\prod_{i,j} h_{ij}},$$
where $h_{ij} = \lambda_i + \lambda'_j + 1 - i - j$, the ij-hook length.

Proof of Theorem 2.1(i)

Let $G = S_n$. By the observation (a) above, in proving Theorem 2.1(i) we can restrict our attention to characters χ^λ for partitions λ satisfying $\lambda'_1 \leq \lambda_1$ (that is, tableaux with at least as many columns as rows).

Among such partitions, let $\Lambda = \{\lambda : \lambda_1 \geq \frac{2n}{3}\}$, and for $1 \leq l \leq \frac{n}{3}$, define $\Lambda_l = \{\lambda : \lambda_1 = n - l\}$. Then $|\Lambda_l| = p(l)$, where p denotes the partition function, and Λ is the union of the sets Λ_l together with the partition (n). We claim that

$$\chi^\lambda(1) \geq \binom{n-l}{l} \text{ for all } \lambda \in \Lambda_l. \tag{2.1}$$

To see this, let $\lambda \in \Lambda_l$ and let r be the number of rows of λ. Consider the following procedure. Write the numbers $1, \ldots, l$ in ascending order at the beginning of the first row of a λ-tableau. Then choose any l of the remaining $n-l$ numbers and arrange them in rows $2, \ldots, r$ of the λ-tableau, increasing along rows and columns. Finally, write the remaining $n - 2l$ 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 $\binom{n-l}{l}$ ways, proving (2.1).

Using (2.1) and the bound $p(l) < c_1^{\sqrt{l}}$ (where c_1 is an absolute constant), it is straightforward to see that

$$\sum_{\lambda \in \Lambda} \chi^\lambda(1)^{-s} \leq 1 + \sum_{1 \leq l \leq 2n/3} \frac{p(l)}{\binom{n-l}{l}^s} = 1 + O(n^{-s}). \tag{2.2}$$

Now let Δ be the set of partitions λ such that $\lambda_1 < \frac{2n}{3}$ (and $\lambda'_1 \leq \lambda_1$). We claim that there is an absolute constant $c_2 > 1$ such that

$$\chi^\lambda(1) > c_2^n \text{ for all } \chi \in \Delta. \tag{2.3}$$

To see this, we first count standard λ-tableaux in similar fashion to above, to obtain, for $\chi^\lambda \in \Delta$,

$$\chi^\lambda(1) \geq \max\left(\binom{n-\lambda_2}{n-\lambda_1},\ 2^{\lambda_2-1}\right).$$

Hence we can assume that $\lambda_2 < \epsilon n$ and $\lambda_1 \leq \lambda_2 + \epsilon n < 2\epsilon n$, where $\epsilon = \frac{1}{8e}$. Now apply the Hook Formula. The ij-hook $h_{ij} = \lambda_i + \lambda'_j + 1 - i - j \leq \lambda_1 + \lambda'_1 < \frac{n}{4e}$. Hence

$$\chi^\lambda(1) \geq \frac{n!}{(n/4e)^n} > c_2^n,$$

proving (2.3). It follows that

$$\sum_{\lambda \in \Delta} \chi^\lambda(1)^{-s} < p(n)\, c_2^{-ns} = O(n^{-s}). \tag{2.4}$$

Theorem 2.1(i) follows from (2.2) and (2.4).

2.2. **Random generation.** Theorem 2.1 has immediate applications to random generation properties of alternating and symmetric groups, via Proposition 1.4. For a finitely generated group Γ, let $\mathrm{Hom}_{trans}(\Gamma, S_n)$ denote the set of homomorphisms $\Gamma \to S_n$ having as image a transitive subgroup of S_n.

Theorem 2.2. *Let $g \geq 2$, and let Γ_g be the surface group of genus g, as in* (1.1)*. The following hold:*

(i) $|\mathrm{Hom}(\Gamma_g, S_n)| = \left(2 + O(n^{-(2g-2)})\right)\ (n!)^{2g-1}$;
(ii) $|\mathrm{Hom}_{trans}(\Gamma_g, S_n)| = \left(2 + O(n^{-(2g-2)})\right)\ (n!)^{2g-1}$;
(iii) $P_{\Gamma_g}(A_n) \to 1$ *as* $n \to \infty$.

Part (i) is immediate from Theorem 2.1 and Proposition 1.4. As for (ii), any homomorphism $\Gamma_g \to S_n$ with intransitive image maps Γ_g to $S_k \times S_{n-k}$ for some k with $1 \leq k \leq \frac{n}{2}$, so

$$\begin{aligned}
\tfrac{|\mathrm{Hom}_{intrans}(\Gamma_g, S_n)|}{|\mathrm{Hom}(\Gamma_g, S_n)|} &\leq \textstyle\sum_{k=1}^{[n/2]} \binom{n}{k} \frac{|\mathrm{Hom}(\Gamma_g, S_k \times S_{n-k})|}{|\mathrm{Hom}(\Gamma_g, S_n)|} \\
&\leq C \textstyle\sum_{k=1}^{[n/2]} \binom{n}{k} \left(\frac{k!(n-k)!}{n!}\right)^{2g-1} \quad (C \text{ a constant}) \\
&= C \textstyle\sum_{k=1}^{[n/2]} \frac{1}{\binom{n}{k}^{2g-2}} = O(n^{-(2g-2)}).
\end{aligned}$$

As for (iii): the above shows that $\mathrm{Prob}(\phi \in \mathrm{Hom}(\Gamma_g, S_n)$ has transitive image$) \to 1$ as $n \to \infty$, and a suitable adjustment in the proof gives the same conclusion for $\mathrm{Hom}(\Gamma_g, A_n)$. We now need to show that the probability that ϕ has an image that is imprimitive, or primitive but not equal to A_n, tends to 0. This is again a counting argument, but is more complicated – for a proof, see [38, Theorem 1.7].

Corollary 2.3. *Given $g \geq 2$, there is an integer N_g such that $\Gamma_g \twoheadrightarrow A_n$ for all $n \geq N_g$.*

We can also deduce the *subgroup growth* of surface groups – that is, the behaviour of the function $a_n(\Gamma_g)$ recording the number of subgroups of index n in Γ_g, for $n \in \mathbb{N}$. This result was first proved in [48, 50].

Corollary 2.4. *We have $a_n(\Gamma_g) = (n!)^{2g-2+o(1)}$.*

Proof. It is well known and elementary to see that for a finitely generated group Γ,

$$a_n(\Gamma) = \frac{|\mathrm{Hom}_{trans}(\Gamma, S_n)|}{(n-1)!}.$$

Hence the result is immediate from Theorem 2.2(ii). □

Naturally, one would like to prove versions of Theorem 2.2 for much wider classes of finitely generated groups. It turns out that character-theoretic methods are well suited to handle a much wider class – namely, the *Fuchsian groups*. Recall that a Fuchsian group is a discrete group of isometries of the hyperbolic plane. We shall restrict attention to Fuchsian groups Γ that are co-compact and orientation-preserving; these have nice presentations, as follows:

$$\begin{array}{rl} \text{generators:} & a_1, b_1, \ldots, a_g, b_g, \, x_1, \ldots, x_d \\ \text{relations:} & x_1^{m_1} = \cdots = x_d^{m_d} = 1, \\ & [a_1, b_1] \cdots [a_g, b_g] \, x_1 \cdots x_d = 1, \end{array} \tag{2.5}$$

where $g, d \geq 0$, each $m_i \geq 2$, and the *measure*

$$\mu(\Gamma) := 2g - 2 + \sum_{i=1}^{d} \left(1 - \frac{1}{m_i}\right) > 0.$$

Examples are surface groups Γ_g (for which $d = 0$, $g \geq 2$), and *triangle groups* $T_{m_1 m_2 m_3}$ (which have $d = 3, g = 0$), where

$$T_{m_1 m_2 m_3} = \langle x_1, x_2, x_3 \, : \, x_1^{m_1} = x_2^{m_2} = x_3^{m_3} = x_1 x_2 x_3 = 1 \rangle,$$

and $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} < 1$. The Fuchsian group with smallest possible measure is the Hurwitz triangle group T_{237}, of measure $\frac{1}{42}$.

The appropriate character-theoretic tool for studying $\mathrm{Hom}(\Gamma, G)$ for Fuchsian groups Γ (and G a finite group), is Lemma 1.8(ii): this says that if Γ is as in (2.5), and $C_1, \ldots, C_d$ are conjugacy classes of elements of orders $m_1, \ldots, m_d$ in G, then

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{2g-1} \prod |C_i| \sum_{\chi \in Irr(G)} \frac{\chi(c_1) \cdots \chi(c_d)}{\chi(1)^{d-2+2g}}, \tag{2.6}$$

where $\mathbf{C} = (C_1, \ldots, C_d)$, $c_i \in C_i$, and $\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)$ is the set of homomorphisms $\phi : \Gamma \to G$ such that $\phi(x_i) \in C_i$ for all i.

If $g \geq 2$ then the character sum in (2.6) is bounded in absolute value by $\sum_\chi \chi(1)^{-(2g-2)} = \zeta^G(2g-2)$, so for $G = A_n$ its behaviour is given by Theorem 2.1(ii). However, for $g = 0$ or 1, this is not the case, and a much more detailed character-theoretic analysis is required to bound this sum. In particular, one needs precise information about the *character ratios* $\frac{\chi(x)}{\chi(1)}$ for $x \in G$. For the alternating and symmetric groups, the following result is often a useful tool in analysing these.

Theorem 2.5. (Murnaghan-Nakayama Rule, [24, 21.1]) *Let $\rho\sigma \in S_n$, where ρ is an r-cycle and σ is a permutation of the remaining $n - r$ points. Then*

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

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

In the statement, a *rim r-hook* ν is a connected part of the rim containing r nodes, which can be removed to leave a proper tableau, denoted by $\lambda \setminus \nu$. If, moving from right to left, the rim hook ν starts in row i and finishes in column j, the *leg-length* $l(\nu)$ is defined to be $\lambda'_j - i$ (the number of nodes below the ij-node in the λ-tableau).

Examples

(1) Note that the values $\chi^\lambda(x)$ for x an n-cycle, given in Example (1) after Lemma 1.8, follow immmediately from the Murnaghan-Nakayama Rule.
(2) Using the Murnaghan-Nakayama Rule together with the Hook Formula, one can get a precise expression for the character ratios of a transposition in S_n:

$$\frac{\chi^\lambda(12)}{\chi^\lambda(1)} = \frac{1}{n(n-1)} \sum_j \left(\lambda_j^2 - (2j-1)\lambda_j\right). \tag{2.7}$$

Another powerful tool in analysing character ratios for symmetric groups is the following result of Fomin and Lulov [13].

Theorem 2.6. *Fix an integer $m \geq 2$. Let $n = ma$ with $a \in \mathbb{N}$, and let $\pi \in S_n$ be a permutation of cycle-shape (m^a). Then for any $\chi \in \mathrm{Irr}(S_n)$,*

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

where the constant c depends only on m.

Using the Murnaghan-Nakayama Rule, one can extend this to show that if $n = ma + f$ and $\pi \in S_n$ has shape $(m^a, 1^f)$, then for any $\chi \in \mathrm{Irr}(S_n)$,

$$|\chi(\pi)| \leq \chi(1)^{\frac{1}{m}} \cdot c\,(2n)^{\frac{1}{2}(f+1)}. \tag{2.8}$$

We now demonstrate how this can be used to study the spaces $\mathrm{Hom}(\Gamma, S_n)$ when Γ is a triangle group.

Proposition 2.7. *Let $\Gamma = T_{m_1m_2m_3}$ be a Fuchsian triangle group with measure $\mu = 1 - \sum \frac{1}{m_i}$. For $i = 1, 2, 3$, 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 $\prod \mathrm{sgn}(C_i) = 1$, and write $\mathbf{C} = (C_1, C_2, C_3)$. Then*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| = (n!)^{2g-1}|C_1|\,|C_2|\,|C_3| \cdot (2 + O(n^{-\mu})).$$

Here is a sketch of the proof of the proposition. This amounts to showing that the character sum in the right hand side of (2.6) is equal to $2 + O(n^{-\mu})$. To do this we use (2.8); for ease of exposition we shall ignore the "error term" $c\,(2n)^{\frac{1}{2}(f+1)}$ on the right hand side of (2.8) – the complete argument can be found in [38, 2.15]. Applying (2.8) then, the character sum in question is

$$\sum_{\chi \in Irr(S_n)} \frac{\chi(c_1)\chi(c_2)\chi(c_3)}{\chi(1)} \leq \sum_{\chi \in Irr(S_n)} \frac{\chi(1)^{\frac{1}{m_1}+\frac{1}{m_2}+\frac{1}{m_3}}}{\chi(1)} = \zeta^{S_n}(\mu),$$

and now the conclusion follows from Theorem 2.1(i).

Using Stirling's formula one can show that if m, f are fixed and $\pi \in S_n$ has cycle-shape $(m^a, 1^f)$, then

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

Hence Proposition 2.7 yields, for sufficiently large n,

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| \geq (n!)^{2g-1+\sum\left(1-\frac{1}{m_i}\right)} = (n!)^{\mu+1}.$$

In fact it turns out that this is the correct order of magnitude for all Fuchsian groups ([38, 1.2]):

Theorem 2.8. *For any Fuchsian group Γ,*

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

where $o(1)$ denotes a quantity that tends to 0 as $n \to \infty$.

As for surface groups, these and many further arguments lead to a probabilistic version ([38, 1.7]):

Theorem 2.9. *Let Γ be a Fuchsian group. The probability that a random homomorphism in $\mathrm{Hom}_{trans}(\Gamma, A_n)$ is an epimorphism tends to 1 as $n \to \infty$.*

Corollary 2.10. *Every Fuchsian group surjects onto all but finitely many alternating groups.*

Corollary 2.10 was a well-known conjecture of Graham Higman, formulated in the 1960s. Telling contributions were made by Conder and others for triangle groups (e.g. [5, 6]) using Higman's method of coset diagrams, and the conjecture was finally proved in this way by Everitt in [12]. The above probabilistic method, based on character theory, was a completely different approach.

2.3. **Random walks.** There is a huge literature concerning random walks on the symmetric groups, inspired by Diaconis's pioneering work on card shuffling and his book [7]. As mentioned in Section 1.2, character theoretic methods apply most strongly in cases where the random walk is based on a generating set that is a union of conjugacy classes. Here are a couple of examples.

Examples

(1) Fix an integer $m \geq 2$. Let $n = ma$ with $a \in \mathbb{N}$, and consider the random walk on A_n based on the conjugacy class C with cycle-shape (m^a) (assuming this class lies in A_n). Let P_k be the probability distribution on A_n after k steps of the walk, so that by Proposition 1.7,

$$||P_k - U||^2 \leq \sum_{1 \neq \chi \in Irr(A_n)} \left(\frac{|\chi(c)|}{\chi(1)} \right)^{2k} \chi(1)^2,$$

where $c \in C$. Applying Theorem 2.6, and once again ignoring the error term (and also details about restricting S_n-characters to A_n), this gives

$$||P_k - U||^2 \leq \sum_{1 \neq \chi \in Irr(A_n)} \chi(1)^{\frac{2k}{m} - 2k + 2}.$$

By Theorem 2.1(ii), the right hand side tends to 0 as $n \to \infty$, provided $k > \frac{m}{m-1}$. Hence we obtain the result, due to Lulov [44], that the mixing time of this random walk is 2 if $m \geq 3$, and is at most 3 if $m = 2$. (In fact it is equal to 3 in the latter case.)

(2) Let us return to the transposition Example (b) at the beginning of Section 1.2. Here the generating set $S = \{e, (ij) : i \neq j\}$ is a union of two classes of S_n, with initial distribution $P(e) = \frac{1}{n}$, $P(ij) = \frac{2}{n^2}$. For this random walk, the "averaged version" of the upper bound lemma 1.7 works out as follows:

$$||P_k - U||^2 \leq \sum_{1 \neq \chi \in Irr(S_n)} \left| \frac{1}{n} + \frac{n-1}{n} \frac{\chi(12)}{\chi(1)} \right|^{2k} \chi(1)^2.$$

The values of the character ratios $\frac{\chi(12)}{\chi(1)}$ are given in (2.7). Using all this, Diaconis and Shahshahani [8] were able to show that there is a positive constant b such that if $k = \frac{1}{2} n \log n + cn$ with $c > 0$, then $||P_k - U|| < be^{-2c}$. As a consequence, the mixing time of this random walk is at most $\frac{1}{2} n \log n$, and in fact this is the correct order of magnitude (also shown in [8]).

These random walk questions generated a large effort to study character ratios for symmetric groups. We mention a few highlights. First, a well-known result of Roichman [54]:

Theorem 2.11. *Let $x \in S_n$, and let* $\mathrm{supp}(x)$ *denote the number of points in* $\{1, \dots, n\}$ *that are not fixed by* x.

(i) *There exist constants $b > 0$ and $0 < q < 1$ such that for any irreducible character χ^λ of S_n,*
$$\frac{|\chi^\lambda(x)|}{\chi^\lambda(1)} \leq m(\lambda)^{b\, supp(x)},$$
where $m(\lambda) = \max\left(\frac{\lambda_1}{n}, \frac{\lambda'_1}{n}, q\right)$.

(ii) *Let $\delta > 0$ be a constant, and assume that* $\mathrm{supp}(x) < (1-\delta)n$ *and $x \in A_n$. Then the mixing time of the random walk on A_n based on the conjugacy class of x is of the order of $\frac{n \log n}{supp(x)}$. More precisely, there are postive constants c_1, c_2 such that the mixing time is between $c_1 \frac{n \log n}{supp(x)}$ and $c_2 \frac{n \log n}{supp(x)}$.*

This was greatly generalised by Müller and Schlage-Puchta in [51], in particular removing the need for the assumption on $\mathrm{supp}(x)$ in (ii), and supplying precise, rather than unknown, constants. We state their main character-theoretic result [51, Theorem 1]. In the statement, $\mathrm{fix}(x)$ denotes the number of fixed points in $\{1, \dots, n\}$ of an element $x \in S_n$ (so of course $\mathrm{fix}(x) = n - \mathrm{supp}(x)$).

Theorem 2.12. *For sufficiently large n, for any non-identity $x \in S_n$ and any $\chi^\lambda \in \mathrm{Irr}(S_n)$, we have*
$$|\chi^\lambda(x)| \leq \chi(1)^{1 - \frac{1 - 1/(\log n)}{6t(x)}},$$
where for $1 \leq \mathrm{fix}(x) \leq n-2$,
$$\left| t(x) - \frac{2 \log n}{\log(n/fix(x))} \right| \leq 3,$$
while $t(x) = 2$ for $\mathrm{fix}(x) = 0$.

From this result, it is deduced that the mixing time for the corresponding random walk based on the class of x is between $t(x)$ and $10t(x)$.

More recently, very strong asymptotic results were obtained by Larsen and Shalev [32]. We state a selection from [32, 1.2–1.4]. In the statement, as before $o(1)$ denotes a quantity that tends to 0 as $n \to \infty$.

Theorem 2.13. *Let $x \in S_n$ and $\chi \in \mathrm{Irr}(S_n)$.*

(i) *Fix a positive integer m. If x has at most $n^{o(1)}$ cycles of length less than m, then*
$$|\chi(x)| \leq \chi(1)^{\frac{1}{m} + o(1)}.$$

(ii) *Let* $f = \max(\mathrm{fix}(x), 1)$. *Then*
$$|\chi(x)| \leq \chi(1)^{1 - \frac{\log(n/f)}{2 \log n} + o(1)}.$$

(iii) *Fix $\alpha \leq 1$, and suppose the number of cycles of x is at most n^α. Then*
$$|\chi(x)| \leq \chi(1)^{\alpha + o(1)}.$$

These imply even more precise results on mixing times of random walks than those mentioned before, and a host of further applications are given in [32].

Based on the above results, it can be said that random walks on the alternating and symmetric groups based on conjugacy classes are fairly well understood. We shall see in

the next section that the same cannot be said for the other families of simple groups, namely the finite groups of Lie type.

3. Groups of Lie type

In this section we shall survey some character theory and applications for the finite groups of Lie type. Our notation for these is as follows. Let K be an algebraically closed field of characteristic $p > 0$, and let $\bar{G}$ be a simple algebraic group over K. Let F be a Frobenius endomorphism of $\bar{G}$ such that the fixed point group $(\bar{G}^F)' = G(q)$ is a quasisimple group of Lie type over $\mathbb{F}_q$, where $q = p^a$. Define the rank of $G(q)$ to be the rank of the algebraic group $\bar{G}$. For example, we could have $\bar{G} = SL_n(K)$ and $G(q) = SL_n(q)$ or $SU_n(q)$, both of rank $n-1$; or $\bar{G} = PGL_n(K)$ and $G(q) = PSL_n(q)$ or $PSU_n(q)$.

3.1. **Character degrees.** We begin with a result about the zeta function $\zeta^{G(q)}(s)$, defined at the beginning of Section 2.1. This is taken from [39].

Theorem 3.1. (i) *Let $G(q)$ be as above, and let h be the Coxeter number of $\bar{G}$. If $t > \frac{2}{h}$, then*

$$\zeta^{G(q)}(t) \to 1 \quad as \quad q \to \infty.$$

(ii) *Fix $t > 0$. Then there is an integer $r(t)$ such that for groups $G = G(q)$ of rank $r \geq r(t)$,*

$$\zeta^{G(q)}(t) \to 1 \quad as \quad |G| \to \infty.$$

We remind the reader that the Coxeter number h in part (i) satisfies $\frac{2}{h} = \frac{r}{N}$, where r is the rank and N is the number of positive roots in the root system of $\bar{G}$. The bound $\frac{2}{h}$ is sharp, as we shall see in the sketch of the proof which follows.

Here is a brief sketch of the proof of part (i) of the theorem. For full details, see [39]. We shall need some of the Deligne-Lusztig theory of irreducible characters of $G(q)$, as presented in [9]. For convenience of exposition, we exclude the Suzuki and Ree groups (types ${}^2B_2$, ${}^2G_2$, ${}^2F_4$) from the discussion. Take $\bar{G}$ to be of simply connected type of rank r, and let $(\bar{G}^*, F^*)$ be dual to $(\bar{G}, F)$, as defined in [9, 13.10]. Write $(\bar{G}^*)^{F^*} = G^*$. (For example, if $\bar{G} = SL_n(K)$ then $\bar{G}^* = PGL_n(K)$ and $G^* = PGL_n(q)$.) The irreducible characters of $G(q) = \bar{G}^F$ are partitioned into Lusztig series $\mathcal{E}(\bar{G}^F, (s))$, where (s) ranges over conjugacy classes of semisimple elements s of G^*. The characters in $\mathcal{E}(\bar{G}^F, 1)$ are known as the unipotent characters of $G(q)$, and their degrees are known polynomials in q. There is a bijection ψ_s from $\mathcal{E}(\bar{G}^F, (s))$ to the set of unipotent characters of the centralizer $C_{G^*}(s)$, and the degree of any character $\chi \in \mathcal{E}(\bar{G}^F, (s))$ is given by

$$\chi(1) = |G^* : C_{G^*}(s)|_{p'} \cdot (\psi_s(\chi))(1) \tag{3.1}$$

(see [9, 13.23,13.24]). We remark also that the number of characters in a Lusztig series $\mathcal{E}(\bar{G}^F, (s))$ is bounded above in terms of the rank r (see [39, 2.1]).

Consider first the contribution of the characters in $\mathcal{E}(\bar{G}^F, (s))$ to the zeta function $\zeta^{G(q)}(t)$ from *regular* semisimple classes (s) (i.e. those for which $C_{\bar{G}^*}(s) = T_r$, a maximal torus). The number of such classes is of the order of q^r, and by (3.1), the degrees of the characters are $|G^* : T_r^{F^*}|_{p'}$, which is of the order of q^N (where N is the number of positive roots). Hence the contribution to $\zeta^{G(q)}(t)$ from these Lusztig series is of the order of $q^r \cdot q^{-Nt}$. This tends to 0 for $t > \frac{r}{N} = \frac{2}{h}$ (but not for $t \leq \frac{2}{h}$, showing the sharpness of the bound in part (i) of the theorem).

Now consider the contribution to $\zeta^{G(q)}(t)$ from series $\mathcal{E}(\bar{G}^F, (s))$ for which $C_{\bar{G}^*}(s)^0 = LT_k$, where L is semisimple and T_k is a central torus of rank k with $0 \leq k < r$. The number of such classes is of the order of q^k, and $|G^* : C_{G^*}(s)|_{p'} \sim q^{N-N_L}$, where N_L is the number of positive roots in the root system of L. So the contribution to $\zeta^{G(q)}(t)$ is of

the order of $q^k \cdot q^{-t(N-N_L)}$. One now checks that $\frac{k}{N-N_L} \leq \frac{r}{N}$ for all possible L, except of course for $L = \bar{G}^*$.

Finally, for $L = \bar{G}^*$ we have $s = 1$ and $\mathcal{E}(\bar{G}^F, (s))$ is the set of unipotent characters of $G(q)$. There are boundedly many of these; the trivial character contributes 1 to $\zeta^{G(q)}(t)$, and the contribution of the remaining unipotent characters tends to 0 as $q \to \infty$. This completes the proof of Theorem 3.1(i). □

Using the degree formula (3.1), the irreducible characters of $G(q)$ of the smallest few degrees were determined in [59]. More recently, *gap* results for degrees have appeared: in such results, a polynomial $f(q)$ is specified, usually of much larger degree than that of the smallest nontrivial character, and the irreducible characters of degree less than $f(q)$ are classified explicitly. See [60] for a survey of such results. Here is an example, taken from [19, 6.2].

Theorem 3.2. *Suppose $G = Sp_{2n}(q)$ with q even and $n \geq 4$. There is a collection $\mathcal{W}$ of $q+3$ irreducible characters of G such that if $1 \neq \chi \in \mathrm{Irr}(G) \backslash \mathcal{W}$, then*

$$\chi(1) \geq \frac{(q^{2n}-1)(q^{n-1}-1)(q^{n-1}-q^2)}{2(q^4-1)}.$$

The characters in $\mathcal{W}$ are well understood: their degrees are all of the order of q^{2n-1}, and information about their values is given in [19].

3.2. **Random generation and representation varieties.** Theorem 3.1 has similar consequences for groups of Lie type as its counterpart 2.1 for symmetric and alternating groups. First, the analogue of Theorem 2.2:

Theorem 3.3. *Let $G(q)$ be a group of fixed Lie type, and let Γ_g ($g \geq 2$) be the surface group of genus g. Then*

(i) $|\mathrm{Hom}(\Gamma_g, G(q))| = (1 + o(1))\,|G(q)|^{2g-1}$, *where $o(1)$ denotes a quantity that tends to 0 as $q \to \infty$;*
(ii) $P_{\Gamma_g}(G(q)) \to 1$ *as $q \to \infty$.*

This result can be extended to all Fuchsian groups of genus $g \geq 2$, but this takes a great deal of work – indeed, this is the main focus of [40]. As discussed in Section 2.2, the case of genus $g = 0$ or 1 is much harder. We shall discuss some results for this case in Section 3.4, but many open questions remain.

For a finitely generated group Γ and an algebraically closed field K, define the *representation variety* $R_{n,K}(\Gamma)$ of Γ in dimension n to be

$$R_{n,K}(\Gamma) = \mathrm{Hom}(\Gamma, GL_n(K)).$$

If K has prime characteristic p, $q = p^a$ and F_q is the Frobenius endomorphism of $GL_n(K)$ sending matrix entries to their q^{th} powers, then F_q acts naturally on $R_{n,K}(\Gamma)$, with fixed points $R_{n,K}(\Gamma)^{F_q} = \mathrm{Hom}(\Gamma, GL_n(q))$. Take $\Gamma = \Gamma_g$ for example; now Theorem 3.1 can be extended to show that for $s \geq 2$,

$$\zeta^{GL_n(q)}(s) = q - 1 + \delta + o(1),$$

where $\delta = 1$ if $(n, s) = (2, 2)$ and $\delta = 0$ otherwise. As a consequence, Proposition 1.4 implies that

$$|\mathrm{Hom}(\Gamma_g, GL_n(q))| = (1 + o(1))\, q^{n^2(2g-1)+1}.$$

Now the Lang-Weil theorem [29] implies that the dimension of the variety $R_{n,K}(\Gamma)$ is equal to the degree of the leading term in the order of the fixed point space $R_{n,K}(\Gamma)^{F_q}$, so we deduce

Proposition 3.4. *For $n, g \geq 2$, we have* $\dim R_{n,K}(\Gamma_g) = n^2(2g-1)+1$.

This is a nice illustration of the use of methods for finite groups (e.g. character theory) to deduce results about infinite spaces. More results of this flavour can be found in [40].

3.3. **Width.** Here we discuss applications of character theory to width questions – specifically Theorems 1.10-1.12 in Section 1.3.

3.3.1. *Class width.* First we prove a special case of Theorem 1.10; the proof we give has several of the ingredients of the general proof, which can be found in [47] for many cases, and is completed in [18].

Theorem 3.5. *Let $G = PSL_n(q)$ with $n \geq 4$, and assume $(n, q-1) = 1$. Then G has conjugacy classes C_1, C_2 such that $G^\sharp \subseteq C_1C_2$.*

Proof. Note that the assumption $(n, q-1) = 1$ is made in order to simplify the exposition – it ensures that

$$G = SL_n(q) = PGL_n(q) = G^*.$$

Now G has cyclic maximal tori T_1 and T_2, where

$$|T_1| = \frac{q^n-1}{q-1},\ |T_2| = q^{n-1}-1.$$

For $(n,q) \neq (6,2)$, it is well known [61] that q^n-1 has a *primitive prime divisor* r_1 – that is, r_1 is a prime that divides q^n-1 but not q^i-1 for $1 \leq i \leq n-1$; similarly $q^{n-1}-1$ has a primitive prime divisor r_2 (excluding $(n-1,q) = (6,2)$). Ignoring these small exceptions (which can easily be handled by computation), let $x_i \in T_i$ have order r_i, for $i = 1, 2$. Then x_1, x_2 are regular semisimple elements, and $C_G(x_i) = T_i$.

Let $C_i = x_i^G$ for $i = 1, 2$. We claim that

$$G^\sharp \subseteq C_1C_2. \tag{3.2}$$

By Lemma 1.5, to prove this it is sufficient to establish that for any $z \in G^\sharp$,

$$\Sigma := 1 + \sum_{1 \neq \chi \in Irr(G)} \frac{\chi(x_1)\chi(x_2)\chi(z^{-1})}{\chi(1)} \neq 0. \tag{3.3}$$

First we find which irreducible characters χ satisfy $\chi(x_1)\chi(x_2) \neq 0$. To do this, we use the fact [18, 3.2] that if $x \in G$ is regular semisimple, with $C_G(x) = T$, a maximal torus, and $\chi \in \mathcal{E}(G,(s))$ is an irreducible character such that $\chi(x) \neq 0$, then s is conjugate to an element of the dual torus $T^* \leq G^*$. Moreoever, $|T^*| = |T|$. In our situation, we have $(|T_1|, |T_2|) = 1$. Hence, if $\chi(x_1)\chi(x_2) \neq 0$ then $\chi \in \mathcal{E}(G,1)$ – in other words, χ is a unipotent character of G.

Next we apply a result of Brauer [23, 8.17]: if r is a prime and $\chi \in \mathrm{Irr}(G)$ has r-defect zero (i.e. r does not divide $\frac{|G|}{\chi(1)}$), then $\chi(x) = 0$ whenever $x \in G$ has order divisible by r.

Let χ be a unipotent character of G. Brauer's result implies that if $\chi(x_1)\chi(x_2) \neq 0$, then χ cannot have defect zero for either of the primes r_1 and r_2, so r_1r_2 divides $\frac{|G|}{\chi(1)}$. Inspecting the list of degrees of unipotent characters of G, which can be found in [4, p.465], we see that the only such unipotent characters of G are the trivial character and the Steinberg character St. Thus

$$\chi(x_1)\chi(x_2) \neq 0 \Rightarrow \chi \in \{1,\ St\}.$$

The values of St are given by [4, 6.4.7]:

$$St(x) = \begin{cases} 0, \text{ if } p \text{ divides } o(x) \\ \pm|C_G(x)|_p, \text{ otherwise.} \end{cases}$$

Now returning to (3.3), it follows that for $z \in G^\sharp$,

$$\Sigma = 1 + \frac{St(x_1)St(x_2)St(z^{-1})}{St(1)} = \begin{cases} 1, \text{ if } p \text{ divides } o(z) \\ 1 \pm \frac{|C_G(z)|_p}{q^N}, \text{ otherwise.} \end{cases}$$

Hence $\Sigma \neq 0$, and therefore $G^\sharp \subseteq C_1C_2$, as claimed. □

3.3.2. *Involution width.* The idea of the previous proof was very useful in the proof of the involution width theorem 1.12 in [45]. We shall not go into any detail, but the basic strategy is to find classes C_1, C_2 of a simple group G such that

(a) $G^\sharp \subseteq C_1C_2$, and
(b) C_1, C_2 are both *strongly real* classes.

Here, a class $C = x^G$ is strongly real if x is conjugate to its inverse by an involution; this is equivalent to the property that x is a product of two involutions. Clearly, if (a) and (b) hold, then every element of G is a product of at most four involutions. The properties (a) and (b) are established in [45] for some families of groups of Lie type (such as symplectic and unitary groups), but for other families different methods are used to bound the involution width.

3.3.3. *Commutator width.* Although the Ore Conjecture (Theorem 1.11) has been well covered in several other surveys (see for example [46]), it is hard to resist including a little material on it here, as it is such a good illustration of the applications of character theory. The conjecture emerged from a 1951 paper of Ore [52] in which the case of alternating groups was considered, after which many partial results were obtained, notably those of Thompson [58] for special linear groups, and of Ellers and Gordeev [11] proving the result for groups of Lie type over sufficiently large fields $\mathbb{F}_q$ ($q \geq 8$ suffices). The proof was finally completed in [42], where groups of Lie type over small fields were handled. One of the main strategies in [42] was to show that for an element $g \neq 1$ of a finite simple group G,

$$\sum_{1 \neq \chi \in Irr(G)} \frac{|\chi(g)|}{\chi(1)} < 1. \tag{3.4}$$

It then follows from Corollary 1.6 that g is a commutator in G.

Here we sketch the proof for one family of classical groups over a small field, which illustrates some aspects of the proof in [42].

Theorem 3.6. *For $n \geq 3$, every element of the symplectic group $Sp_{2n}(2)$ is a commutator.*

Note that of course $Sp_2(2)$ and $Sp_4(2)$ are non-perfect, so Theorem 3.6 does not apply to these.

Proof. The argument proceeds by induction. The base cases for the induction are $Sp_{2n}(2)$ with $3 \leq n \leq 6$, and these can be handled computationally.

Write $G = Sp_{2n}(2)$. Let $g \in G$, and write g in block-diagonal form

$$g = \begin{pmatrix} X_1 & 0 & \cdots & 0 \\ 0 & X_2 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & X_k \end{pmatrix} \in Sp_{2n_1}(2) \times \cdots \times Sp_{2n_k}(2) < G,$$

where $\sum n_i = n$, this decomposition being as refined as possible. If each X_i is a commutator in $Sp_{2n_i}(2)$ then g is a commutator in G. Hence induction gives the conclusion except when either

(1) $k = 1$, or
(2) one of the factors $Sp_{2n_i}(2)$ is $Sp_2(2)$ or $Sp_4(2)$.

We call g *unbreakable* if (1) or (2) holds for every such block-diagonal decomposition of g. Thus to prove the theorem for this case it suffices to show that every unbreakable element g of $G = Sp_{2n}(2)$ with $n \geq 7$ is a commutator.

The first step is to prove that the unbreakable element g has small centralizer, namely

$$|C_G(g)| < 2^{2n+15}.$$

For example, if g is unipotent its unbreakability means that it can have few Jordan blocks, and the possiblities for the centralizers of such elements are given by [35, Chapter 7].

Next, Theorem 3.2 shows that there is a collection $\mathcal{W}$ of 5 irreducible characters of G such that

$$\chi(1) \geq \frac{1}{30}(2^{2n}-1)(2^{n-1}-1)(2^{n-1}-4) \text{ for } 1 \neq \chi \in \mathrm{Irr}(G) \setminus \mathcal{W}.$$

Set

$$\Sigma_1(g) = \sum_{\chi \in \mathcal{W}} \frac{|\chi(g)|}{\chi(1)}, \;\; \Sigma_2(g) = \sum_{1 \neq \chi \in \mathrm{Irr}(G) \setminus \mathcal{W}} \frac{|\chi(g)|}{\chi(1)}.$$

Letting $k(G)$ denote the number of conjugacy classes of G, it follows from [14, 3.13] that $k(G) \leq (15.2) \cdot 2^n$. Also $\sum_{\chi \in Irr(G)} |\chi(g)|^2 = |C_G(g)|$ by the orthogonality relations, from which the Cauchy-Schwartz inequality implies that

$$\sum_{\chi \in Irr(G)} |\chi(g)| \leq k(G)^{1/2} |C_G(g)|^{1/2}.$$

Plugging all this into the expression defining $\Sigma_2(g)$, we obtain

$$\Sigma_2(g) < \frac{30\sqrt{15.2} \cdot 2^{n/2} \cdot |C_G(g)|^{1/2}}{(2^{2n}-1)(2^{n-1}-1)(2^{n-1}-4)} < \frac{30\sqrt{15.2} \cdot 2^{n/2} \cdot 2^{n+7.5}}{(2^{2n}-1)(2^{n-1}-1)(2^{n-1}-4)} < 0.6.$$

Bounding $\Sigma_1(g)$ depends on some detailed analysis of the values $\chi(g)$ for the characters $\chi \in \mathcal{W}$, from which one shows that $\Sigma_1(g) < 0.2$.

Hence $\Sigma_1(g) + \Sigma_2(g) < 0.8$, which implies that (3.4) holds, and hence g is a commutator, as required. □

This example gives the flavour of the proof of Theorem 1.11, but it must be said that other families of classical groups over small fields do not yield as easily as this. Indeed the unitary groups presented too many technical obstacles to be handled in this fashion, and a completely different method was used for these in [42].

3.4. **Character ratios.** For a finite group G, a *character ratio* is a complex number of the form $\frac{\chi(x)}{\chi(1)}$, where $x \in G$ and $\chi \in \mathrm{Irr}(G)$. We have seen powerful results and applications of character ratios for symmetric groups in Section 2.2, and it is of course desirable to have similar results for groups of Lie type. These have proved hard to come by, but there has been some substantial recent progress, which we shall describe in this section.

The first substantial results on character ratios of groups of Lie type were proved by Gluck. In [15] he showed that $|\frac{\chi(x)}{\chi(1)}| \leq 3q^{-\frac{1}{2}}$ for all non-central $x \in G(q)$ and all nontrivial $\chi \in \mathrm{Irr}(G(q))$, and in [16] he proved the following result. In the statement, for an element $x \in GL(V)$, we write $[V, x]$ for the commutator space of x on V.

Theorem 3.7. *Suppose $G(q)$ is a quasisimple classical group, with natural module V of dimension n, and let $d < n$ be a positive integer. There is a positive number $\gamma = \gamma(d, q)$ such that for any $x \in G(q)$ with $\dim[V, x] \leq d$, and any $1 \neq \chi \in \mathrm{Irr}(G(q))$,*

$$\left|\frac{\chi(x)}{\chi(1)}\right| < \chi(1)^{-\gamma/n}.$$

If we plug this result into the upper bound lemma 1.7, applied to the random walk on $G = G(q)$ based on the conjugacy class x^G, we get

$$\begin{aligned} ||P_k - U||^2 &\leq \sum_{1 \neq \chi \in Irr(G)} \left|\frac{\chi(x)}{\chi(1)}\right|^{2k} \chi(1)^2 \\ &\leq \sum_{1 \neq \chi \in Irr(G)} \chi(1)^{-2k\gamma/n} \chi(1)^2 \\ &= \zeta^G\left(\tfrac{2k\gamma}{n} - 2\right) - 1. \end{aligned}$$

Now applying Theorem 3.1, we see that for $|G|$ sufficiently large, the mixing time of this random walk is bounded above by $2\gamma^{-1}n$. Note that this does not give a true linear bound for the mixing time in all cases, since γ depends on q; but when q and d are fixed and $n \to \infty$, for example, it does give a linear bound.

One would like to prove much more precise results. For example, consider $G = PSL_n(q)$ with $n \geq 3$, $q \geq 4$. When $g \in G$ is a transvection, the width of G with respect to the class g^G is n (see [34]), and the mixing time is also of order n by [22]; whereas if $g = \mathrm{diag}(\lambda, \lambda^{-1}, J_{n-2}) \in G$, where $\lambda \neq \pm 1$ and J_{n-2} is a single unipotent Jordan block, then the width is 2 (see [33, p.265]), and the mixing time is also 2, by [39, 1.8].

What is needed are better character ratio bounds, and we now present a recent such result from [2]. This applies to a slightly broader class of groups than the quasisimple groups $G(q)$ considered above – for example, it applies to $GL_n(q)$ as well as $SL_n(q)$. Let $\bar{G}$ be a connected reductive algebraic group of rank r over an algebraically closed field of characteristic $p > 0$, such that the commutator subgroup $\bar{G}'$ is simple, and let $G(q) = \bar{G}^F$ where F is a Frobenius endomorphism of $\bar{G}$. We assume that the characteristic p is *good* for $\bar{G}$ (meaning that $p \neq 2$ for types B_n, C_n, D_n; $p \neq 2, 3$ for exceptional types, and also $p \neq 5$ for type E_8). We call a Levi subgroup $\bar{L}$ of $\bar{G}$ *split* if it is an F-stable Levi subgroup of an F-stable proper parabolic subgroup of $\bar{G}$. If $\bar{L}$ is not a torus, write $\bar{L}_{unip}$ for the set of non-identity unipotent elements of $\bar{L}$, and define

$$\alpha(\bar{L}) = \max_{u \in \bar{L}_{unip}} \frac{\dim u^{\bar{L}}}{\dim u^{\bar{G}}}.$$

If $\bar{L}$ is a torus, define $\alpha(\bar{L}) = 0$.

Theorem 3.8. *Let $G = G(q)$ as above, and suppose $x \in G$ is an element such that $C_G(x) \leq \bar{L}^F$, where $\bar{L}$ is a split Levi subgroup of $\bar{G}$. Then for any $\chi \in \mathrm{Irr}(G)$,*

$$|\chi(x)| \leq f(r) \cdot \chi(1)^{\alpha(\bar{L})},$$

where $f(r)$ depends only on the rank r of $\bar{G}$.

Here are some comments on the theorem. First, an example: when $G = SL_3(q)$ the hypothesis on $C_G(x)$ holds for all $x \in G$ except unipotent elements, and regular semisimple elments with centralizer a cyclic torus of order $q^2 + q + 1$. For all other elements $x \in G$ the theorem gives $|\chi(x)| \leq c\,\chi(1)^{\frac{1}{2}}$ where c is an absolute constant, and the exponent $\frac{1}{2}$ here is sharp for many elements x and characters χ.

The exponent $\alpha(\bar{L})$ is in fact sharp, or close to sharp, in many cases. For example, [2, 1.3] shows that if $G = GL_n(q)$ with q large, then for any split Levi subgroup $\bar{L}$ of $\bar{G}$, there is a semisimple element $x \in G$ and a unipotent character $\chi \in \mathrm{Irr}(G)$ such that $C_G(x) = \bar{L}^F$ and $|\chi(x)| \geq \frac{1}{4}\chi(1)^{\alpha(\bar{L})}$.

To apply Theorem 3.8 it is important to calculate, or at least bound, the values $\alpha(\bar{L})$, and [2] has several results doing this. For $\bar{G}$ of exceptional type, the values are computed explicitly – here they are for type E_8:

$\bar{L}'$	E_7	D_7	E_6, E_6A_1	D_6	A_7	rest
$\alpha(\bar{L})$	$\frac{17}{29}$	$\frac{9}{23}$	$\frac{11}{29}$	$\frac{9}{29}$	$\frac{15}{56}$	$\leq \frac{1}{4}$

Here is an example of such a computation for classical groups: if $\bar{G} = GL_n(K)$ and $\bar{L} = GL_{n/m}(K)^m$ where m is a proper divisor of n, then $\alpha(\bar{L}) = \frac{1}{m}$. As a consequence Theorem 3.8 gives the following result, which can be regarded as a Lie analogue of the Fomin-Lulov theorem 2.6:

Corollary 3.9. *Let $G = GL_n(q)$, let m be a proper divisor of n, and let L be a Levi subgroup of the form $GL_{n/m}(q)^m$. If $x \in G$ with $C_G(x) \leq L$, then for all $\chi \in \mathrm{Irr}(G)$,*

$$|\chi(x)| \leq f(n)\chi(1)^{\frac{1}{m}}.$$

A drawback of Theorem 3.8 is that it does not apply to all elements of $G(q)$ – for example, it does not apply to unipotent elements. This is remedied somewhat in [2], at least for $SL_n(q)$ and $GL_n(q)$:

Theorem 3.10. *Let $n \geq 5$ and let $G = SL_n(q)$ or $GL_n(q)$. Then for any $\chi \in \mathrm{Irr}(G)$ and any non-central $x \in G$,*

$$|\chi(x)| \leq h(n) \cdot \chi(1)^{1-\frac{1}{2n}}.$$

Theorem 3.8 has many consequences for random generation, representation varieties, width questions and random walks, which can be found in [2] and [41]. We conclude with just a couple of these consequences.

The first concerns random walks and width for exceptional groups of Lie type. This is part of [2, 1.12], which also has similar results for classical groups.

Proposition 3.11. *Let $G = G(q)$ be an exceptional group of Lie type, and suppose $x \in G$ is such that $C_G(x) \leq \bar{L}^F$, where $\bar{L}$ is a split Levi subgroup of $\bar{G}$. Write $C = x^G$. Then for large q, the following hold.*

(i) *The mixing time of the random walk on G based on C is at most 3.*
(ii) $\mathrm{width}(G, C) \leq 6$.

Proof. Write $\alpha = \alpha(\bar{L})$. For (i), Proposition 1.7 together with Theorem 3.8 give

$$\begin{aligned} ||P_k - U||^2 &\leq \sum_{\chi \neq 1} \left|\tfrac{\chi(x)}{\chi(1)}\right|^{2k} \chi(1)^2 \\ &\leq f(r)^{2k} \sum_{\chi \neq 1} \chi(1)^{2k(\alpha-1)+2} \\ &= f(r)^{2k} \left(-1 + \zeta^G(2k(1-\alpha)-2)\right), \end{aligned}$$

Consider for example $G = E_8(q)$. From the table of α-values given above, we have $\alpha \leq \frac{17}{29}$. Taking $k = 3$, check that $2k(1-\alpha) - 2 \geq 6.\frac{12}{29} - 2 > \frac{2}{h}$ holds, where $h = 30$ is the Coxeter number of G. Hence the conclusion of (i) holds for type E_8 by Theorem 3.1. Other exceptional types are handled in the same way.

Part (ii) is proved in similar fashion to (i), using Lemma 1.8(i) (with $C_i = C$ for all i) instead of Proposition 1.7. □

Note that there are classes C for which the bound 3 in Proposition 3.11(i) is sharp – for example, classes x^G for which $\dim x^{\bar{G}} < \frac{1}{2}\dim \bar{G}$.

Finally, here are two consequences of Theorem 3.8 for random generation, taken from [41, 1.5,1.9].

Theorem 3.12. *Let Γ be a Fuchsian group as in (2.5), and define Q to be the set of prime powers q such that $q \equiv 1$ mod m_i for all i.*

(i) *Assume $\mu(\Gamma) > \max\left(2,\ 1 + \sum \frac{1}{m_i}\right)$. Then there is an integer $N(\Gamma)$ such that for any fixed $n \geq N(\Gamma)$,*

$$\lim_{q \to \infty,\, q \in Q} P_\Gamma(SL_n(q)) = 1.$$

(ii) *Assume* $(m_i, 30) = 1$ *for all* i*, and let* $G(q)$ *be of exceptional Lie type in good characteristic. Then*

$$\lim_{q\to\infty,\, q\in Q} P_\Gamma(G(q)) = 1.$$

Applying part (ii) with Γ a triangle group, we see that all exceptional groups $G(q)$ in good characteristic, with $q \in Q$ sufficiently large, are images of the triangle group $T_{m_1m_2m_3}$. Results of this flavour on triangle generation were obtained by completely different methods in [30, 31].

References

[1] M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, *J. Algebra* **90** (1984), 446–460.

[2] R. Bezrukavnikov, M. W. Liebeck, A. Shalev, and P. H. Tiep, Character bounds for finite groups of Lie type, arXiv:1707.03896.

[3] E. Breuillard, B. Green and T. Tao, Approximate subgroups of linear groups, *Geom. Funct. Anal.* **21** (2011), 774–819.

[4] R.W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley Interscience, 1985.

[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] P. Diaconis, *Group representations in probability and statistics*, Institute of Mathematical Statistics Lecture Notes – Monograph Series **11**, Institute of Mathematical Statistics, Hayward, CA, 1988.

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

[9] F. Digne and J. Michel, *Representations of finite groups of Lie type*, London Math. Soc. Student Texts 21, Cambridge Univ. Press, 1991.

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

[11] E.W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.

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

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

[14] J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), 3023–3070.

[15] D. Gluck, Sharper character value estimates for groups of Lie type, *J. Algebra* **174** (1995), 229–266.

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

[17] R.M. Guralnick, F. Lübeck and A. Shalev, Zero-one laws for random generation of simple groups, preprint.

[18] R.M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.

[19] R. Guralnick and P.H. Tiep, Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.* **356** (2004), 4969–5023.

[20] H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, *Annals of Math.* **167** (2008), 601–623.

[21] H.A. Helfgott and A. Seress, On the diameter of permutation groups, *Annals of Math.* **179** (2014), 611–658.

[22] M. Hildebrand, Generating random elements in $SL_n(\mathbb{F}_q)$ by random transvections, *J. Alg. Comb.* **1** (1992), 133–150.

[23] I.M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics, No. 69, Academic Press, New York-London, 1976.

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

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

[26] G.D. James and M.W. Liebeck, *Representations and characters of groups*, Cambridge Univ. Press, 2nd Edition, Cambridge, 2001.

[27] W.M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), 67–87.

[28] F. Knuppel and K. Nielsen, $SL(V)$ is 4-reflectional, *Geom. Dedicata* **38** (1991), 301–308.
[29] S. Lang and A. Weil, Number of points of varieties over finite fields, *Amer. J. Math.* **76** (1954), 819-827.
[30] M. Larsen, A. Lubotzky and C. Marion, Deformation theory and finite simple quotients of triangle groups I, *J. Eur. Math. Soc.* **16** (2014), 1349–1375.
[31] M. Larsen, A. Lubotzky and C. Marion, Deformation theory and finite simple quotients of triangle groups II, *Groups Geom. Dyn.* **8** (2014), no. 3, 811–836.
[32] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Invent. Math.* **174** (2008), 645–687.
[33] A. Lev, Products of cyclic similarity classes in the groups $GL_n(F)$, *Linear Alg. Appl.* **202** (1994), 235–266.
[34] A. Lev, The covering number of the group $PSL_n(F)$, *J. Algebra* **182** (1996), 60–84.
[35] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Amer. Math. Soc. Surveys and Monographs **180** (2012).
[36] M.W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113.
[37] M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the $(2,3)$-generation problem, *Annals of Math.* **144** (1996), 77–125.
[38] M.W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552–601.
[39] M.W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc.* **90** (2005), 61–86.
[40] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties, *Invent. Math.* **159** (2005), 317–367.
[41] M. W. Liebeck, A. Shalev, and P. H. Tiep, Character ratios, representation varieties and random generation of finite groups of Lie type, preprint.
[42] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, The Ore conjecture, *J. Eur. Math. Soc.* **12** (2010), 939–1008.
[43] F. Lübeck and G. Malle, $(2,3)$-generation of exceptional groups, *J. London Math. Soc.* **59** (1999), 109–122.
[44] N. Lulov, Random walks on symmetric groups generated by conjugacy classes, Ph.D. Thesis, Harvard University, 1996.
[45] A.J. Malcolm, The involution width of finite simple groups, math arXiv:1611.06900.
[46] G. Malle, The proof of Ore's conjecture (after Ellers-Gordeev and Liebeck-O'Brien-Shalev-Tiep), *Astérisque* No. 361 (2014), Exp. No. 1069, ix, 325–348.
[47] G. Malle, J. Saxl and T. Weigel, Generation of classical groups, *Geom. Dedicata* **49** (1994), 85–116.
[48] A.D. Mednykh, On the number of subgroups in the fundamental group of a closed surface, *Commun. in Alg.* **16** (1988), 2137-2148.
[49] G.A. Miller, On the groups generated by two operators, *Bull. Amer. Math. Soc.* **7** (1901), 424–426.
[50] 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.
[51] T.W. Müller and J-C. Schlage-Puchta, Character theory of symmetric groups, subgroup growth of Fuchsian groups, and random walks, *Adv. Math.* **213** (2007), 919–982.
[52] O. Ore, Some remarks on commutators, *Proc. Amer. Math. Soc.* **2** (1951), 307–314.
[53] L. Pyber and E. Szabó, Growth in finite simple groups of Lie type of bounded rank, *J. Amer. Math. Soc.* **29** (2016), 95–146.
[54] Y. Roichman, Upper bound on the characters of the symmetric groups, *Invent. Math.* **125** (1996), 451-485.
[55] R. Steinberg, Generators for simple groups, *Canad. J. Math.* **14** (1962), 277–283.
[56] M.C. Tamburini and M. Vsemirnov, Hurwitz groups and Hurwitz generation, Handbook of algebra Vol. 4, pp.385–426, Elsevier/North-Holland, Amsterdam, 2006.
[57] M.C. Tamburini, J.S. Wilson and N. Gavioli, On the $(2,3)$-generation of some classical groups I, *J. Algebra* **168** (1994), 353–370.
[58] R.C. Thompson, Commutators in the special and general linear groups, *Trans. Amer. Math. Soc.* **101** (1961), 16–33.
[59] P.H. Tiep and A.E. Zalesskii, Minimal characters of the finite classical groups, *Comm. Alg.* **24** (1996), 2093–2167.
[60] P.H. Tiep, Low dimensional representations of finite quasisimple groups, *Groups, combinatorics and geometry* (Durham, 2001), 277–294, World Sci. Publ., River Edge, NJ, 2003.
[61] K. Zsigmondy, Zur Theorie der Potenzereste, *Monatsh. für Math. und Phys.* **3** (1892), 265–284.

M.W. Liebeck, Department of Mathematics, Imperial College, London SW7 2BZ, UK
E-mail address: m.liebeck@imperial.ac.uk