# Chapter 1
# Probabilistic and asymptotic aspects of finite simple groups

Martin W. Liebeck

This is a survey of recent developments in the probabilistic and asymptotic theory of finite groups, with a particular emphasis on the finite simple groups. The first two sections are concerned with random generation, while the third section focusses on some applications of probabilistic methods in representation theory. The final section deals with some of the asymptotic aspects of the diameter and growth of Cayley graphs.

## 1.1 Random generation of simple groups and maximal subgroups

### *1.1.1 Alternating groups*

It is an elementary and well known fact that every alternating group $A_n$ can be generated by two elements – for example, by $(1\,2\,3)$ and $(1\,2\,\cdots n)$ if $n$ is odd, and by $(1\,2\,3)$ and $(2\,\cdots n)$ if $n$ is even. As long ago as 1892, Netto conjectured that almost all pairs of elements of $A_n$ will generate the whole group (see [79, p.90]). That is, if for a finite group $G$ we define $P(G)$ to be the probability that $\langle x, y\rangle = G$ for $x, y \in G$ chosen uniformly at random – so that

$$P(G) = \frac{|\{(x,y) \in G \times G : \langle x, y\rangle = G\}|}{|G|^2},$$

then Netto's conjecture was that $P(A_n) \to 1$ as $n \to \infty$.

It was not until 1969 that Netto's conjecture was proved by Dixon [17]:

**Theorem 1.** *Netto's conjecture holds – that is, $P(A_n) \to 1$ as $n \to \infty$.*

In fact Dixon proved more than this, showing that $P(A_n) > 1 - \frac{8}{(\log\log n)^2}$ for sufficiently large $n$.

We shall give a sketch of Dixon's proof. It relies on two classical results on permutation groups. The first goes back to Jordan (1873) (see [19, p.84] for a proof).

**Lemma 1.** *Suppose that $X$ is a subgroup of $S_n$ which acts primitively on the set $\{1, \ldots, n\}$ and contains a $p$-cycle for some prime $p \leq n-3$. Then $X = A_n$ or $S_n$.*

The second result was deduced by Dixon (see Lemma 3 of [17]) from the paper [21] of Erdös and Turán – the second of their series of seven pioneering papers on the statistical theory of the symmetric group.

**Lemma 2.** *Let $p_n$ be the probability that a permutation in $S_n$, chosen uniformly at random, has one of its powers equal to a $p$-cycle for some prime $p \leq n-3$. Then $p_n \to 1$ as $n \to \infty$.*

**Sketch proof of Dixon's Theorem 1**

Let $G = A_n$. Observe that if $x, y \in G$ do not generate $G$, then they both lie in a maximal subgroup $M$ of $G$. Given $M$, the probability that this happens (for random $x, y$) is $\frac{|M|^2}{|G|^2} = |G:M|^{-2}$. Hence

$$1 - P(G) = \mathrm{Prob}(\langle x, y\rangle \neq G \text{ for random } x, y) \leq \sum_{M \ max \ G} |G:M|^{-2} \qquad (1.1)$$

where the notation $M \ max \ G$ means $M$ is a maximal subgroup of $G$. Let $\mathcal{M}$ be a set of representatives of the conjugacy classes of maximal subgroups of $G$. For a maximal subgroup $M$, the number of conjugates of $M$ is $|G : N_G(M)| = |G : M|$, and hence

$$1 - P(G) \leq \sum_{reps. \ M \in \mathcal{M}} |G:M|^{-1}. \qquad (1.2)$$

The maximal subgroups of $G = A_n$ fall into three categories, according to their actions on the set $\{1, \ldots, n\}$:

(a) intransitive subgroups $M = (S_k \times S_{n-k}) \cap G$ for $1 \leq k \leq [\frac{n}{2}]$
(b) imprimitive subgroups $M = (S_r \,\mathrm{wr}\, S_{n/r}) \cap G$, preserving a partition into $\frac{n}{r}$ $r$-subsets, for divisors $r$ of $n$ with $1 < r < n$
(c) primitive subgroups $M$.

Denote the contributions to the sum in (1.2) from categories (a),(b),(c) by $\Sigma_a$,$\Sigma_b$,$\Sigma_c$, respectively, so that $1 - P(G) \leq \Sigma_a + \Sigma_b + \Sigma_c$. The index in $G$ of a maximal subgroup in (a) is $\binom{n}{k}$, and hence

$$\Sigma_a = \sum_{k=1}^{[n/2]} \binom{n}{k}^{-1}.$$

Similarly

$$\Sigma_b = \sum_{r|n, \, 1<r<n} \big( \tfrac{n!}{(r!)^{n/r}(\frac{n}{r}!)} \big)^{-1}.$$

Elementary arguments (see Lemmas 1 and 2 in [17]) yield

$$\Sigma_a = \frac{1}{n} + O(\frac{1}{n^2}),\ \Sigma_b < n \cdot 2^{-n/4}.$$

So clearly

$$\Sigma_a + \Sigma_b \to 0 \text{ as } n \to \infty. \tag{1.3}$$

Estimating $\Sigma_c$ is less straightforward, however. In fact, instead of estimating this we deal instead with the probability $P_c$ that a random pair $x, y \in G$ generates a proper primitive subgroup of $G$. Here Lemmas 1 and 2 show that $P_c \to 0$ as $n \to \infty$. Since $1 - P(G) \leq \Sigma_a + \Sigma_b + P_c$, it follows from (1.3) that $1 - P(G) \to 0$ as $n \to \infty$, proving Dixon's theorem. □

The right hand sides of the inequalities (1.1),(1.2) suggest that we define, for any finite group $G$, the *maximal subgroup zeta function*

$$\zeta_G(s) = \sum_{M\ max\ G} |G : M|^{-s} = \sum_{n \geq 1} m_n(G) n^{-s}$$

for a real variable $s$, where $m_n(G)$ denotes the number of maximal subgroups of index $n$ in $G$. By the argument for (1.1), we have

$$P(G) \geq 1 - \zeta_G(2). \tag{1.4}$$

For $G = A_n$ we expressed $\zeta_G(2) = \Sigma_a + \Sigma_b + \Sigma_c$ in the above proof. Using the classification of finite simple groups (CFSG), Babai showed in [4] that the number of conjugacy classes of maximal primitive subgroups of $A_n$ is at most $c^{\log^4 n}$ for some absolute constant $c$. Each such subgroup has index at least $\frac{1}{2}[\frac{n+1}{2}]!$ by a classical result of Bochert (see [19, Theorem 3.3B]), and hence

$$\Sigma_c \leq 2c^{\log^4 n}([\frac{n+1}{2}]!)^{-1} = O(\frac{1}{n^2}).$$

This proves [4, 1.2]:

**Theorem 2.** *For $G = A_n$ we have $\zeta_G(2) = \frac{1}{n} + O(\frac{1}{n^2})$ and $P(G) = 1 - \frac{1}{n} + O(\frac{1}{n^2})$.*

A detailed asymptotic expansion of $P(A_n)$ can be found in [18], and precise bounds are given in [74].

### *1.1.2 Groups of Lie type*

At this point we move on to discuss the other non-abelian finite simple groups. By the classification (CFSG), these are the finite groups of Lie type, together with the 26 sporadic groups. Steinberg proved in [85] that every simple group of Lie type is 2-generated (i.e. can be generated by 2 elements), and this has also been verified for

the sporadic groups (see [2]). Hence $P(G) > 0$ for all finite simple groups $G$. In the same paper [17] in which he proved Theorem 1, Dixon also made the following conjecture:

**Dixon's Conjecture.** *For finite simple groups $G$ we have $P(G) \to 1$ as $|G| \to \infty$.*

For alternating groups this is of course the content of Theorem 1. The conjecture was proved for classical groups by Kantor and Lubotzky in [38], and for exceptional groups of Lie type by Liebeck and Shalev in [58]. These proofs were rather lengthy, but more recent work has led to a much shorter proof, which we shall now sketch. It is based on the following result, taken from [48].

**Theorem 3.** *Fix $s > 1$. For finite simple groups $G$, we have $\zeta_G(s) \to 0$ as $|G| \to \infty$.*

Note that the condition $s > 1$ in the theorem is necessary, since as in (1.2) above,

$$\zeta_G(s) = \sum_{reps.\ M \in \mathcal{M}} |G : M|^{1-s} \tag{1.5}$$

where $\mathcal{M}$ is a set of representatives of the conjugacy classes of maximal subgroups of $G$. Before discussing the proof of the theorem, here are a couple of immediate consequences. Firstly, by (1.4) we have

**Corollary 1.** *Dixon's conjecture holds.*

Next, recalling that $\zeta_G(s) = \sum_{n \geq 1} m_n(G) n^{-s}$ where $m_n(G)$ denotes the number of maximal subgroups of index $n$ in $G$, we deduce

**Corollary 2.** *Given $\epsilon > 0$, there exists $N$ such that for any $n > N$ and any finite simple group $G$, we have $m_n(G) < n^{1+\epsilon}$.*

### Sketch proof of Theorem 3

For $G = A_n$, the argument given for $\zeta_G(2)$ in the proof of Theorem 2 works equally well replacing 2 by any $s > 1$, to give $\zeta_G(s) = O(n^{1-s})$. So the main task is to prove Theorem 3 for groups of Lie type.

### Classical groups

We begin with an elementary example.

**Example.** Let $G = PSL_2(q)$ with $q$ odd. It is well known (see for example [34, p.191]) that the maximal subgroups of $G$ are among the following: $P$ (a parabolic subgroup of index $q+1$), $D_{q\pm 1}$ (dihedral), $PSL_2(q_0)$ or $PGL_2(q_0)$ (where $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$), $A_4$, $S_4$ or $A_5$. There are at most 2 conjugacy classes for each subgroup listed, and the number of subfields of $\mathbb{F}_q$ is at most $\log_2 \log_2 q$. It follows

that for $s > 1$ we have $\zeta_G(s) = (q+1)^{1-s} + O(q^{\frac{3}{2}(1-s)} \log\log q) = O(q^{1-s})$. In particular, $\zeta_G(s) \to 0$ as $q \to \infty$.

Now we sketch the general argument of the proof of Theorem 3 for classical groups, which is essentially that given in [38]. Let $G = Cl_n(q)$ denote a simple classical group over $\mathbb{F}_q$ with natural module $V$ of dimension $n$ (so $G = PSL_n(q)$, $PSU_n(q)$, $PSp_n(q)$ or $P\Omega_n^{\pm}(q)$). According to a well known theorem of Aschbacher [1], the maximal subgroups of $G$ fall into the following nine families:

$\mathcal{C}_1$: Stabilizers of totally singular or nonsingular subspaces of $V$ (any subspaces if $G = PSL_n(q)$)
$\mathcal{C}_2$: Stabilizers of direct sum decompositions of $V$
$\mathcal{C}_3$: Stabilizers of extension fields of $\mathbb{F}_q$ of prime degree
$\mathcal{C}_4$: Stabilizers of tensor product decompositions $V = V_1 \otimes V_2$
$\mathcal{C}_5$: Stabilizers of subfields of $\mathbb{F}_q$ of prime index
$\mathcal{C}_6$: Normalizers of $r$-groups of symplectic type in absolutely irreducible representations ($r$ a prime not dividing $q$)
$\mathcal{C}_7$: Stabilizers of tensor product decompositions $V = V_1 \otimes \cdots \otimes V_m$ with all $V_i$ isometric
$\mathcal{C}_8$: Classical subgroups (of type $PSp_n(q)$,$PSO_n(q)$,$PSU_n(q^{1/2})$ in $G = PSL_n(q)$, or $O_n(q)$ in $Sp_n(q)$ with $q$ even)
$\mathcal{S}$: Almost simple subgroups with socle acting absolutely irreducibly on $V$ and defined over no proper subfield of $\mathbb{F}_q$ (of $\mathbb{F}_{q^2}$ if $G$ is unitary).

Denote by $N_{\mathcal{C}}$ (respectively, $N_{\mathcal{S}}$) the total number of $G$-conjugacy classes of maximal subgroups in $\bigcup_{i=1}^{8} \mathcal{C}_i$ (respectively, in $\mathcal{S}$).

**Lemma 3.** *Let $G = Cl_n(q)$ as above. There are positive absolute constants $c_1, c_2, c_3, c_4$ such that the following hold:*
(i) $N_{\mathcal{C}} \leq c_1 n^2 + n \log\log q$*;*
(ii) $N_{\mathcal{S}} \leq f(n)$*, where $f(n)$ is a function depending only on $n$;*
(iii) *also $N_{\mathcal{S}} \leq c_2 n^2 q^{6n} \log q$; and $|G : M| > q^{c_3 n^2}$ for all $M \in \mathcal{S}$;*
(iv) $|G : M| > c_4 q^{n/2}$ *for all maximal subgroups $M$ of $G$.*

Precise descriptions of the families $\mathcal{C}_i$ can be found in [41, Chapter 4], and the number of conjugacy classes of subgroups in each family is also given there. Adding these numbers up, we easily see that the number of $G$-conjugacy classes of maximal subgroups in $\bigcup_{i \neq 5} \mathcal{C}_i$ is less than $c_1 n^2$ for some absolute constant $c_1$, while the number in $\mathcal{C}_5$ is less than $n \log\log q$. Part (i) of the lemma follows.

Short arguments for parts (ii) and (iii) can be found in [48, p.552] and [59, p.89]. Finally, (iv) follows from [41, 5.2.2] (which gives the subgroups of minimal index in all simple classical groups).

**Corollary 3.** *The total number of conjugacy classes of maximal subgroups of $Cl_n(q)$ is at most $f(n) + c_1 n^2 + n \log\log q$.*

**Remark.** It is of interest to find good bounds for the function $f(n)$ in part (ii) of the lemma. This involves estimating, for each finite quasisimple group $S$, prime $p$ and natural number $n$, the number of absolutely irreducible representations of $S$ of dimension $n$ over a field of characteristic $p$. This is a tough problem, especially when $S$ is an alternating group or a group of Lie type in characteristic $p$. A recent paper [26] of Guralnick, Larsen and Tiep bounds the number of absolutely irreducible representations of any $S$ of dimension $n$ by the function $n^{3.8}$, and uses this to show that $f(n) < an^6$ for some absolute constant $a$. This has been sharpened by Häsä [30], who has shown that the total number $m(G)$ of conjugacy classes of maximal subgroups of any almost simple group $G$ with socle a classical group $Cl_n(q)$ satisfies

$$m(G) < 2n^{5.2} + n \log_2 \log_2 q.$$

Using Lemma 3 we can complete the proof of Theorem 3 for classical groups $G = Cl_n(q)$. Let $s > 1$. The argument is divided into the cases where $n$ is bounded and where $n$ is unbounded. For the case where $n$ is bounded, parts (i), (ii) and (iv) of the lemma give

$$\zeta_G(s) = \sum_{reps.\ M} |G : M|^{1-s} < (f(n) + c_1 n^2 + n \log\log q)(c_4 q^{n/2})^{1-s}$$

which tends to 0 as $q \to \infty$. And for the case where $n$ is unbounded, parts (i), (iii) and (iv) of the lemma give

$$\begin{aligned} \zeta_G(s) &\leq \textstyle\sum_{reps.\ M \in \mathcal{C}} |G : M|^{1-s} + \sum_{reps.\ M \in \mathcal{S}} |G : M|^{1-s} \\ &\leq (c_1 n^2 + n \log\log q)\,(c_4 q^{n/2})^{1-s} + (c_2 n^2 q^{6n} \log q)\,(q^{c_3 n^2})^{1-s} \end{aligned}$$

which tends to 0 as $n \to \infty$.

**Exceptional groups of Lie type**

Now we discuss the proof of Theorem 3 when $G = G(q)$ is a simple exceptional group of Lie type over $\mathbb{F}_q$ – that is, a group in one of the families $E_8(q)$, $E_7(q)$, $E_6(q)$, ${}^2E_6(q)$, $F_4(q)$, ${}^2F_4(q)$, $G_2(q)$, ${}^3D_4(q)$, ${}^2G_2(q)$, ${}^2B_2(q)$.

Let $\bar{G}$ be the simple algebraic group over $K = \bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, corresponding to $G(q)$; so if $G = E_8(q)$ then $\bar{G} = E_8(K)$, if $G = {}^2E_6(q)$ then $\bar{G} = E_6(K)$, and so on. There is a Frobenius endomorphism $\sigma$ of $\bar{G}$ such that $G = \bar{G}'_\sigma$, where $\bar{G}_\sigma$ denotes the fixed point group $\{g \in \bar{G} : g^\sigma = g\}$ (see [86]). When $G$ is not a twisted group, $\sigma$ is just a field morphism which acts on root groups $U_\alpha = \{U_\alpha(t) : t \in K\}$ as $U_\alpha(t) \to U_\alpha(t^q)$; when $G$ is twisted, $\sigma$ also involves a graph morphism of $\bar{G}$.

Beginning with the work of Dynkin [20], a great deal of effort has gone into determining the maximal closed subgroups of positive dimension in the algebraic group $\bar{G}$, culminating in [57], where this task was completed. The conclusion (see [57, Cor. 2]) is that there are only finitely many conjugacy classes of maximal closed subgroups of positive dimension in $\bar{G}$: these are

(a) maximal parabolic subgroups;
(b) normalizers of reductive subgroups of maximal rank – these are subgroups containing a maximal torus of $\bar{G}$, and have root system a subsystem of the root system of $\bar{G}$;
(c) a few further classes of (normalizers of) semisimple subgroups.

For example, when $\bar{G} = E_6(K)$ the subgroups under (a) are the parabolics $P_i$ for $1 \leq i \leq 6$; those under (b) are the normalizers of the subsystem subgroups $A_1A_5$, $A_2^3$, $D_4T_2$ and $T_6$ (a maximal torus); and those under (c) are the normalizers of subgroups of types $F_4$, $C_4$, $A_2$, $G_2$, and $A_2G_2$.

In parallel with this, there are results which relate the subgroup structure of the finite groups $G(q)$ with that of $\bar{G}$. The following is taken from [55, Corollary 8]:

**Theorem 4.** *There is an absolute constant $c$ such that if $M$ is a maximal subgroup of the exceptional group $G(q) = \bar{G}'_\sigma$, then one of the following holds:*
(i) $|M| < c$;
(ii) *$M$ is a subfield subgroup $G(q_0)$, or a twisted subgroup (such as ${}^2E_6(q^{1/2}) < E_6(q)$);*
(iii) *$M = \bar{M}_\sigma$ for some $\sigma$-stable maximal closed subgroup $\bar{M}$ of $\bar{G}$ of positive dimension.*
*The maximal subgroups $M$ under* (ii),(iii) *fall into at most $d \log\log q$ conjugacy classes of subgroups in $G(q)$; all satisfy $|G(q) : M| > d'q^r$ (here $r$ is the rank of $\bar{G}$ and $d, d'$ are positive absolute constants).*

This is nice, but it gives no information about the number of conjugacy classes of bounded maximal subgroups under (i). The possibilities for these subgroups were determined up to isomorphism in [56], but nothing much was proved about their conjugacy until the work of Ben Martin [75], which was a major ingredient in the proof of the following result, taken from [48, Theorem 1.2]:

**Theorem 5.** *Let $N, R$ be positive integers, and let $G$ be a finite almost simple group with socle a group of Lie type of rank at most $R$. Then the number of conjugacy classes of maximal subgroups of $G$ of order at most $N$ is bounded by a function $f(N, R)$ of $N, R$ only.*

Applying this to the finite exceptional groups of Lie type, and combining with Theorem 4, we have:

**Corollary 4.** *There is an absolute constant $e$ such that the number of conjugacy classes of maximal subgroups of any finite exceptional group $G(q)$ is bounded above by $e \log\log q$.*

This leads immediately to the proof of Theorem 3 for exceptional groups: for $s > 1$,

$$\zeta_G(s) = \sum_{reps.\ M} |G : M|^{1-s} < (e \log\log q)(d'q^r)^{1-s}$$

which tends to 0 as $q \to \infty$. $\square$

We conclude this section with a brief discussion of Theorem 5. The proof of this uses geometric invariant theory, via the theory of *strongly reductive* subgroups of the algebraic group $\bar{G}$, a notion due to Richardson. These are closed subgroups $H$ which are not contained in any proper parabolic subgroup of $C_{\bar{G}}(T)$, where $T$ is a maximal torus of $C_{\bar{G}}(H)$; in particular, subgroups lying in no proper parabolic of $\bar{G}$ are strongly reductive. Martin's main result in [75] is that the number of conjugacy classes of strongly reductive subgroups of $\bar{G}$ of order at most $N$ is bounded by a function $g(N, R)$, where $R$ is the rank of $\bar{G}$. To adapt this to the analysis of subgroups of the finite group $G(q) = \bar{G}_\sigma$, the following was proved in [48, 2.2]:

**Lemma 4.** *If $F$ is a finite subgroup of $\bar{G}$ which is invariant under $\sigma$, then either $F$ is strongly reductive, or $F$ is contained in a $\sigma$-invariant proper parabolic subgroup of $\bar{G}$.*

The proof of this involves geometric invariant theory. The lemma implies that maximal non-parabolic subgroups of $\bar{G}_\sigma$ are strongly reductive in $\bar{G}$, at which point Martin's result can be used to deduce Theorem 5.

We mention finally that Corollaries 3 and 4 can be used along with arguments in [60] to prove the following, which is [48, 5.2]:

**Theorem 6.** *The symmetric group has $n^{o(1)}$ conjugacy classes of primitive maximal subgroups, and $\frac{1}{2}n + n^{o(1)}$ classes of maximal subgroups in total.*

### *1.1.3 Other results on random generation*

We have discussed at length Dixon's conjecture, that for $G$ simple, $P(G) = \mathrm{Prob}(\langle x, y\rangle = G) \to 1$ as $|G| \to \infty$. Since the conjecture was proved, many variants have been established where one insists on various properties of the generators $x, y$, and we now briefly discuss some of these.

The first concerns the notion of $(2, 3)$-generation. A group $G$ is said to be $(2, 3)$-*generated* if it can be generated by two elements $x, y$ such that $x^2 = y^3 = 1$. It is well known that such groups are precisely the images of the modular group $PSL_2(\mathbb{Z})$ (since $PSL_2(\mathbb{Z})$ is isomorphic to the free product of the cyclic groups $C_2$ and $C_3$). A question which goes back a long way is:

**Problem.** *Which finite simple groups are $(2, 3)$-generated?*

For simple alternating groups this was answered in 1901 by G.A. Miller [78], who showed that $A_n$ is $(2, 3)$-generated if and only if $n \neq 6, 7, 8$. There is quite a large literature on the problem for classical groups – for example, Tamburini, Wilson and Gavioli [89] showed that many classical groups of large dimension are $(2, 3)$-generated. The approach in these papers and many others is to produce explicit generators of the required orders. Is there a probabilistic approach?

In [59], for any finite group $G$, Liebeck and Shalev defined $P_{2,3}(G)$ to be the probability that two randomly chosen elements $x, y$ of orders 2,3 generate $G$. That is, writing $I_r(G)$ for the set of elements of order $r$ in $G$, and $i_r(G) = |I_r(G)|$,

$$P_{2,3}(G) = \frac{|\{(x,y) \in I_2(G) \times I_3(G) : \langle x,y\rangle = G\}|}{i_2(G)i_3(G)}.$$

For finite simple groups $G$, we can attempt to estimate $P_{2,3}(G)$ using a similar approach to the proof of Dixon's conjecture. Given a maximal subgroup $M$ of $G$, the probability that a random pair $x, y$ of elements of orders 2,3 lies in $M$ is $\frac{i_2(M)i_3(M)}{i_2(G)i_3(G)}$, and hence

$$1 - P_{2,3}(G) \leq \sum_{M\ max\ G} \frac{i_2(M)i_3(M)}{i_2(G)i_3(G)}.$$

We were able to prove that for alternating groups, and also for classical groups with some low-dimensional exceptions,

$$\frac{i_2(M)}{i_2(G)} < c|G:M|^{-2/5}, \quad \frac{i_3(M)}{i_3(G)} < c|G:M|^{-5/8}$$

for all maximal subgroups $M$, where $c$ is a constant. Hence, excluding the low-dimensional exceptions

$$1 - P_{2,3}(G) \leq \sum_{M\ max\ G} c^2|G:M|^{-2/5-5/8} = c^2\,\zeta_G(\frac{41}{40}),$$

which tends to 0 as $|G| \to \infty$ by Theorem 3. In fact the low-dimensional exceptions led to some interesting and unexpected counterexamples to $(2,3)$-generation, namely 4-dimensional symplectic groups in characteristics 2 and 3. The final result is [59, 1.4]:

**Theorem 7.** *For $G$ an alternating group, or a finite simple classical group not isomorphic to $PSp_4(q)$, we have $P_{2,3}(G) \to 1$ as $|G| \to \infty$.*

*For $G = PSp_4(2^a)$ or $PSp_4(3^a)$ we have $P_{2,3}(G) = 0$; while for $G = PSp_4(p^a)$ with $p > 3$ prime, we have $P_{2,3}(G) \to \frac{1}{2}$ as $p^a \to \infty$.*

As a consequence, all but finitely many classical groups ($\neq PSp_4(2^a), PSp_4(3^a)$) are $(2,3)$-generated. The exceptional families $PSp_4(2^a)$, $PSp_4(3^a)$ were a surprise at the time, but are rather easily seen not to be $(2,3)$-generated. For example, consider $G = PSp_4(q)$ with $q = 3^a$, and regard $G$ as the isomorphic orthogonal group $\Omega_5(q) = \Omega(V)$. If $x, y \in G$ are elements of orders 2,3 respectively, then the $-1$-eigenspace of $x$ on $V$ has dimension at least 3, while the 1-eigenspace of $y$ has dimension 3. Hence these eigenspaces intersect nontrivially, and it follows that $\langle x,y\rangle \neq G$.

There are many further results of this flavour in the literature. Here is a selection. For a positive integer $k$, define $P_{k,*}(G)$ to be the probability that $G$ is generated by a random element of order $k$ and a random further element; so $P_{k,*}(G) = \frac{|\{(x,y)\in I_k(G)\times G : \langle x,y\rangle = G\}|}{i_k(G)|G|}$. And let $P_C(G)$ be the probability that $G$ is generated by two randomly chosen conjugates – that is, $P_C(G) = \mathrm{Prob}(\langle x, x^y\rangle = G$ for random $x, y \in G)$.

**Theorem 8.** *For all finite simple groups $G$,*
(i) $P_{2,*}(G) \to 1$ *as* $|G| \to \infty$
(ii) $P_{3,*}(G) \to 1$ *as* $|G| \to \infty$
(iii) $P_C(G) \to 1$ *as* $|G| \to \infty$.

Parts (i) and (ii) are taken from [61], while (iii) is the main result of [27].

We conclude this section by mentioning a couple of results of a slightly different, and rather useful, style, in that they provide explicit constants. The first is taken from [25]:

**Theorem 9.** *In any finite simple group $G$ there is a conjugacy class $C$ such that for any $1 \neq x \in G$,*

$$\mathrm{Prob}(\langle x, c\rangle = G \text{ for random } c \in C) > \frac{1}{10}.$$

In other words, for every non-identity $x \in G$, we have $\langle x, c\rangle = G$ for at least a tenth of the elements $c \in C$. As a consequence, for every $1 \neq x \in G$ there exists $y$ such that $\langle x, y\rangle = G$ (a property known as the $\frac{3}{2}$-*generation* of $G$).

The final result is taken from [77]:

**Theorem 10.** *We have $P(G) \geq \frac{53}{90}$ for all finite simple groups $G$, with equality if and only if $G = A_6$.*

Further results on random generation of simple groups (such as "random Fuchsian generation") can be found in Section 3.

### *1.1.4 Generation of maximal subgroups*

Having discussed the generation of finite simple groups, we move on to the generation of their maximal subgroups. We know that $d(G) = 2$ for every (non-abelian) simple group, where $d(G)$ denotes the minimal number of generators of $G$. What about $d(M)$ for maximal subgroups $M$?

We have sketched some results about maximal subgroups of simple groups in the previous sections. Much more complete information can be found in [41] for classical groups and in [54] for exceptional groups of Lie type; in particular, the only unknown maximal subgroups $M$ are almost simple, and for these we have $d(M) \leq 3$ by [15]. And for alternating groups, the O'Nan-Scott theorem (see for example the Appendix of [3]) shows that the primitive maximal subgroups fall into several classes – affine type, product type, diagonal type and almost simple type – so again the unknown ones are almost simple.

Despite being "known", the non-almost simple maximal subgroups can have quite intricate structures, which makes the proof of the following recent result, taken from [11, Theorem 1], rather delicate.

**Theorem 11.** *If $G$ is a finite simple group, and $M$ is a maximal subgroup of $G$, then $d(M) \leq 4$.*

Equality can hold here. For example, let $G = P\Omega^+_{a^2}(q)$ with $a \equiv 2 \bmod 4$ and $q \equiv 1 \bmod 4$. Then $G$ has a maximal subgroup $M$ of type $O^+_a \otimes O^+_a$, in the tensor product family $\mathcal{C}_7$ (see [41, 4.7.6]), and the precise structure of $M$ is $(P\Omega^+_a(q) \times P\Omega^+_a(q)).2^4$, so clearly $d(M) \geq 4$.

The theorem has quite a neat consequence concerning primitive permutation groups (see [11, Theorem 7]): if $G$ is a primitive group with point-stabilizer $M$, then $d(M) \leq d(G) + 4$.

Having found the minimal number of generators, one might ask questions about the random generation properties of maximal subgroups. Some of these will be addressed in the next section (see Corollary 5).

## 1.2 Random generation of arbitrary finite groups

For a finite group $G$, recall that $d(G)$ is the minimal number of generators of $G$. For $k \geq d(G)$ let $d_k(G)$ be the number of generating $k$-tuples of elements of $G$. That is,

$$d_k(G) = |\{(x_1, \ldots, x_k) \in G^k : \langle x_1, \ldots, x_k \rangle = G\}|.$$

Set

$$P_k(G) = \frac{d_k(G)}{|G|^k},$$

so that $P_k(G)$ is the probability that $k$ randomly chosen elements generate $G$. Following Pak [80], define

$$\nu(G) = \min\{k \in \mathbb{N} : P_k(G) \geq \frac{1}{e}\}$$

(where $e$ is as usual the base of natural logarithms). The choice of the constant $1/e$ here is for convenience, and is not significant; note that for any $r \geq 1$, we have $P_{r\nu(G)}(G) \geq 1 - (1 - \frac{1}{e})^r$.

A basic goal is to understand the relationship between $\nu(G)$ and $d(G)$ for finite groups $G$. We begin with a couple of examples.

**Examples** 1. Let $G$ be a $p$-group for some prime $p$, and let $d = d(G)$. For any $k$, we have $P_k(G) = P_k(G/\Phi(G)) = P_k(C_p^d)$. Taking $k = d$,

$$P_d(G) = P_d(C_p^d) = \frac{p^d - 1}{p^d} . \frac{p^d - p}{p^d} \ldots \frac{p^d - p^{d-1}}{p^d} = \prod_1^d (1 - \frac{1}{p^i}),$$

and it is easy to see that this product is at least $1 - \frac{1}{p} - \frac{1}{p^2}$, which is greater than $\frac{1}{e}$ when $p > 2$, and is $\frac{1}{4}$ when $p = 2$. A slightly refinement gives $P_{d+1}(G) > \frac{1}{e}$ in all cases, and hence $\nu(G) \leq d(G) + 1$ for $p$-groups.

2. For simple groups $G$, Dixon's conjecture says that $P_2(G) \to 1$ as $|G| \to \infty$, which implies that $\nu(G) = 2$ for sufficiently large $G$. In fact, Theorem 10 gives $\nu(G) = 2$ for all finite simple groups $G$.

It is not too hard to generalize Example 1 to all nilpotent groups. This is done in [80], where the much less easy case of soluble groups is also considered:

**Theorem 12.** (i) *For $G$ nilpotent, $\nu(G) \leq d(G) + 1$.*
(ii) *For $G$ soluble, $\nu(G) \leq 3.25\, d(G) + 10^7$.*

Examples due to Mann [70] show that it is not possible to improve the constant 3.25 in part (ii) by much.

One might be tempted to think that for any finite group $G$, $\nu(G)$ and $d(G)$ are closely related – perhaps $\nu(G) < c \cdot d(G)$ for some absolute constant $c$? This is in fact far from being true, as is shown by the following result, taken from [38].

**Lemma 5.** *For any real number $R$, there exists a finite group $G$ such that $d(G) = 2$ and $\nu(G) > R$.*

*Proof.* To prove the lemma, Kantor and Lubotzky construct such a group $G$ of the form $T^N$, where $T$ is a non-abelian simple group. A result of Philip Hall [29] shows that the maximal value of $N$ such that $T^N$ is 2-generated is $d_2(T)/|\mathrm{Aut}(T)|$. For example, when $T = A_5$, Hall calculated that $d_2(A_5)/|S_5| = 19$, so that $A_5^{19}$ is 2-generated whereas $A_5^{20}$ is not.

Now let $T = A_n$. By Dixon's Theorem 1, for large $n$, $d_2(T)$ is at least $\frac{2}{3}|T|^2$, and so $d_2(T)/|\mathrm{Aut}(T)|$ is at least $\frac{2}{3}|A_n|^2/|S_n| = n!/6$. Set $N = n!/8$, and define $G = T^N$. Then $d(G) = 2$.

Now consider $P_k(G)$. The probability that a random $k$-tuple of elements of $A_n$ generates $A_n$ is at most $1 - \frac{1}{n^k}$ (since $\frac{1}{n^k}$ is the probability that all of the $k$ permutations fix 1). If a random $k$-tuple in $G = A_n^N$ generates $G$, then each of the $N$ $k$-tuples in a given coordinate position must generate $A_n$, and the probability that this happens is at most $(1 - \frac{1}{n^k})^N = (1 - \frac{1}{n^k})^{n!/8}$. For this to be at least $\frac{1}{e}$, $k$ must be of the order of $n$. Hence $\nu(G)$ can be arbitrarily large, while $d(G) = 2$. □

So it seems that it will be tricky to find a general relationship between $\nu(G)$ and $d(G)$. In [80], Pak proves that $\nu(G) \leq \lceil \log_2 |G| \rceil + 1$ for all finite groups $G$, and conjectures that there is a constant $C$ such that $\nu(G) < C \cdot d(G) \cdot \log\log|G|$. This was proved in a strong form by Lubotzky [67] (see also [15, Theorem 20]):

**Theorem 13.** *For all finite groups $G$,*

$$\nu(G) \leq d(G) + 2\log_2\log_2|G| + 4.02.$$

We now discuss Lubotzky's proof in some detail. Recall that $m_n(G)$ denotes the number of maximal subgroups of index $n$ in the finite group $G$. Define

$$\mu(G) = \max_{n \geq 2} \frac{\log m_n(G)}{\log n}.$$

So $m_n(G) \leq n^{\mu(G)}$ for all $n$, and we can think of $\mu(G)$ as the "polynomial degree" of the rate of growth of $m_n(G)$.

**Lemma 6.** *For any finite group $G$, $\nu(G) \leq \lceil \mu(G) + 2.02 \rceil$.*

*Proof.* For any positive integer $k$, if $x_1, \ldots, x_k$ denote randomly chosen elements of $G$, we have

$$\begin{aligned} 1 - P_k(G) &= \mathrm{Prob}(\langle x_1, \ldots, x_k \rangle \neq G) \\ &\leq \textstyle\sum_{M \, max \, G} \mathrm{Prob}(x_1, \ldots, x_k \in M) \\ &= \textstyle\sum_{M \, max \, G} \frac{|M|^k}{|G|^k} \\ &= \textstyle\sum_{n \geq 2} m_n(G) n^{-k} \\ &\leq \textstyle\sum_{n \geq 2} n^{\mu(G)-k}. \end{aligned}$$

Hence if $k \geq \mu(G) + 2.02$, then $1 - P_k(G) \leq \sum_{n \geq 2} n^{-2.02}$, which is less than $1 - \frac{1}{e}$. Therefore $P_k(G) \geq \frac{1}{e}$ for such $k$, giving the result. □

By the lemma, to prove Theorem 13, it is sufficient to bound $m_n(G)$ for arbitrary finite groups $G$. Each maximal subgroup of index $n$ in $G$ gives a homomorphism $\pi : G \to S_n$ with image $\pi(G)$ a primitive subgroup of $S_n$ and kernel $\mathrm{Ker}(\pi) = \mathrm{core}_G(M) = \bigcap_{g \in G} M^g$.

We call a maximal subgroup $M$ *core-free* if $\mathrm{core}_G(M) = 1$. According to a result of Pyber, which appeared later in improved form as [53, Theorem 1.4], the number of core-free maximal subgroups of index $n$ in $G$ is at most $n^2$ (the improved form is $cn^{3/2}$). The proof relies on the detailed description of core-free maximal subgroups given by Aschbacher and Scott in [3].

Now consider the non-core-free maximal subgroups. Each corresponds to a homomorphism $\pi : G \to S_n$ with $\pi(G)$ primitive and $\mathrm{Ker}(\pi) \neq 1$. To compute $m_n(G)$, we need to count the number of possibilities for $\mathrm{Ker}(\pi)$ (and then multiply by $n^2$, by Pyber's result). To do this, we consider chief series $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ (so $N_i \lhd G$ and each $N_i/N_{i-1}$ is minimal normal in $G/N_{i-1}$). A finite group can have many chief series, but the number $r$, and the collection of chief factors $N_i/N_{i-1}$, are uniquely determined by $G$, as is the collection of normal subgroups $C_1, \ldots, C_r$, where $C_i = C_G(N_i/N_{i-1})$, the kernel of the action of $G$ on $N_i/N_{i-1}$.

By the O'Nan-Scott theorem (see [19, Theorems 4.3B,4.7A]), there are three possibilities for the structure of the primitive permutation group $\pi(G)$:

(1) $\pi(G)$ has a unique minimal normal subgroup $K$, and $K \cong T^k$ for some non-abelian simple group $T$;
(2) $\pi(G)$ has exactly two minimal normal subgroups $K_1, K_2$, and $K_1 \cong K_2 \cong T^k$ for some non-abelian simple group $T$;
(3) $\pi(G)$ is an *affine* group: it has a unique minimal normal subgroup $K \cong C_p^k$ for some prime $p$.

In case (1), Lubotzky showed that $\mathrm{Ker}(\pi)$ must be one of the $r$ subgroups $C_i$; and in case (2), $\mathrm{Ker}(\pi)$ must be $C_i \cap C_j$ for some $i, j$ (see [67, 2.3]). Thus these cases contribute at most $\frac{1}{2}r(r+1)n^2$ to $m_n(G)$. Further argument [67, 2.5] shows that case (3) contributes at most $rn^{d(G)+2}$, and hence

**Lemma 7.** *For a finite group $G$ which has $r$ chief factors, $m_n(G) \leq r^2 n^{d(G)+2}$.*

Since $r < \log |G|$, the lemma gives $\mu(G) \leq d(G) + 2 + 2 \log r \leq d(G) + 2 + 2 \log \log |G|$, so Theorem 13 follows using Lemma 6.

Building on Lubotzky's ideas, and adding a lot more of their own, Jaikin-Zapirain and Pyber proved the following remarkable result in [35], giving upper and lower bounds for $\nu(G)$ which are tight up to a multiplicative constant.

To state the result we need a few definitions. For a non-abelian characteristically simple group $A$ (i.e. $A \cong T^k$ with $T$ simple), denote by $\mathrm{rk}_A(G)$ the maximal number $r$ such that $G$ has a normal section which is the product of $r$ chief factors isomorphic to $A$. Let $l(A)$ be the minimal degree of a faithful transitive permutation representation of $A$. Finally, define

$$\rho(G) = \max_A \frac{\log \mathrm{rk}_A(G)}{\log l(A)}.$$

For example, if $G = (A_n)^t$ ($n \geq 5$), then all chief factors are isomorphic to $A_n$, and $\mathrm{rk}_{A_n}(G) = t$, $l(A_n) = n$, so $\rho(G) = \log t / \log n$. On the other hand, if $G = A_n \,\mathrm{wr}\, A_t$ ($t \geq 5$), then a chief series is $1 \leq (A_n)^t \leq G$, and $\mathrm{rk}_A(G) = 1$ for both chief factors of $G$, so $\rho(G) = 0$.

**Theorem 14.** *There exist absolute constants $\alpha, \beta > 0$ such that for all finite groups $G$,*

$$\alpha(d(G) + \rho(G)) < \nu(G) < \beta d(G) + \rho(G).$$

If we return to the example $G = (A_n)^{n!/8}$ in the proof of Lemma 5, the theorem says that $\nu(G)$ is of the order of $\log(n!)/\log n$, hence of the order of $n$ (while $d(G) = 2$). On the other hand, for the wreath product $G = A_n \,\mathrm{wr}\, A_t$, the theorem tells us that $\nu(G)$ is bounded.

### Applications

We conclude this section by discussing a few applications of Theorem 14. The first is to the random generation of maximal subgroups of finite simple groups, taken from [11]. Recall from Theorem 11 that such a maximal subgroup $M$ satisfies $d(M) \leq 4$. It is shown also in [11, 8.2] that $M$ has at most three non-abelian chief factors. Hence $\nu(M)$ is bounded by Theorem 14, and so we have

**Corollary 5.** *Given $\epsilon > 0$, there exists $k = k(\epsilon)$ such that $P_k(M) > 1 - \epsilon$ for any maximal subgroup $M$ of any finite simple group.*

One might be tempted to think, in the spirit of Dixon's conjecture, that there is a constant $k$ such that $P_k(M) \to 1$ as $|M| \to \infty$. But this is not the case, as is shown by the maximal subgroups $S_{n-2}$ of $A_n$, for which $P_k(S_{n-2}) \leq 1 - \frac{1}{2^k}$ for any $k$.

The second application is to linear groups [35, 9.7]. Let $G$ be a finite subgroup of $GL_n(K)$ for some field $K$. A result of Fisher [23] implies that the number of non-abelian chief factors of $G$ is less than $n$. Hence Theorem 14 gives

**Corollary 6.** *There is an absolute constant $c$ such that if $G$ is any finite linear group in dimension $n$ over some field $K$, then $\nu(G) < c \cdot d(G) + \log n$.*

It is striking that the number of random generators does not depend on the field $K$.

The third application relates $\nu(G)$ to the sizes of so-called *minimal* generating sets of $G$ – that is, generating sets $S$ such that no proper subset of $S$ generates $G$. Define $\tilde{d}(G)$ to be the maximal size of a minimal generating set of $G$. For example, if $G = S_n$ then $\{(1\,2),\,(2\,3),\ldots,(n-1\,n)\}$ is a minimal generating set of size $n-1$, and a result of Whiston [90] shows that $\tilde{d}(S_n) = n-1$.

It is proved in [35, 9.9] that $\mathrm{rk}_A(G) \leq \tilde{d}(G)$ for any non-abelian characteristically simple group $A$, and hence Theorem 14 gives

**Corollary 7.** *There is an absolute constant $c$ such that for any finite group $G$, $\nu(G) < c \cdot d(G) + \log \tilde{d}(G)$.*

This result has some significance in the analysis of the Product Replacement Algorithm for choosing random elements in a finite group, since the quantities $\nu(G)$ and $\tilde{d}(G)$ play a role in this analysis. We refer the reader to [81] for details.

## 1.3 Representation varieties and character-theoretic methods

If $\Gamma$ is a finitely generated group, $K$ a field and $n$ a natural number, we call $\mathrm{Hom}(\Gamma, GL_n(K))$, the set of representations $\rho : \Gamma \to GL_n(K)$, the *representation variety* of $\Gamma$ in dimension $n$ over $K$. In this section we shall show how probabilistic and character-theoretic methods can be brought to bear on the study of such varieties over algebraically closed fields and also over finite fields, for a particular class of finitely generated groups $\Gamma$. We shall also consider the representation spaces $\mathrm{Hom}(\Gamma, G(K))$ and $\mathrm{Hom}(\Gamma, S_n)$, where $G(K)$ is a simple algebraic group over $K$, which are of interest in a variety of contexts.

### *1.3.1 Fuchsian groups*

The class of finitely generated groups $\Gamma$ we shall consider are the *Fuchsian* groups, i.e. finitely generated discrete groups of isometries of the hyperbolic plane. By classical work of Fricke and Klein, the orientation-preserving Fuchsian groups $\Gamma$ have presentations of the following form:

$$\begin{array}{ll} \text{generators:} & a_1, b_1, \ldots, a_g, b_g \ \text{(hyperbolic)} \\ & x_1, \ldots, x_d \ \text{(elliptic)} \\ & y_1, \ldots, y_s \ \text{(parabolic or hyperbolic boundary)} \\ \\ \text{relations:} & x_1^{m_1} = \cdots = x_d^{m_d} = 1, \\ & x_1 \cdots x_d y_1 \cdots y_s [a_1, b_1] \cdots [a_g, b_g] = 1 \end{array}$$

where $g, d, s \geq 0$ and $m_i \geq 2$ for all $i$, and the *measure* $\mu(\Gamma) > 0$, where

$$\mu(\gamma) = 2g - 2 + s + \sum_1^d (1 - \frac{1}{m_i}).$$

The number $g$ is called the *genus* of $\Gamma$.

There are also results along the lines discussed below for non-orientation preserving Fuchsian groups, but for brevity's sake we shall not mention these.

**Examples** 1. *Surface groups* These are the groups with $s = d = 0$ and $g \geq 2$: let

$$\Gamma_g = \langle a_1, b_1, \ldots, a_g, b_g : \prod_i [a_i, b_i] = 1 \rangle$$

so that $\Gamma_g = \pi_1(S)$, the fundamental group of a surface $S$ of genus $g$.

2. *Triangle groups* These have $g = s = 0$, $d = 3$. For positive integers $a, b, c$ define

$$T = T_{a,b,c} = \langle x, y, z : x^a = y^b = z^c = xyz = 1 \rangle,$$

where $\mu(T) = 1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c} > 0$, and call this the $(a, b, c)$-triangle group. The minimal value of $\mu$ for a triangle group is $\frac{1}{42}$, which occurs for the *Hurwitz* triangle group $T_{2,3,7}$.

3. *Free products* When $s > 0$, $\Gamma$ is a free product of cyclic groups, such as the free group $F_r$ of rank $r$, or a free product $C_a * C_b = \langle x, y : x^a = y^b = 1 \rangle$ (which has $\mu = 1 - \frac{1}{a} - \frac{1}{b}$).

The Fuchsian groups for which $s = 0$ are said to be *co-compact*.

Let $q$ be a prime power and $K = \bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$. In the sections below, we shall discuss the representation spaces $\mathrm{Hom}(\Gamma, G)$, where $\Gamma$ is a Fuchsian group and $G$ is $GL_n(K)$, $G(K)$ (a simple algebraic group over $K$), $G(q)$ (a group of Lie type over $\mathbb{F}_q$), or $S_n$. These representation spaces have many connections with other areas, some of which we shall now point out.

The first connection is with the area of random generation. To say that a finite group $G$ is generated by two elements is to say that there exists an epimorphism in the space $\mathrm{Hom}(F_2, G)$, where $F_2$ is the free group of rank 2. The probability $P(G)$ (defined in Section 1.1.1) that $G$ is generated by two randomly chosen elements is then

$$P(G) = \frac{|\{\phi \in \mathrm{Hom}(F_2, G) : \phi \text{ epi}\}|}{|\mathrm{Hom}(F_2, G)|} = \text{Prob}(\text{random } \phi \in \mathrm{Hom}(F_2, G) \text{ is epi}).$$

For any Fuchsian group $\Gamma$, we can similarly define

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

Dixon's conjecture (Corollary 1) asserts that $P(G) \to 1$ as $|G| \to \infty$ for finite simple groups $G$, and one could hope to prove similar results for the probabilities $P_\Gamma(G)$. For example, a question posed many years ago asks which finite simple groups are $(2, 3, 7)$-generated – that is, generated by three elements of orders 2,3 and 7 with product equal to 1. There are many results on this question in which the approach is to construct explicit generators, but one might hope to shed further light by studying the probabilities $P_\Gamma(G)$, where $G$ is simple and $\Gamma$ is the triangle group $T_{2,3,7}$. Results on this and other probabilities $P_\Gamma(G)$ will be discussed below.

Other connections concern the representation space $\mathrm{Hom}(\Gamma, S_n)$. The *subgroup growth* of $\Gamma$ is measured by the growth of the function $a_n(\Gamma)$, the number of subgroups of index $n$ in $\Gamma$, and it is an elementary fact that

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

where $\mathrm{Hom}_{\mathrm{trans}}(\Gamma, S_n)$ is the set of homomorphisms $\Gamma \to S_n$ which have image which is transitive on $\{1, \ldots, n\}$. Another connection is Hurwitz's theory that $\mathrm{Hom}(\Gamma, S_n)$ counts branched coverings of Riemann surfaces, where $g$ is the genus of the surface and the images of $x_1, \ldots, x_d$ are the monodromy permutations around the branch points (see [63, Section 8] for details).

### *1.3.2 Character theory*

The connection between the sizes of the spaces $\mathrm{Hom}(\Gamma, G)$ and character theory is given by the following lemma, which goes back to Frobenius and Hurwitz. Let $\Gamma$ be a co-compact Fuchsian group with generators $a_i, b_i, x_i$ as above, and let $G$ be a finite group. For conjugacy classes $C_i$ in $G$ having representatives $g_i$ of order dividing $m_i$ ($1 \leq i \leq d$), define $\mathbf{C} = (C_1, \ldots, C_d)$ and

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

Denote by $\mathrm{Irr}(G)$ the set of irreducible (complex) characters of $G$.

**Lemma 8.** *With the above notation,*

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

For a proof, see [63, 3.2]. For example, applying this with $g = 0$ and $d = 3$, we obtain the well known formula of Frobenius that if $C_1, C_2, C_3$ are three classes in $G$, then the number of solutions to the equation $x_1 x_2 x_3 = 1$ for $x_i \in C_i$ is

$$\frac{|C_1||C_2||C_3|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(g_1)\chi(g_2)\chi(g_3)}{\chi(1)}. \tag{1.6}$$

When $G$ is a finite simple group, a major tool in the analysis of $\mathrm{Hom}(\Gamma, G)$ is provided by the *representation zeta function* of $G$, defined for a real variable $s$ by

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

The next result is taken from [63, 1.1] for alternating groups, and from [64, 1.1,1.2] for groups of Lie type.

**Theorem 15.** (i) *If $G = A_n$ and $s > 0$, then $\zeta^G(s) \to 1$ as $n \to \infty$.*

(ii) *If $G = G(q)$ is of fixed Lie type with Coxeter number $h$, and $s > \frac{2}{h}$, then $\zeta^G(s) \to 1$ as $q \to \infty$.*

(iii) *For any $s > 0$, there exists $r = r(s)$ such that for $G = G(q)$ of rank at least $r$, we have $\zeta^G(s) \to 1$ as $|G| \to \infty$.*

In part (ii), the *Coxeter number* $h$ of $G(q)$ is defined to be the number of roots in the root system of $G(q)$ divided by the rank; for example, if $G = PSL_n(q)$, $PSp_{2n}(q)$ or $E_8(q)$, $h$ is $n$, $2n$ or 30, respectively. The bound $\frac{2}{h}$ is tight, in that $\zeta^{G(q)}(2/h)$ is bounded away from 1. Moreover, if we write $r_n(G)$ for the number of irreducible characters of degree $n$, then $\zeta^G(s) = \sum_{n \geq 1} r_n(G) n^{-s}$, so for example part (ii) implies that for $G(q)$ of fixed Lie type, $r_n(G(q)) < cn^{2/h}$ for all $n$, where $c$ is an absolute constant.

Theorem 15 also holds for the corresponding *quasisimple* groups – that is, perfect groups $G$ such that $G/Z(G)$ is a finite simple group.

### *1.3.3 Symmetric and alternating groups*

Here we discuss some of the ramifications of the representation space $\mathrm{Hom}(\Gamma, S_n)$. Let us begin the story with a well known result of Conder [13], inspired by the ideas of his supervisor Graham Higman: for $n \geq 168$, $A_n$ is $(2,3,7)$-generated. (There is a reason for the number 168 here: $A_{167}$ is not $(2,3,7)$-generated.) This was part of a more general conjecture, attributed to Higman in the 1960s:

**Higman's Conjecture.** *For any Fuchsian group $\Gamma$, there exists $N(\Gamma)$ such that $\Gamma$ surjects onto $A_n$ for all $n > N(\Gamma)$.*

Conder's result covers the case $\Gamma = T_{2,3,7}$. Higman's conjecture was eventually proved in 2000 by Everitt [22]. One can quickly reduce to the case of genus 0 – for example, a Fuchsian group of genus $g \geq 2$ maps onto the free group $F_2$ on generators $x, y$ (send $a_1 \to x, a_2 \to y$ and all other generators to 1), and then $F_2$ maps onto $A_n$. For the genus 0 case, Everitt's approach was based on constructing generators using Higman's method of coset diagrams.

Inspired by Everitt's result, Liebeck and Shalev started thinking a few years later about whether there might be probabilistic approach to Higman's conjecture: if one could show that $P_\Gamma(A_n) = \mathrm{Prob}(\phi \in \mathrm{Hom}(\Gamma, A_n)$ is epi$)$ tends to 1 (or indeed anything nonzero) as $n \to \infty$, then of course Higman's conjecture would follow.

Our approach to studying $P_\Gamma(A_n)$ was similar to the approach to Dixon's conjecture. Namely, if $\phi \in \mathrm{Hom}(\Gamma, A_n)$ is not an epimorphism, then $\phi(\Gamma) \leq M$ for some maximal subgroup $M$ of $A_n$; and given $M$, this happens with probability $|\mathrm{Hom}(\Gamma, M)|/|\mathrm{Hom}(\Gamma, A_n)|$. Therefore

$$1 - P_\Gamma(A_n) \leq \sum_{M\ max\ A_n} \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, A_n)|}.$$

Hence the task was to estimate $|\mathrm{Hom}(\Gamma, A_n)|$ and also $|\mathrm{Hom}(\Gamma, M)|$ for maximal subgroups $M$. Notice that these estimates must be delicate enough to distinguish between $|\mathrm{Hom}(\Gamma, A_n)|$ and $|\mathrm{Hom}(\Gamma, A_{n-1})|$, since $A_{n-1}$ is one possibility for $M$.

Here is an example of an ingredient of how $|\mathrm{Hom}(\Gamma, A_n)|$ is estimated, for the triangle group $\Gamma = T_{2,3,7}$, taken from [63]. For convenience take $n$ to be divisible by $2 \cdot 3 \cdot 7$ and such that the conjugacy classes $C_1, C_2, C_3$ consisting of fixed-point-free permutations of shapes $(2^{n/2})$, $(3^{n/3})$, $(7^{n/7})$ respectively, all lie in $A_n$. One can prove that for $r = 2, 3, 7$ the following hold:

(i) $|C_r| \sim (n!)^{1-\frac{1}{r}}$, and

(ii) for any $\chi \in \mathrm{Irr}(A_n)$ and $c_r \in C_r$, we have $|\chi(c_r)| < cn^{1/2} \cdot \chi(1)^{1/r}$.

Part (i) is routine, but (ii) is hard and uses much of the well-developed character theory of symmetric groups. If we ignore the $cn^{1/2}$ term in (ii), then, writing $\mathbf{C} = (C_1, C_2, C_2)$, the formula (1.6) gives

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, A_n)| \geq \frac{(n!)^{\frac{1}{2}+\frac{2}{3}+\frac{6}{7}}}{n!}(1 - \sum_{1 \neq \chi \in Irr(A_n)} \frac{\chi(1))^{\frac{1}{2}+\frac{1}{3}+\frac{1}{7}}}{\chi(1)})$$

$$= (n!)^{\frac{43}{42}}\,(1 - (\zeta^{A_n}(\frac{1}{42}) - 1)).$$

Now $\mu(\Gamma) = \mu(T_{2,3,7}) = \frac{1}{42}$, and $\zeta^{A_n}(\frac{1}{42}) \to 1$ as $n \to \infty$ by Theorem 15(i), so for large $n$ this shows that $|\mathrm{Hom}(\Gamma, A_n)|$ is at least roughly $(n!)^{1+\mu(\Gamma)}$. Adapting this calculation to take care of the $cn^{1/2}$ term in (ii) is a fairly routine technical matter.

It turns out that $(n!)^{1+\mu(\Gamma)}$ is the correct order of magnitude for $|\mathrm{Hom}(\Gamma, A_n)|$ and also $|\mathrm{Hom}(\Gamma, S_n)|$. The following result is [63, Theorem 1.2].

**Theorem 16.** *For any Fuchsian group $\Gamma$ we have* $|\mathrm{Hom}(\Gamma, S_n)| = (n!)^{1+\mu(\Gamma)+o(1)}$.

In fact some much more precise estimates were obtained (and were needed, as remarked above). We were also able to prove that the subgroup growth function $a_n(\Gamma) = |\mathrm{Hom}_{\mathrm{trans}}(\Gamma, S_n)|/(n-1)!$ satisfies $a_n(\Gamma) = (n!)^{\mu(\Gamma)+o(1)}$, and establish the following probabilistic result ([63, Theorem 1.7]).

**Theorem 17.** *For any Fuchsian group $\Gamma$, the probability that a random homomorphism in* $\mathrm{Hom}_{\mathrm{trans}}(\Gamma, S_n)$ *is an epimorphism tends to* 1 *as* $n \to \infty$.

This implies Higman's conjecture, which was our original motivation. The character-theoretic methods and estimates in [63] for symmetric and alternating groups have been developed and improved in a number of subsequent papers, notably Larsen-Shalev [44], where very strong estimates on character values are obtained and a variety of applications given; in particular they solve a number of long-standing problems concerning mixing times of random walks on symmetric groups, but we shall not go into this here.

### *1.3.4 Groups of Lie type*

We now discuss results analogous to Theorems 16 and 17 for groups $G = G(q)$ of Lie type. Let $\Gamma$ be a co-compact Fuchsian group as in Section 1.3.1. Again we seek to apply Lemma 8. If $g_i$ ($1 \leq i \leq d$) are elements of $G$ of order dividing $m_i$, and $\chi \in \mathrm{Irr}(G)$, then $\frac{|\chi(g_1)\cdots\chi(g_d)|}{\chi(1)^{2g-2+d}} \leq \chi(1)^{-(2g-2)}$, which quickly yields

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

This observation is only useful when $g \geq 2$, in which case Theorem 15 gives $\zeta^G(2g-2) \to 1$ as $|G| \to \infty$. In this case, applying Lemma 8 and summing over all classes of elements of orders dividing $m_1, \ldots, m_d$ leads to the following result, which is part of [65, 1.2,1.4]. In the statement, $j_m(G)$ denotes the number of elements of $G$ of order dividing $m$.

**Theorem 18.** *Let $\Gamma$ be a co-compact Fuchsian group of genus $g \geq 2$ as in Section* 1.3.1.

(i) *For all finite quasisimple groups $G$,*

$$|\mathrm{Hom}(\Gamma, G)| = (1 + o(1)) \cdot |G|^{2g-1} \cdot \prod_1^d j_{m_i}(G),$$

*where $o(1)$ refers to a quantity which tends to 0 as $|G| \to \infty$.*

(ii) *For groups $G$ of Lie type of rank $r$, $|\mathrm{Hom}(\Gamma, G)| = |G|^{1+\mu(\Gamma)+O(\frac{1}{r})}$.*

Part (ii) follows from (i), since one can show that for groups $G$ of large rank, $j_m(G)$ is roughly $|G|^{1-\frac{1}{m}}$.

As in the previous section, the analysis of the probabilities $P_\Gamma(G)$ is much harder, and for groups of Lie type has only been completed for the case where $g \geq 2$. Here is [65, Theorem 1.6].

**Theorem 19.** *Let $\Gamma$ be a co-compact Fuchsian group of genus $g \geq 2$. Then for all finite simple groups $G$, the probability $P_\Gamma(G) \to 1$ as $|G| \to \infty$.*

Note that the conclusion of the theorem does not remain true for genus 0 or 1, since there are Fuchsian groups of such genus which do not have all sufficiently large finite simple groups as quotients. For example, a result of Macbeath [69] says that $PSL_2(q)$ can only be an image of the genus 0 group $T_{2,3,7}$ if $q = p$ or $p^3$ for some prime $p$. Nevertheless, the genus 0 or 1 case does lead to some very interesting questions which we shall discuss below in Section 1.3.6. For the moment, we conclude this section by stating a conjecture from [65]:

**Conjecture.** *For any Fuchsian group $\Gamma$ there is an integer $f(\Gamma)$ such that for finite simple classical groups $G$ of rank at least $f(\Gamma)$, we have $P_\Gamma(G) \to 1$ as $|G| \to \infty$.*

### *1.3.5 Representation varieties*

Let $\Gamma$ be a Fuchsian group, and let $K = \bar{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$, where $p$ is prime. Recall that the representation variety of $\Gamma$ in dimension $n$ over $K$ is the variety $V = \mathrm{Hom}(\Gamma, GL_n(K))$. One of the most basic questions about $V$ is: what is the dimension of $V$?

This question can be attacked using results in the previous section. Here's how. Let $q$ be a power of the characteristic $p$, and define the field morphism

$\sigma : GL_n(K) \to GL_n(K)$ to be the map sending the matrix $(a_{ij}) \to (a_{ij}^q)$. The fixed point group of $\sigma$ is $GL_n(K)_\sigma = GL_n(q)$. Observe that $\sigma$ also acts on the variety $V$: for $\phi \in V, \gamma \in \Gamma$, define $\phi^\sigma(\gamma) = \phi(\gamma)^\sigma$. Then the fixed point set $V_\sigma = V(q)$ is the finite representation variety $\mathrm{Hom}(\Gamma, GL_n(q))$.

When the genus of $\Gamma$ is at least 2, the size of $\mathrm{Hom}(\Gamma, GL_n(q))$ can be estimated as in the previous section. The connection between this and the dimension of $V$ is given by a classical result of Lang-Weil [42]:

**Lemma 9.** *Let $V$ be an algebraic variety over $\bar{\mathbb{F}}_p$ of dimension $f$, with $e$ components of dimension $f$. For a power $q$ of $p$, let $V(q)$ be the set of $q$-rational points in $V$. Then there is a power $q_0$ of $p$ such that $|V(q)| = (e + o(1))q^f$ for all powers $q$ of $q_0$.*

In estimating $|V(q)| = |\mathrm{Hom}(\Gamma, GL_n(q))|$ we need to know the limiting behaviour of the zeta function $\zeta^{GL_n(q)}(s)$. This is a little different from Theorem 15, because $GL_n(q)$ has $q-1$ linear characters (which contribute $q-1$ to $\zeta^{GL_n(q)}(s)$). The outcome is [65, 2.10]: for $s \geq 2$ and fixed $n$,

$$\zeta^{GL_n(q)}(s) \to q - 1 + \delta \text{ as } q \to \infty,$$

where $\delta = 1$ if $n = s = 2$ and $\delta = 0$ otherwise. Using this $|\mathrm{Hom}(\Gamma, GL_n(q))|$ can be computed as in the previous section. The conclusion is a little awkward to state in general, so we just state it for surface groups and refer the reader to [65, 3.8] for the general case.

**Proposition 1.** *If $\Gamma$ is a surface group of genus $g \geq 2$, then for fixed $n \geq 2$, $|\mathrm{Hom}(\Gamma, GL_n(q))| = (q - 1 + \delta + o(1)) \cdot |GL_n(q)|^{2g-1}$.*

By Lemma 9, this implies

**Theorem 20.** *Let $\Gamma$ be a surface group of genus $g \geq 2$, and let $V$ be the representation variety $\mathrm{Hom}(\Gamma, GL_n(K))$. Then $\dim V = (2g-1)n^2 + 1$, and $V$ has a unique irreducible component of highest dimension.*

Arguing similarly for the varieties $\mathrm{Hom}(\Gamma, \bar{G})$, where $\bar{G} = G(K)$ is a simple algebraic group over $K$, we obtain the following, which is [65, 1.10]. In the statement, $J_m(\bar{G})$ is the subvariety of elements $x \in \bar{G}$ satisfying $x^m = 1$. The dimensions of these subvarieties are studied by Lawther in [46]; in particular, $\dim J_m(\bar{G})$ tends to $(1 - \frac{1}{m}) \dim \bar{G}$ as the rank of $\bar{G}$ tends to infinity.

**Theorem 21.** *Let $\Gamma$ be a Fuchsian group of genus $g \geq 2$ as in Section 1.3.1, and let $\bar{G} = G(K)$ be a simple algebraic group. If $V$ is the variety $\mathrm{Hom}(\Gamma, \bar{G})$, then*

$$\dim V = (2g - 1) \dim \bar{G} + \sum_1^d \dim J_{m_i}(\bar{G}).$$

Other results along these lines can be found in [65].

### *1.3.6 Triangle groups*

All the results in the previous two sections concerning the spaces $\mathrm{Hom}(\Gamma, G)$ for $G$ a finite or algebraic group of Lie type assume that the genus of $\Gamma$ is at least 2. This is not because the genus 0 or 1 cases are uninteresting, but rather because the character-theoretic methods in these cases require much more delicate information. For example, to estimate the sum in the formula (1.6), one needs information on the character values $\chi(g)$ for irreducible characters $\chi$ of $G$, and usable estimates on character values are hard to come by.

As a result, rather little is known about the spaces $\mathrm{Hom}(\Gamma, G)$ and their ramifications when $G$ is a group of Lie type and $\Gamma$ has genus 0 or 1. (Note however that this is not so for $G = S_n$ or $A_n$, since the results of Section 1.3.3 hold for all genera.) Nevertheless there are some results and also conjectures, which make this a very interesting case.

We shall focus on the case for which most is known – namely that in which $\Gamma$ is a triangle group $T_{a,b,c}$ (of genus 0).

**Triangle generation**

Let $T = T_{a,b,c} = \langle x, y, z : x^a = y^b = z^c = xyz = 1\rangle$ be a Fuchsian triangle group (so $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$). We shall say that a finite group $G$ is $(a, b, c)$-*generated* if it is an image of $T$. And for a family of simple groups $G(q)$ of fixed Lie type, we say that $G(q)$ is *randomly* $(a, b, c)$-*generated* if

$$P_T(G(q)) = \mathrm{Prob}(\text{random } \phi \in \mathrm{Hom}(T, G(q)) \text{ is epi}) \to 1$$

as $q \to \infty$ through values for which $a, b$ and $c$ divide $|G(q)|$.

**Question.** *Which finite simple groups of Lie type are (randomly)* $(a, b, c)$*-generated?*

This question goes back quite a long way, particularly in the case where $(a, b, c) = (2, 3, 7)$ – indeed, $(2, 3, 7)$-generated groups are also called *Hurwitz groups*, and are of interest because they are precisely the groups which realize a well known upper bound of Hurwitz for the number of automorphisms of a compact Riemann surface (see [14] for example).

The first substantial result on this question was that of Macbeath [69], who showed that $PSL_2(q)$ is $(2, 3, 7)$-generated if and only if either $q = p \equiv 0, \pm 1 \bmod 7$, or $q = p^3$ and $p \equiv \pm 2, \pm 3 \bmod 7$, where $p$ denotes a prime. Many further results on $(2, 3, 7)$-generation have followed since – for example, $PSL_3(q)$ is only $(2, 3, 7)$-generated if $q = 2$, while $SL_n(q)$ is $(2, 3, 7)$-generated for all $n \geq 287$ (see [88] for a survey).

Concerning $(a, b, c)$-generation for more general values, nothing much was done until the following two results of Marion [71, 73]. In both results, assume $a, b, c$ are *primes* and $a \leq b \leq c$.

**Theorem 22.** *Given a prime $p$, there is a unique power $p^r$ such that $PSL_2(p^r)$ is $(a,b,c)$-generated – namely, the minimal power such that $a, b$ and $c$ divide $|PSL_2(p^r)|$.*

A few moments' thought show that this agrees with Macbeath's result on $(2,3,7)$-generation stated above. In particular, the theorem shows that $PSL_2(q)$ is far from being randomly $(a,b,c)$-generated.

For 3-dimensional classical groups Marion proved

**Theorem 23.** *Let $G = PSL_3(q)$ or $PSU_3(q)$.*

(i) *If $a > 2$, then $G$ is randomly $(a,b,c)$-generated.*

(ii) *If $a = 2$, then given a prime $p$, there are at most four values of $q = p^r$ such that $G$ is $(a,b,c)$-generated.*

The proofs of these two theorems are character-theoretic. The second theorem takes a great deal of effort, and appears in a series of three papers [73]. Using the same methods to tackle higher dimensional groups is not an appetising prospect.

The dichotomy in parts (i) and (ii) of Theorem 23 is quite striking. In seeking to explain it, Marion introduced the idea of rigidity.

### Rigidity

Now switch attention to $\bar{G}$, a simple algebraic group over $K = \bar{\mathbb{F}}_p$, $p$ prime. For $a \geq 2$, define

$$\delta_a = \max\{\dim x^{\bar{G}} : x \in \bar{G} \text{ of order } a\}.$$

Straightforward matrix calculations give

**Lemma 10.** (i) *If $\bar{G} = PSL_2(K)$ then $\delta_a = 2$ for all $a \geq 2$.*

(ii) *If $\bar{G} = PSL_3(K)$ then $\delta_2 = 4$, while $\delta_a = 6$ for $a > 2$.*

For example, consider $G = PSL_3(K)$ with $\mathrm{char}(K) \neq 2$. Any involution $t \in G$ is conjugate to the image modulo scalars of the diagonal matrix $\mathrm{diag}(-1,-1,1)$; then $\dim C_G(t) = 4$ and so $\dim t^G = 4$. On the other hand, for any odd prime $a \neq \mathrm{char}(K)$ there is an element $u \in G$ of order $a$ having distinct eigenvalues, so that $\dim C_G(u) = 2$ and $\dim u^G = 6$.

The relevance of the above definition to $(a,b,c)$-generation is given by

**Proposition 2.** *If $\delta_a + \delta_b + \delta_c < 2 \dim \bar{G}$, then $G(q)$ is not $(a,b,c)$-generated for any $q$.*

This is [72, Prop. 1]. The proof is an application of a well known result of Scott [83] which is one of the main tools in this whole area. Here is a sketch for the case where $p$ is a "very good prime" for $\bar{G}$ – this means that $p$ is not 2 when $\bar{G}$ is symplectic or orthogonal, $p$ is not 2 or 3 when $\bar{G}$ is of exceptional type (and also not 5 when $\bar{G} = E_8$), and $p$ does not divide $n$ when $\bar{G} = PSL_n(K)$.

We consider the action of $\bar{G}$ on its Lie algebra $V = L(\bar{G})$. Under the assumption that $p$ is very good, $G(q)$ acts irreducibly on $V$ for any $q$, and also $\dim C_V(g) = \dim C_{\bar{G}}(g)$ for all $g \in \bar{G}$ (see [12, 1.14]). If $G(q)$ is generated by $x_1, x_2, x_3$ of orders

$a, b, c$ with $x_1x_2x_3 = 1$, then Scott's result implies that $\sum(\dim V - \dim C_V(x_i)) \geq 2\dim V$. As $\dim V = \dim \bar{G}$, this means that $\sum \dim x_i^G \geq 2\dim \bar{G}$, contradicting the hypothesis that $\delta_a + \delta_b + \delta_c < 2\dim \bar{G}$.

The proposition motivates the following definition.

**Definition.** We say that a triple $(a, b, c)$ of primes (with $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$) is *rigid* for $\bar{G}$ if $\delta_a + \delta_b + \delta_c = 2\dim \bar{G}$.

For example, if $\bar{G} = PSL_2(K)$ then $\dim \bar{G} = 3$, so by Lemma 10, every triple is rigid for $\bar{G}$. On the other hand, if $\bar{G} = PSL_3(K)$ then $\dim \bar{G} = 8$ and triples $(2, b, c)$ are rigid, while triples $(a, b, c)$ with $a > 2$ are not (recall that $a \leq b \leq c$).

In view of these examples, Theorems—22 and 23 support the following conjecture, stated in [72].

**Conjecture.** *Let $p$ be a prime and $\bar{G}$ a simple algebraic group over $K = \bar{\mathbb{F}}_p$. Suppose $(a, b, c)$ is a rigid triple of primes for $\bar{G}$. Then there are only finitely many powers $q = p^r$ such that $G(q)$ is $(a, b, c)$-generated.*

Note that the converse to the conjecture does not hold: for example, it is known that $SL_7(q)$ is never a Hurwitz group (see [76]), but $(2, 3, 7)$ is not a rigid triple for $SL_7(K)$. It would be very interesting to find a variant of the conjecture which could work both ways round.

Theorem 3 of [72] classifies all the rigid triples of primes for simple algebraic groups. The list is not too daunting: for $\bar{G} = PSL_n$ or $SL_n$, rigid triples exist only for $n \leq 10$; for symplectic groups, only for dimensions up to 26 (and only the Hurwitz triple $(2, 3, 7)$ can be rigid beyond dimension 10); for orthogonal groups, the only rigid triple is $(2, 3, 7)$ for the groups $\mathrm{Spin}_{11,12}$; and the only exceptional type which has a rigid triple is $G_2$ with triple $(2, 5, 5)$.

As remarked above, one would not want to adopt the character-theoretic method of proof of Theorems 22, 23 for larger rank cases. Fortunately there is another tool which can be used to attack the conjecture, namely the classical notion of rigidity for algebraic groups.

### Classical rigidity

Let $\bar{G}$ be a simple algebraic group over an algebraically closed field $K$, and let $C_1, \ldots, C_r$ be conjugacy classes in $\bar{G}$. Define

$$C_0 = \{(x_1, \ldots, x_r) : x_i \in C_i,\ x_1 \ldots x_r = 1\}.$$

Following [87], we say that $(C_1, \ldots, C_r)$ is a *rigid* tuple of classes if $C_0 \neq \emptyset$ and $G$ acts transitively on $C_0$ by conjugation.

Rigid tuples play a major role in inverse Galois theory and other areas. Their relevance to triangle generation and in particular to the above Conjecture is via the following observations. Assume for convenience of discussion that the characteristic of $K$ is a very good prime for $\bar{G}$.

(1) If $(C_1, C_2, C_3)$ is a rigid triple of classes, and $C_{L(\bar{G})}(x_1, x_2, x_3) = 0$ for $(x_1, x_2, x_3) \in C_0$, then $\sum \dim C_i = 2 \dim \bar{G}$ (see [87, 3.2]).

(2) Suppose one can prove a converse to (1) – namely, that if $(C_1, C_2, C_3)$ is a triple of classes such that $\sum \dim C_i = 2 \dim \bar{G}$ and $C_{L(\bar{G})}(x_1, x_2, x_3) = 0$ for $(x_1, x_2, x_3) \in C_0$, then $(C_1, C_2, C_3)$ is a rigid triple.

(3) Now let $(a, b, c)$ be a rigid triple of primes. Simple algebraic groups have only finitely many classes of elements of any given order, and hence $\bar{G}$ has finitely many triples $(C_1, C_2, C_3)$ of classes of elements of orders $a, b, c$ satisfying $\dim C_i = 2 \dim \bar{G}$ (and the other triples of such classes have dimensions adding to less than $2 \dim \bar{G}$).

Given (1), (2) and (3), define $\mathcal{T}$ to be the set of triples $(g_1, g_2, g_3)$ of elements of $\bar{G}$ of orders $a, b, c$ with product 1 such that $C_{L(\bar{G})}(g_1, g_2, g_3) = 0$ and $\sum \dim C_i = 2 \dim \bar{G}$, where $C_i = g_i^{\bar{G}}$. For $(g_1, g_2, g_3) \in \mathcal{T}$, the triple of classes $(C_1, C_2, C_3)$ is one of the finitely many in (3), and is rigid by (2). It follows that $\bar{G}$ has only finitely many orbits in its conjugation action on $\mathcal{T}$, and so there can be only finitely many groups $G(q)$ generated by such triples $g_1, g_2, g_3$, proving the Conjecture.

Hence, if we can prove the statement in (2), then we can prove the Conjecture. Unfortunately, the only known case of (2) is the following result of Strambach and Völklein [87, 2.3] for $\bar{G} = SL_n$; in the case of characteristic zero it goes back to Katz [40].

**Theorem 24.** *Let $\bar{G} = SL_n(K)$, and let $(C_1, \ldots, C_r)$ be a tuple of classes in $\bar{G}$ such that $\sum \dim C_i = 2 \dim \bar{G}$ and $\langle x_1, \ldots, x_r \rangle$ is irreducible on the natural module $V_n(K)$ for some $(x_1, \ldots, x_r) \in C_0$. Then $(C_1, \ldots, C_r)$ is a rigid tuple.*

The Conjecture follows in the case where $\bar{G} = SL_n$ (see [72] for details). Further cases are handled in [72], but quite a few remain open. The most elegant way to finish the proof would be to prove a version of Theorem 24 for all types of simple algebraic groups, but this seems difficult. One further case – that in which $\bar{G} = G_2$ in characteristic 5 and $(a, b, c) = (2, 5, 5)$ (the only rigid triple of primes for exceptional types) – was handled in [47].

Recently, Larsen, Lubotzky and Marion [43] have introduced the method of deformation theory into the picture, and used it to prove Marion's conjecture for all cases where the underlying characteristic does not divide product $abc$ of the exponents of the triangle group.

## 1.4 Cayley graphs of simple groups: diameter and growth

Let $G$ be a finite group with a generating set $S$ which is symmetric – that is, closed under taking inverses – and does not contain the identity. The *Cayley graph* $\Gamma(G,S)$ is defined to be the graph with vertex set $G$ and edges $\{g, gs\}$ for all $g \in G, s \in S$. It is connected and regular of valency $|S|$, and $G$ acts regularly on $\Gamma(G,S)$ by left multiplication. Because of the transitive action of $G$, the diameter of $\Gamma(G,S)$, denoted by $\mathrm{diam}(G,S)$, is equal to the maximum distance between the identity element and any $g \in G$, and so

$$\mathrm{diam}(G,S) = \max\{l(g) : g \in G\}$$

where $l(g)$ is the length of the shortest expression for $g$ as a product of elements of $S$. If $d = \mathrm{diam}(G,S)$, then $G = \{e\} \cup \bigcup_{r=1}^{d} S^r$ (where $S^r = \{s_1 \dots s_r : s_i \in S\}$), and so $|G| \leq \sum_{r=0}^{d} |S|^r < |S|^{d+1}$. Hence

$$\mathrm{diam}(G,S) > \frac{\log|G|}{\log|S|} - 1. \tag{1.7}$$

**Examples** 1. Let $G = C_n = \langle x \rangle$, a cyclic group of order $n$, and let $S = \{x, x^{-1}\}$. Then $\Gamma(G,S)$ is an $n$-gon. So $\mathrm{diam}(G,S)$ is $[\frac{n}{2}]$, whereas $\frac{\log|G|}{\log|S|}$ is $\frac{\log n}{\log 2}$.

2. Let $G = S_n$ and $S$ the set of all transpositions. Here $\mathrm{diam}(G,S)$ is $n-1$, while $\frac{\log|G|}{\log|S|}$ is roughly $\frac{n}{2}$.

3. Let $G = S_n$ and $S = \{(1\,2),\ (1\,2\cdots n)^{\pm 1}\}$. In this case $\mathrm{diam}(G,S)$ is roughly $n^2$, while $\frac{\log|G|}{\log|S|}$ is of the order of $n \log n$. The same orders of magnitude apply to a similar generating set for $A_n$ consisting of a 3-cycle and an $n$- or $(n-1)$-cycle and their inverses.

4. For $G = SL_n(q)$ and $S$ the set of transvections, we have $\mathrm{diam}(G,S) \approx n$ and $\frac{\log|G|}{\log|S|} \approx \frac{n}{2}$.

5. Let $G = SL_n(p)$ ($p$ prime) and $S = \{x^{\pm 1}, y^{\pm 1}\}$ where

$$x = \begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & . & & \\ & & & . & \\ & & & & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 1 & & & \\ 0 & 0 & 1 & & \\ & & & . & \\ & & & & . \\ \pm 1 & & & & 1 \end{pmatrix}$$

Then $\frac{\log|G|}{\log|S|} \sim n^2 \log p$, and also $\mathrm{diam}(G,S) \sim n^2 \log p$.

All the above examples are elementary except the last, where the fact that $\mathrm{diam}(G,S) \leq Cn^2 \log p$ for some constant $C$ is a result of Kassabov and Riley [39].

Define $\mathrm{diam}(G)$ to be the maximum of $\mathrm{diam}(G,S)$ over all generating sets $S$. The main conjecture in the field is due to Babai, and appears as Conjecture 1.7 in [7]:

**Babai's Conjecture.** *There is a constant $c$ such that $\mathrm{diam}(G) < (\log |G|)^c$ for any non-abelian finite simple group $G$.*

It can be seen from Example 3 above that $c$ must be at least 2 for the conjecture to hold.

There has been a great deal of recent progress on this conjecture, but before presenting some of this we shall discuss the special case where $S$ is a union of conjugacy classes, which has various other connections.

### *1.4.1 Conjugacy classes*

In the case where the generating set $S$ is a union of classes (which occurs in Examples 2 and 4 above), a strong form of Babai's conjecture holds:

**Theorem 25.** *There is a constant $C$ such that for any non-abelian finite simple group $G$ and any non-identity union $S$ of conjugacy classes of $G$,*

$$\mathrm{diam}(G,S) < C\frac{\log |G|}{\log |S|}.$$

*Indeed, $G = S^k$ for all $k \geq C\frac{\log |G|}{\log |S|}$.*

This is the main theorem of [62]. In view of (1.7), the diameter bound is best possible, apart from reduction of the constant $C$.

#### Consequences

First we point out an obvious consequence. If $S$ is the set of involutions in a simple group $G$, then of course $S$ is a union of classes, and it is not hard to prove that $|S| > c|G|^{1/2}$ (see [59, 4.2,4.3]). Hence Theorem 25 implies that every element of every simple group is a product of $k$ involutions, for some absolute constant $k$. The same holds for elements of any fixed order.

A more substantial consequence concerns *word maps* on simple groups. For a group $G$ and a nontrivial word $w = w(x_1, \ldots, x_d)$ in the free group of rank $d$, define

$$w(G) = \{w(g_1, \ldots, g_d) : g_i \in G\},$$

the set of $w$-values in $G$. For example, if $w = [x_1, x_2]$ or $x_1^k$, then $w(G)$ is the set of commutators or $k^{th}$ powers in $G$. Clearly $w(G)$ is a union of classes of $G$.

Given $w$, it is possible to show that there is a constant $c = c(w) > 0$ depending only on $w$, such that $|w(G)| > |G|^c$ for all simple groups $G$ such that $w(G) \neq 1$ (see [62, 8.2]). Hence Theorem 25 gives

**Corollary 8.** *For any nontrivial word $w$, there is a constant $c = c(w)$ such that $w(G)^c = G$ for every finite simple group $G$ for which $w(G) \neq 1$.*

A result of Jones [37] ensures that $w(G) \neq 1$ provided $G$ is sufficiently large (i.e. provided $|G| > f(w)$ where this depends only on $w$). Recent work of Larsen, Shalev and Tiep, culminating in [45], shows that the number $c(w)$ in the corollary can be replaced by 2. So for example, every element of every sufficiently large simple group is product of two commutators or two $k^{th}$ powers, and so on.

Notice that for certain words $w$, it is definitely not possible to replace $c(w)$ by 1. For example the $k^{th}$ power word map $x_1^k$ is not surjective on any finite group of order not coprime to $k$ (since it is not injective). To date, there are just a few instances of word maps which have been shown to be surjective on all simple groups. The first was the commutator word: it was proved in [51] that every element of every non-abelian finite simple group is a commutator, a result known as the Ore conjecture. Some further surjective word maps such as $x_1^p x_2^p$ ($p$ prime) are produced in [28, 52]. One might conjecture that every non-power word map is surjective on sufficiently large simple groups, but this has recently been shown to be false in [36]: for example, the word map $(x, y) \to x^2[x^{-2}, y^{-1}]^2$ is non-surjective on $PSL_2(p^{2r+1})$ for all non-negative integers $r$ and all odd primes $p$ such that $p^2 \not\equiv 1 \bmod 16$ and $p^2 \not\equiv 0, 1 \bmod 5$.

This is one of a number of "width" questions about simple groups. Another is the conjecture proposed in [50], that if $A$ is any subset of size at least 2 in a finite simple group $G$, then $G$ is a product of $N$ conjugates of $A$ for some $N \leq c \log |G| / \log |A|$, where $c$ is an absolute constant. This has been proved in some cases in [49, 50, 24].

### *1.4.2 Babai's Conjecture*

There have been spectacular recent developments on Babai's conjecture, both for groups of Lie type and for alternating groups. We shall discuss these separately.

#### Groups of Lie type

For a long time, even $SL_2(p)$ ($p$ prime) was a mystery as far as proving Babai's conjecture was concerned. Probably the first small (symmetric) generating set one thinks of for this group is

$$S = \{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\pm 1} \}.$$

Babai's conjecture asserts that $\mathrm{diam}(G, S) < (\log p)^c$ for these generators. Surely this must be easy?

In fact it is not at all easy, and was proved by the following beautiful but indirect method (see [66]). First observe that the matrices in $S$, when regarded as integer matrices, generate $SL_2(\mathbb{Z})$. Now let $\Gamma(p)$ denote the congruence subgroup which

is the kernel of the natural map from $SL_2(\mathbb{Z}) \to SL_2(p)$. If $\mathbb{H}$ is the upper half plane and $X(p)$ denotes the Riemann surface $\Gamma(p)\backslash\mathbb{H}$, denote by $\lambda_1(X(p))$ the smallest eigenvalue for the Laplacian on $X(p)$. A theorem of Selberg [84] gives $\lambda_1(X(p)) \geq \frac{3}{16}$ for all $p$, and this can be used to show that the Cayley graphs $\{\Gamma_p = \Gamma(SL_2(p), S) : p \text{ prime}\}$ have their second largest eigenvalues bounded away from the valency, and hence that they form a family of *expander graphs*. This means that there is an *expansion* constant $c > 0$, independent of $p$, such that for every set $A$ consisting of fewer that half the total number of vertices in $\Gamma_p$, we have $|\delta A| > c|A|$, where $\delta A$ is the boundary of $A$ – that is, the set of vertices not in $A$ which are joined to some vertex in $A$. From the expansion property it is easy to deduce that $\Gamma_p$ has logarithmic diameter, so that $\mathrm{diam}(\Gamma(SL_2(p), S) < c \log p$, a strong form of Babai's conjecture.

One can adopt essentially the same method for the generators

$$\{\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{\pm 1}\}$$

of $SL_2(p)$, since, while these do not generate $SL_2(\mathbb{Z})$, they do generate a subgroup of finite index therein. But what if we replace the 2s in these generators with 3s? Then the matrices generate a subgroup of infinite index in $SL_2(\mathbb{Z})$, and the above method breaks down. This question became known as Lubotzky's 1-2-3 problem, as was not solved until the breakthrough achieved by Helfgott [31]:

**Theorem 26.** *Babai's conjecture holds for $G = SL_2(p)$. That is, $\mathrm{diam}(SL_2(p)) < (\log p)^c$, where $c$ is an absolute constant.*

Helfgott deduced this from his key proposition: for any generating set $S$ of $G = SL_2(p)$, either $|S^3| > |S|^{1+\epsilon}$, or $S^k = G$, where $\epsilon > 0$ and $k$ do not depend on $p$. (Later it was observed that one can take $k = 3$ here.) The heart of his proof is to relate the growth of powers of subsets $A$ of $G$ with the growth of the corresponding set of scalars $B = \mathrm{tr}(A) = \{\mathrm{tr}(x) : x \in A\}$ in $\mathbb{F}_p$ under sums and products. By doing this he could tap into the theory of additive combinatorics, using results such as the following, taken from [9]: if $B$ is a subset of $\mathbb{F}_p$ with $p^\delta < |B| < p^{1-\delta}$ for some $\delta > 0$, then $|B \cdot B| + |B + B| > |B|^{1+\epsilon}$, where $\epsilon > 0$ depends only on $\delta$.

Following Helfgott's result, there was a tremendous surge of progress in this area. Many new families of expanders were constructed in [8]. Helfgott himself extended his result to $SL_3$ in [32], and this has now been proved for all groups of Lie type of bounded rank in [10, 82]. As a consequence, we have

**Theorem 27.** *If $G = G(q)$ is a simple group of Lie type of rank $r$, then $\mathrm{diam}(G) < (\log |G|)^{c(r)}$ where $c(r)$ depends only on $r$.*

Again, the theorem is proved via a growth statement: for any generating set $S$ of $G(q)$, either $|S^3| > |S|^{1+\epsilon}$, or $S^3 = G$, where $\epsilon > 0$ depends only on $r$.

These results, and particularly their developments into the theory of expanders, have many wonderful and surprising applications. For a survey of these developments and some of the applications, see [68].

Finally, let us remark that Babai's conjecture remains open for groups of Lie type of unbounded rank.

### Alternating groups

For the alternating groups $A_n$, Babai's conjecture is that there is a constant $C$ such that $\mathrm{diam}(A_n) < n^C$. Until very recently, the best bound for $\mathrm{diam}(A_n)$ was that obtained by Babai and Seress in [6], where it was proved that

$$\mathrm{diam}(A_n) < \exp((1+o(1)) \cdot (n \log n)^{1/2}) = \exp((1+o(1)) \cdot (\log |A_n|)^{1/2}).$$

Babai and Seress also obtained a bound of the same magnitude for the diameter of an arbitrary subgroup of $S_n$ in [7]; this is best possible, as can be seen by constructing a cyclic subgroup generated by a permutation with many cycles of different prime lengths. Various other partial results appeared at regular intervals, such as that in [5], where it was shown that if the generating set $S$ contains a permutation of degree at most $0.33n$, then $\mathrm{diam}(A_n, S)$ is polynomially bounded. But no real progress was made on Babai's conjecture until a recent breakthrough of Helfgott and Seress [33]:

**Theorem 28.** *We have* $\mathrm{diam}(A_n) \leq \exp(O((\log n)^4 \log\log n))$*, where the implied constant is absolute.*

This does not quite prove Babai's conjecture, but it does prove that $\mathrm{diam}(A_n)$ is "quasipolynomial" (where a quasipolynomial function $f(n)$ is one for which $\log f(n)$ is polynomial in $\log n$), which represents a big step forward. The same paper also gives a bound of the same magnitude for the diameter of any transitive subgroup of $S_n$.

## References


1. M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.
2. M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, *J. Algebra* **90** (1984), 446–460.
3. M. Aschbacher and L. Scott, Maximal subgroups of finite groups, *J. Algebra* **92** (1985), 44–80.
4. L. Babai, The probability of generating the symmetric group, *J. Combin. Theory Ser. A* **52** (1989), 148–153.
5. L. Babai, R. Beals and A. Seress, On the diameter of the symmetric group: polynomial bounds, Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms, 1108–1112, ACM, New York, 2004.
6. L. Babai and A. Seress, On the diameter of Cayley graphs of the symmetric group, *J. Combin. Theory Ser. A* **49** (1988), 175–179.
7. L. Babai and A. Seress, On the diameter of permutation groups, *European J. Combin.* **13** (1992), 231–243.
8. J. Bourgain and A. Gamburd, Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$, *Annals of Math.* **167** (2008), 625–642.
9. J. Bourgain, N. Katz and T. Tao, A sum-product estimate in finite fields, and applications, *Geom. Funct. Anal.* **14** (2004), 27–57.

10. E. Breuillard, B. Green and T. Tao, Approximate subgroups of linear groups, available at arXiv:1005.1881.
11. T.C. Burness, M.W. Liebeck and A. Shalev, Generation and random generation: from simple groups to maximal subgroups, preprint, available at http://eprints.soton.ac.uk/151795.
12. R.W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Pure and Appl. Math., Wiley-Interscience, New York, 1985.
13. M.D.E. Conder, Generators for alternating and symmetric groups, *J. London Math. Soc.* **22** (1980), 75–86.
14. M.D.E. Conder, Hurwitz groups: a brief survey, *Bull. Amer. Math. Soc.* **23** (1990), 359–370.
15. F. Dalla Volta and A. Lucchini, Generation of almost simple groups, *J. Algebra* **178** (1995), 194–223.
16. E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group, *J. Algebra* **265** (2003), 651–668.
17. J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.
18. J.D. Dixon, Asymptotics of generating the symmetric and alternating groups, *Electron. J. Combin.* **12** (2005), 1–5.
19. J.D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**, Springer-Verlag, New York, 1996.
20. E.B. Dynkin, Semisimple subalgebras of semisimple Lie algebras, *Translations Amer. Math. Soc.* **6** (1957), 111-244.
21. P. Erdös and P. Turán, On some problems of a statistical group-theory II, *Acta Math. Acad. Sci. Hungar.* **18** (1967), 151–163.
22. B. Everitt, Alternating quotients of Fuchsian groups, *J. Algebra* **223** (2000), 457–476.
23. R.K. Fisher, The number of non-solvable sections in linear groups, *J. London Math. Soc.* **9** (1974), 80–86.
24. N. Gill, I. Short, L. Pyber and E. Szabó, On the product decomposition conjecture for finite simple groups, available at arXiv:1111.3497.
25. R.M. Guralnick and W.M. Kantor, Probabilistic generation of finite simple groups, *J. Algebra* **234** (2000), 743–792.
26. R. Guralnick, M. Larsen and P. H. Tiep, Representation growth in positive characteristic and conjugacy classes of maximal subgroups, *Duke Math. J.*, to appear, available at arXiv:1009.2437v2.
27. R.M. Guralnick, M.W. Liebeck, J. Saxl and A. Shalev, Random generation of finite simple groups, *J. Algebra* **219** (1999), 345–355.
28. R.M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.
29. P. Hall, The Eulerian functions of a group, *Quart. J. Math.* **7** (1936), 134–151.
30. J. Häsä, Growth of cross-characteristic representations of finite quasisimple groups of Lie type, preprint.
31. H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, *Annals of Math.* **167** (2008), 601–623.
32. H.A. Helfgott, Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, *J. Eur. Math. Soc.* **13** (2011), 761–851.
33. H.A. Helfgott and A. Seress, On the diameter of permutation groups, available at arXiv:1109.3550.
34. B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967.
35. A. Jaikin-Zapirain and L. Pyber, Random generation of finite and profinite groups and group enumeration, *Annals of Math.* **173** (2011), 769–814.
36. S. Jambor, M.W. Liebeck and E.A. O'Brien, Some word maps that are non-surjective on infinitely many finite simple groups, preprint, available at arXiv:1205.1952.
37. G. A. Jones, Varieties and simple groups, *J. Austral. Math. Soc.* **17** (1974), 163–173.
38. W.M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), 67–87.
39. M. Kassabov and T.R. Riley, Diameters of Cayley graphs of Chevalley groups, *European J. Combin.* **28** (2007), 791–800.

40. N. Katz, *Rigid local systems*, Princeton University Press, 1996.
41. P. Kleidman and M.W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press, 1990.
42. S. Lang and A. Weil, Number of points of varieties over finite fields, *Amer. J. Math.* **76** (1954), 819–827.
43. M. Larsen, A. Lubotzky and C. Marion, Deformation theory and finite simple quotients of triangle groups, preprint.
44. M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Invent. Math.* **174** (2008), 645–687.
45. M. Larsen, A. Shalev and P.H. Tiep, Waring problem for finite simple groups, *Annals of Math.* **174** (2011), 1885–1950.
46. R. Lawther, Elements of specified order in simple algebraic groups, *Trans. Amer. Math. Soc.* **357** (2005), 221–245.
47. M.W. Liebeck, A.J. Litterick and C. Marion, A rigid triple of conjugacy classes in $G_2$, *J. Group Theory* **14** (2011), 31–35.
48. M.W. Liebeck, B.M.S. Martin and A. Shalev, On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function, *Duke Math. J.* **128** (2005), 541–557.
49. M.W. Liebeck, N. Nikolov and A. Shalev, A conjecture on product decompositions in simple groups, *Groups Geom. Dyn.* **4** (2010), 799–812.
50. M.W. Liebeck, N. Nikolov and A. Shalev Product decompositions in finite simple groups, *Bull. London Math. Soc.*, to appear, available at arXiv:1107.1528.
51. M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, The Ore conjecture, *J. Eur. Math. Soc.* **12** (2010), 939–1008.
52. M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, Products of squares in finite simple groups, *Proc. Amer. Math. Soc.* **140** (2012), 21–33.
53. M.W. Liebeck, L. Pyber and A. Shalev, On a conjecture of G. E. Wall, *J. Algebra* **317** (2007), 184–197.
54. M.W. Liebeck and G.M. Seitz, Maximal subgroups of exceptional groups of Lie type, finite and algebraic, *Geom. Dedicata* **36** (1990), 353–387.
55. M.W. Liebeck and G.M. Seitz, On the subgroup structure of exceptional groups of Lie type', *Trans. Amer. Math. Soc.* **350** (1998), 3409–3482.
56. M.W. Liebeck and G.M. Seitz, On finite subgroups of exceptional algebraic groups, *J. Reine Angew. Math.* **515** (1999), 25–72.
57. M.W. Liebeck and G.M. Seitz, The maximal subgroups of positive dimension in exceptional algebraic groups, *Mem. Amer. Math. Soc.* **169** (2004), No. 802, 1–227.
58. M.W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113.
59. M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the $(2,3)$-generation problem, *Annals of Math.* **144** (1996), 77–125.
60. M.W. Liebeck and A. Shalev, Maximal subgroups of symmetric groups, *J. Combin. Theory Ser. A* **75** (1996), 341–352.
61. M.W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra* **184** (1996), 31–57.
62. M.W. Liebeck and A. Shalev, Diameters of simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383–406.
63. 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.
64. 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.
65. M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties, *Invent. Math.* **159** (2005), 317–367.
66. A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Progress in Mathematics, vol. 125, Birkhäuser Verlag, Basel, 1994.
67. A. Lubotzky, The expected number of random elements to generate a finite group, *J. Algebra* **257** (2002), 452–459.

68. A. Lubotzky, Expander Graphs in Pure and Applied Mathematics, available at arXiv:1105.2389.
69. A. M. Macbeath, Generators of the linear fractional groups, *Proc. Sympos. Pure Math.*, vol. XII (American Mathematical Society, 1969), pp.14–32.
70. A. Mann, Positively finitely generated groups, *Forum Math.* **8** (1996), 429–459.
71. C. Marion, Triangle groups and $\mathrm{PSL}_2(q)$, *J. Group Theory* **12** (2009), 689–708.
72. C. Marion, On triangle generation of finite groups of Lie type, *J. Group Theory* **13** (2010), 619–648.
73. C. Marion, Random and deterministic triangle generation of three-dimensional classical groups I-III, *Comm. in Alg.*, to appear.
74. A. Maroti and M.C. Tamburini, Bounds for the probability of generating the symmetric and alternating groups, *Arch. Math.* **96** (2011), 115–121.
75. B.M.S. Martin, Reductive subgroups of reductive groups in nonzero characteristic, *J. Algebra* **262** (2003), 265–286.
76. L. Di Martino, M. C. Tamburini and A. E. Zalesskii, On Hurwitz groups of low rank, *Comm. in Alg.* **28** (2000), 5383–5404.
77. N. E. Menezes, M. R. Quick and C. M. Roney-Dougal, The probability of generating a finite simple group, preprint.
78. G.A. Miller, On the groups generated by two operators, *Bull. Amer. Math. Soc.* **7** (1901), 424–426.
79. E. Netto, *The theory of substitutions and its applications to algebra*, Second edition, Chelsea Publishing Co., New York 1964 (first published in 1892).
80. I. Pak, On probability of generating a finite group, preprint, available at http://www.math.ucla.edu/ pak.
81. I. Pak, What do we know about the product replacement algorithm?, Groups and computation, III (Columbus, OH, 1999), 301–347, Ohio State Univ. Math. Res. Inst. Publ. **8**, de Gruyter, Berlin, 2001.
82. L. Pyber and E. Szabó, Growth in finite simple groups of Lie type of bounded rank, available at arXiv:1005.1858.
83. L. L. Scott, Matrices and cohomology, *Annals of Math.* **105** (1977), 473–492.
84. A. Selberg, On the estimation of Fourier coefficients of modular forms, *Proc. Symp. Pure Math.* **8** (1965), 1–15.
85. R. Steinberg, Generators for simple groups, *Canad. J. Math.* **14** (1962), 277–283.
86. R. Steinberg, Endomorphisms of linear algebraic groups, *Mem. Amer. Math. Soc.*, No. 80 (1968), pp.1–108.
87. K. Strambach and H. Völklein, On linearly rigid tuples, *J. Reine Angew. Math.* **510** (1999), 57–62.
88. M.C. Tamburini and M. Vsemirnov, Hurwitz groups and Hurwitz generation, Handbook of algebra Vol. 4, pp.385–426, Elsevier/North-Holland, Amsterdam, 2006.
89. 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.
90. J. Whiston, Maximal independent generating sets of the symmetric group, *J. Algebra* **232** (2000), 255–268.