SIMPLE GROUPS, GENERATION AND PROBABILISTIC METHODS

TIMOTHY C. BURNESS*

*School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
Email: t.burness@bristol.ac.uk

Abstract

It is well known that every finite simple group can be generated by two elements and this leads to a wide range of problems that have been the focus of intensive research in recent years. In this survey article we discuss some of the extraordinary generation properties of simple groups, focussing on topics such as random generation, (a, b)-generation and spread, as well as highlighting the application of probabilistic methods in the proofs of many of the main results. We also present some recent work on the minimal generation of maximal and second maximal subgroups of simple groups, which has applications to the study of subgroup growth and the generation of primitive permutation groups.

1 Introduction

In this survey article we will discuss some of the remarkable generation properties of finite simple groups. Our starting point is the fact that every finite simple group can be generated by just two of its elements (this is essentially a theorem of Steinberg [70], and the proof requires the Classification of Finite Simple Groups). This leads naturally to a wide range of interesting questions concerning the abundance of generating pairs and their distribution across the group, which have been intensively studied in recent years. Our goal in Sections 2 and 3 is to survey some of the main results and open problems.

Another one of our aims is to highlight the central role played by probabilistic methods. In some instances, the given result may already be stated in probabilistic terms (for example, it may refer to the probability that two randomly chosen elements in a group form a generating pair). However, we will see that probabilistic techniques have also been used in an essential way to prove entirely deterministic statements. A striking example is given by Guralnick and Kantor's proof of the so-called $\frac{3}{2}$-*generation* property for simple groups, which we will discuss in Section 3, together with some far-reaching generalisations.

Our understanding of the subgroups of finite simple groups has advanced greatly in recent years. In particular, many results on the generation of simple groups rely on powerful subgroup structure theorems such as the O'Nan–Scott theorem for alternating groups and Aschbacher's theorem for classical groups. In a different direction, it is natural to consider the generation properties of the subgroups themselves, such as maximal and second maximal subgroups that are located at the top of the subgroup lattice. Indeed, we can seek to understand the extent to which

some of the remarkable results for simple groups extend to these subgroups (with suitable modifications, if necessary). The study of problems of this nature was recently initiated through joint work with Liebeck and Shalev and we will discuss some of the main results in Section 4.

The coverage of this article is based on the content of my one-hour lecture at the *Groups St Andrews* conference, which was hosted by the University of Birmingham in August 2017. It is a pleasure to thank the organisers for inviting me to give this lecture and for planning and delivering a very interesting and inspiring meeting. There is a vast literature on the generation of simple groups and so I have had to be very selective in choosing the main topics for this article, which is rather biased towards my own tastes and interests. There are many other excellent survey articles on related topics, which an interested reader may wish to consult. For example, Shalev has written several interesting articles on the use of probabilistic methods in finite group theory, which discuss applications to generation problems and much more (see [68], for example). Liebeck's survey article [40] on probabilistic group theory provides an excellent account of some of the more recent developments.

Let us say a few words on the notation used in this article. In general, our notation is all fairly standard (and new notation will be defined when needed). It might be helpful to point out that we use the notation of [37] for simple groups. For example, we will write $\mathrm{L}_n(q) = \mathrm{PSL}_n(q)$ and $\mathrm{U}_n(q) = \mathrm{PSU}_n(q)$ for linear and unitary groups, and we use $\mathrm{P}\Omega_n^+(q)$, etc., for simple orthogonal groups (this differs from the notation used in the Atlas [19]).

Finally, I would like to thank Scott Harper for helpful comments on an earlier version of this article.

2 Generation properties of simple groups

Let G be a finite group and let

$$d(G) = \min\{|S| \,:\, G = \langle S \rangle\}$$

be the minimal number of generators for G. We will say that G is *n-generated* if $d(G)$ is at most n. In this section we will focus on the generation properties of simple groups, which is an area of research with a long and rich history. Here the most well-known result is the fact that every finite simple group can be generated by two elements.

Theorem 2.1 *Every finite simple group is 2-generated.*

The proof relies on the Classification of Finite Simple Groups. First observe that the alternating groups are straightforward. For example, it is an easy exercise to show that

$$A_n = \begin{cases} \langle (1,2,3), (1,2,\ldots,n) \rangle & n \text{ odd} \\ \langle (1,2,3), (2,3,\ldots,n) \rangle & n \text{ even} \end{cases}$$

In [70], Steinberg presents explicit generating pairs for each simple group of Lie type. For instance, $\mathrm{L}_2(q) = \langle xZ, yZ \rangle$, where $Z = Z(\mathrm{SL}_2(q))$ and

$$x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \quad y = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

with $\mathbb{F}_q^\times = \langle \alpha \rangle$. In [3], Aschbacher and Guralnick complete the proof of the theorem by showing that every sporadic group is 2-generated.

In view of Theorem 2.1, there are many natural extensions and variations to consider. For example:

1. *How abundant are generating pairs in a finite simple group?*
2. *Can we find generating pairs of prescribed orders?*
3. *Does every non-identity element belong to a generating pair?*

As we shall see, problems of this flavour have been the focus of intensive research in recent years, with probabilistic methods playing a central role in the proofs of many of the main results.

2.1 Random generation

Let G be a finite group, let k be a positive integer and let

$$\mathbb{P}_k(G) = \frac{|\{(x_1, \ldots, x_k) \in G^k \,:\, G = \langle x_1, \ldots, x_k \rangle\}|}{|G|^k}$$

be the probability that k randomly chosen elements generate G. For a simple group G, Theorem 2.1 implies that $\mathbb{P}_2(G) > 0$ and it is natural to consider the asymptotic behaviour of $\mathbb{P}_2(G)$ with respect to $|G|$. This is an old problem, which can be traced all the way back to a conjecture of Netto in 1882. In [61], Netto writes

> *"If we arbitrarily select two or more substitutions of n elements, it is to be regarded as extremely probable that the group of lowest order which contains these is the symmetric group, or at least the alternating group."*

In other words, Netto is predicting that $\mathbb{P}_2(A_n) \to 1$ as n tends to infinity. This conjecture was proved by Dixon [21] in a highly influential paper published in 1969, which relies in part on the pioneering work of Erdős and Turán [24] on statistical properties of symmetric groups. In the same paper, Dixon makes the bold conjecture that *all* finite simple groups are strongly 2-generated in the sense of Netto.

Conjecture 2.2 (Dixon, 1969) *Let (G_n) be any sequence of finite simple groups such that $|G_n|$ tends to infinity with n. Then $\mathbb{P}_2(G_n) \to 1$ as $n \to \infty$.*

The proof of Dixon's conjecture was eventually completed in the 1990s. In [35], Kantor and Lubotzky establish the result for classical groups and low rank exceptional groups, and the remaining groups of Lie type were handled by Liebeck and Shalev [43]. The proof is based on the following elementary observations.

Let G be a finite group and let $\mathcal{M}$ be the set of maximal subgroups of G. Set

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

for a real number $s > 0$. For randomly chosen elements $x, y \in G$, observe that $G \neq \langle x, y \rangle$ if and only if $x, y \in H$ for some $H \in \mathcal{M}$. Since $|G : H|^{-2}$ is the probability that these random elements are both contained in H, it follows that

$$1 - \mathbb{P}_2(G) \leqslant \sum_{H \in \mathcal{M}} |G : H|^{-2} = \zeta_G(2).$$

Now assume G is a finite simple group of Lie type. By carefully studying $\mathcal{M}$, using powerful results on the subgroup structure of these groups, such as Aschbacher's theorem [1] for classical groups, one can show that $\zeta_G(2) \to 0$ as $|G|$ tends to infinity. Therefore $\mathbb{P}_2(G) \to 1$ and Dixon's conjecture follows.

It is interesting to note that this probabilistic argument shows that every sufficiently large finite simple group of Lie type is 2-generated, without the need to explicitly construct a pair of generators. Numerous extensions have since been established. For example, the following striking result is [58, Theorem 1.1].

Theorem 2.3 *We have $\mathbb{P}_2(G) \geqslant 53/90$ for every non-abelian finite simple group G, with equality if and only if $G = A_6$.*

It turns out that convergence in Conjecture 2.2 is rather rapid and strong bounds on $\mathbb{P}_2(G)$ have been established for all simple groups G. For example, [60, Theorem 1.1] gives

$$1 - \frac{1}{n} - \frac{8.8}{n^2} \leqslant \mathbb{P}_2(A_n) \leqslant 1 - \frac{1}{n} - \frac{0.93}{n^2}$$

for all $n \geqslant 5$. More generally, by [44, Theorem 1.6], there are absolute constants $c_1, c_2 > 0$ such that

$$1 - \frac{c_1}{m(G)} \leqslant \mathbb{P}_2(G) \leqslant 1 - \frac{c_2}{m(G)}$$

for all finite simple groups G, where $m(G)$ denotes the minimal index of a proper subgroup of G. Note that $m(A_n) = n$. We refer the reader to [28, Table 4] for a convenient list of the precise values of $m(G)$ when G is a simple group of Lie type.

2.2 (a, b)-generation

Another interesting refinement of Theorem 2.1 is to ask if it is possible to find a pair of generators of prescribed orders. With this in mind, for positive integers a and b, let us say that a finite group G is (a, b)-*generated* if $G = \langle x, y \rangle$ with $|x| = a$ and $|y| = b$. It is natural to assume that both a and b are primes, at least one of which is odd (since any group generated by two involutions is dihedral). Here the special case $(a, b) = (2, 3)$ is particularly interesting because a group is $(2, 3)$-generated if and only if it is a quotient of the modular group $\mathrm{PSL}_2(\mathbb{Z}) \cong Z_2 \star Z_3$. The $(2, 3)$-generation problem for simple groups has been widely studied for more than a century and one of the main results is the following.

Theorem 2.4 *All sufficiently large non-abelian finite simple groups are* $(2,3)$*-generated, with the exception of* $\mathrm{PSp}_4(2^f)$*,* $\mathrm{PSp}_4(3^f)$ *and* ${}^2B_2(q)$*.*

This follows from an old theorem of Miller [59] for alternating groups, which reveals that A_n is $(2,3)$-generated unless $n \in \{6,7,8\}$. The result for classical groups was proved by Liebeck and Shalev [45] and the exceptional groups were handled by Lübeck and Malle in [49]. More precisely, the latter paper shows that *every* simple exceptional group of Lie type is $(2,3)$-generated, except for $G_2(2)' \cong \mathrm{U}_3(3)$ and of course the Suzuki groups ${}^2B_2(q)$, which do not contain elements of order 3 (Suzuki [71] showed that these groups are $(2,5)$-generated). For completeness, let us record that every sporadic simple group is $(2,3)$-generated, except for M_{11}, M_{22}, M_{23} and McL (see [74]).

For classical groups, Liebeck and Shalev adopt a probabilistic approach in [45], which uses several results on the maximal subgroups of classical groups, such as Aschbacher's theorem [1] and its extensions. As one might expect, detailed information on the conjugacy classes of elements of order 2 and 3 also plays an important role in the proofs. In [49], Lübeck and Malle adopt rather different techniques to study the $(2,3)$-generation of exceptional groups. Indeed, their main methods are character-theoretic, using the Deligne–Lusztig theory for reductive groups over finite fields.

Let us briefly sketch the main ideas in [45]. For positive integers a and b, let $\mathbb{P}_{a,b}(G)$ be the probability that G is generated by randomly chosen elements of order a and b, so G is (a,b)-generated if and only if $\mathbb{P}_{a,b}(G) > 0$. It is easy to see that

$$1 - \mathbb{P}_{a,b}(G) \leqslant \sum_{H \in \mathcal{M}} \frac{i_a(H) i_b(H)}{i_a(G) i_b(G)}, \tag{2}$$

where $\mathcal{M}$ is the set of maximal subgroups of G as before, and $i_m(X)$ is the number of elements of order m in X. By carefully estimating $i_2(H)$ and $i_3(H)$ for $H \in \mathcal{M}$, Liebeck and Shalev show that there is an absolute constant c such that

$$\sum_{H \in \mathcal{M}} \frac{i_2(H) i_3(H)}{i_2(G) i_3(G)} < \sum_{H \in \mathcal{M}} c|G:H|^{-66/65} = c \cdot \zeta_G(66/65)$$

for any finite simple classical group $G \neq \mathrm{PSp}_4(q)$, where $\zeta_G(s)$ is the zeta function in (1) (see [45, Theorems 2.2 and 2.3]). The result now follows from [45, Theorem 2.1], which states that for any $s > 1$, $\zeta_G(s) \to 0$ as $|G| \to \infty$ (note that $\zeta_G(1)$ is equal to the number of conjugacy classes of maximal subgroups of G, which tends to infinity with $|G|$). Moreover, by combining this result with [45, Proposition 6.3], we get the following natural analogue of Conjecture 2.2 for the $(2,3)$-generation of classical groups.

Theorem 2.5 *For finite simple classical groups* G*, as* $|G| \to \infty$ *we have*

$$\mathbb{P}_{2,3}(G) \to \begin{cases} 0 & \text{if } G = \mathrm{PSp}_4(p^f) \text{ with } p = 2 \text{ or } 3 \\ \frac{1}{2} & \text{if } G = \mathrm{PSp}_4(p^f) \text{ with } p \neq 2,3 \\ 1 & \text{otherwise.} \end{cases}$$

Using a similar approach, the main theorem of [46] shows that if a and b are primes, not both equal to 2, then $\mathbb{P}_{a,b}(G) \to 1$ as $|G| \to \infty$, for all simple classical groups G of sufficiently large rank (a sufficient bound on the rank can be given as a function of a and b).

Remark 2.6 A complete classification of the $(2,3)$-generated finite simple groups remains out of reach, but there has been significant progress by Di Martino, Pellegrini, Tamburini, Vavilov and others, using constructive methods. For example, Pellegrini [64] has very recently resolved the $(2,3)$-generation problem for the linear groups $\mathrm{L}_n(q)$; the only exceptions arise when $(n,q) \in \{(2,9),(3,4),(4,2)\}$, all of which are $(2,5)$-generated. In their recent survey article [65], Pellegrini and Tamburini make the interesting observation that $\Omega_8^+(2)$ and $\mathrm{P}\Omega_8^+(3)$ are the only known simple classical groups with natural module of dimension $n \geqslant 8$ that are not $(2,3)$-generated.

To conclude this section, let us briefly discuss the more general $(2,r)$-generation problem. By a theorem of Malle, Saxl and Weigel [53, Theorem B], every finite simple group G is $(2,r)$-generated for some integer $r \geqslant 3$. In fact, for $G \neq \mathrm{U}_3(3)$, it is proved that G is generated by an involution and a strongly real element (that is, an element x so that $x^{-1} = y^{-1}xy$ for some involution y), which immediately implies that G is generated by 3 involutions (one can show that 4 involutions are needed for $\mathrm{U}_3(3)$). The following refinement of King [36] shows that r can be taken to be a prime.

Theorem 2.7 *Let G be a non-abelian finite simple group. Then there exists a prime r such that G is $(2,r)$-generated.*

Once again, the proof uses probabilistic methods and we give a brief sketch of the main steps. In view of earlier work, we may assume G is a classical group over $\mathbb{F}_q$, with natural module of dimension n. By applying the bound in (2) (with $a = 2$ and $b = 5$), King shows that the symplectic groups $\mathrm{PSp}_4(2^f)$ and $\mathrm{PSp}_4(3^f)$ are $(2,5)$-generated. By combining this observation with previous results in the literature, the problem can be reduced to classical groups with $n \geqslant 8$. To tackle these groups, we need to recall the notion of a primitive prime divisor.

Definition 2.8 For integers $q, e \geqslant 2$, a prime divisor r of $q^e - 1$ is a *primitive prime divisor* (ppd for short) if r does not divide $q^i - 1$ for each $1 \leqslant i < e$.

By a classical theorem of Zsigmondy [75], such a prime r exists unless $(q,e) = (2^a - 1, 2)$ or $(2,6)$. Let r be a ppd of $q^e - 1$, where $e = e(n)$ is maximal with respect to the condition that r divides $|G|$. For instance, $e = n$ if $G = \mathrm{L}_n(q)$ or $\mathrm{PSp}_n(q)$, and $e = n - 2$ if $G = \mathrm{P}\Omega_n^+(q)$. Let $x \in G$ be an element of order r and let $\mathcal{M}(x)$ be the set of maximal subgroups of G containing x.

For $(2,r)$-generation, it suffices to show that $\mathbb{P}_2(G,x) > 0$, where $\mathbb{P}_2(G,x)$ is the probability that x and a randomly chosen involution generate G. Now

$$1 - \mathbb{P}_2(G,x) \leqslant \sum_{H \in \mathcal{M}(x)} \frac{i_2(H)}{i_2(G)} \tag{3}$$

and this essentially reduces the argument to determining $\mathcal{M}(x)$ and then counting the involutions in each $H \in \mathcal{M}(x)$. By choosing r to be a ppd of $q^e - 1$ with $e > n/2$, we can appeal to [30], which uses Aschbacher's theorem [1] to determine the maximal subgroups of G containing elements of order r. It follows that the subgroups in $\mathcal{M}(x)$ are very restricted and this makes it easier to estimate the upper bound in (3). This approach is effective in almost all cases, with only a handful of low-dimensional groups requiring further attention (see [36, Section 7]).

Notice that King's proof does not yield an absolute bound on the prime r in the statement of the theorem (indeed, r tends to infinity with the rank of the group). However, it is natural to ask if there is an absolute constant R such that every finite simple group is $(2, r)$-generated for some prime $r \leqslant R$. In view of the above results, it is not difficult to show that $r \leqslant 5$ if G is an alternating or sporadic group, and King's proof shows that $r \leqslant 7$ if G is a classical group with natural module of dimension $n \leqslant 7$ (the group $\mathrm{U}_3(3)$ is neither $(2, 3)$ nor $(2, 5)$-generated). The bound $r \leqslant 7$ also holds for exceptional groups of Lie type. This leads us naturally to the following conjecture of Conder, which is still open.

Conjecture 2.9 (Conder, 2015) *Every non-abelian finite simple group is* $(2, r)$*-generated for some* $r \in \{3, 5\}$*, except for* $\mathrm{U}_3(3)$*, which is* $(2, 7)$*-generated.*

2.3 Triangle generation

Let a, b and c be positive integers with $a \leqslant b \leqslant c$. We say that a group G is (a, b, c)-*generated* if $G = \langle x, y\rangle$ for elements $x, y \in G$ such that $|x|$, $|y|$ and $|xy|$ divide a, b and c, respectively. This is equivalent to the condition that G is a quotient of the *triangle group*

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

The problem of determining the finite simple quotients of triangle groups has attracted significant attention for more than a century. One of the main motivations stems from a famous theorem of Hurwitz from 1893, which states that $|\mathrm{Aut}(S)| \leqslant 84(g - 1)$ for any compact Riemann surface S of genus $g \geqslant 2$, with equality if and only if $\mathrm{Aut}(S)$ is a $(2, 3, 7)$-group (these groups are called *Hurwitz groups*). There has been substantial progress towards a classification of simple Hurwitz groups, but this remains an open problem (see [18] for a nice survey of results). One of the highlights is the following theorem of Conder [17], which settles a conjecture of Higman from the 1960s asserting that all but finitely many alternating groups are Hurwitz.

Theorem 2.10 *The alternating group* A_n *is a Hurwitz group for all* $n \geqslant 168$*, and for all but* 64 *integers in the range* $3 \leqslant n \leqslant 167$*.*

For the remainder of this section, we will discuss some more recent results concerning the triangle generation of finite simple groups and related problems.

Let G be a simple algebraic group over an algebraically closed field K of characteristic $p > 0$. For a fixed triple (a, b, c) of integers, it is natural to ask if there

are any values of r such that the corresponding finite quasisimple group $G(p^r)$ is (a,b,c)-generated. Here we may assume that (a,b,c) is *hyperbolic*, which means that

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}<1.$$

Indeed, if this condition is not satisfied, then either $T_{a,b,c}$ is soluble, or $(a,b,c)=(2,3,5)$ and $T_{a,b,c}\cong A_5$. In [52], Macbeath proves that $\mathrm{L}_2(p^r)$ is Hurwitz if and only if $r=1$ and $p\equiv 0,\pm 1 \pmod 7$, or $r=3$ and $p\equiv \pm 2,\pm 3 \pmod 7$. This is extended by Marion in [55, Corollary 1], which states that if (a,b,c) is a hyperbolic triple of primes and p is any prime number, then $\mathrm{L}_2(p^r)$ is (a,b,c)-generated if and only if p^r is the smallest power of p such that $\mathrm{lcm}(a,b,c)$ divides $|\mathrm{L}_2(p^r)|$ (in particular, r is unique).

To shed further light on Marion's result for $\mathrm{L}_2(p^r)$, we need some additional terminology. For a positive integer m, let $j_m(G)$ be the dimension of the subvariety of G of elements of order dividing m. Let us say that a triple (a,b,c) of positive integers is *rigid* for G if

$$j_a(G)+j_b(G)+j_c(G)=2\dim G. \tag{4}$$

We can now state the following conjecture (see [56, p.621]).

Conjecture 2.11 (Marion, 2010) *Fix a prime p and let G be a simple algebraic group over an algebraically closed field of characteristic $p>0$. If (a,b,c) is a rigid hyperbolic triple of primes for G, then there are only finitely many positive integers r such that $G(p^r)$ is (a,b,c)-generated.*

In the special case $G=\mathrm{PSL}_2(K)$ we have $\dim G=3$ and $j_m(G)=2$ for all $m\geqslant 2$, so every triple is rigid for G and thus the conclusion of the conjecture is in agreement with [55, Corollary 1], as stated above. Significant progress towards a proof of the conjecture is made in [56], where Marion reduces the problem to a handful of cases with

$$G=\mathrm{Sp}_{2m}(K)\ (\text{for } m\leqslant 13),\ \mathrm{PSp}_4(K) \text{ or } G_2(K).$$

To do this, one first determines the rigid hyperbolic triples of primes for G, which is a relatively straightforward exercise using the known dimensions of conjugacy classes of elements of prime order in simple algebraic groups. The rigidity condition in (4) is highly restrictive. For instance, if G is an exceptional group, then $G=G_2(K)$ with $(a,b,c)=(2,5,5)$ is the only possibility.

To complete the reduction, the main step is to eliminate a handful of linear groups $G=\mathrm{SL}_n(K)$. Here the main tool is a well-known theorem of Scott [67], which is used to show that $\mathrm{GL}_n(K)$ has only finitely many orbits on the set

$$\{(x,y,z)\in G^3 \,:\, x^a=y^b=z^c=1,\ xyz=1,\ \langle x,y\rangle \text{ irreducible}\},$$

where a subgroup of G is said to be irreducible if it acts irreducibly on the natural module for G. Up to conjugacy in $\mathrm{GL}_n(K)$, it follows that there are only finitely

many irreducible (a, b, c)-generated subgroups of G, which immediately gives the desired result in these cases.

Using a completely different approach, Larsen, Lubotzky and Marion [38] apply tools from deformation theory to study a generalised version of Conjecture 2.11, where the prime condition on the triple (a, b, c) is dropped. The main result is [38, Theorem 1.7], which establishes this extended form of the conjecture unless p divides $abcd$, where d is the determinant of the Cartan matrix of G. This result has recently been pushed further in [34], which proves the extended conjecture for all simple groups $G(p^r)$. As in [56], the approach in [34] relies heavily on the classification of hyperbolic rigid triples (with no prime conditions) and most of the work involves the case $G = \mathrm{PSp}_4(K)$ with $(a, b) = (3, 3)$, which requires special attention and different techniques.

Conjecture 2.11 for quasisimple groups is still open, even for prime triples. It is also worth noting that the converse to the conjecture is false. For example, $(2, 3, 7)$ is non-rigid for $G = \mathrm{SL}_7(K)$, but $\mathrm{SL}_7(q)$ is never a Hurwitz group for any prime power q (see [56, p.623] for further details and examples).

Natural extensions of triangle generation can be studied by observing that every hyperbolic triangle group $T_{a,b,c}$ is a special type of *Fuchsian group*. This broader family of groups arises naturally in geometry and combinatorial group theory (formally, a Fuchsian group is a finitely generated non-elementary discrete group of isometries of the hyperbolic plane $\mathbb{H}^2$). An orientation-preserving Fuchsian group Γ has a rather simple presentation, with generators

$$a_1, b_1, \ldots, a_g, b_g,\ x_1, \ldots, x_d,\ y_1, \ldots, y_s,\ z_1, \ldots, z_t$$

and relations

$$x_1^{m_1} = \cdots = x_d^{m_d} = 1,\ x_1 \cdots x_d y_1 \cdots y_s z_1 \cdots z_t [a_1, b_1] \cdots [a_g, b_g] = 1$$

with $g, d, s, t \geqslant 0$ and $m_i \geqslant 2$ for all i. Here $g \geqslant 0$ is called the *genus* of Γ (the non-orientation-preserving groups admit a similar presentation). In this setting, a triangle group corresponds to the situation where $g = s = t = 0$ and $d = 3$, so it is natural to extend the notion of triangle generation by considering the finite quotients of arbitrary Fuchsian groups.

A number of remarkable results in this direction have been established in recent years. For instance, Everitt [25] has shown that if Γ is an oriented Fuchsian group, then all but finitely many alternating groups are quotients of Γ. This establishes a conjecture of Higman (in the oriented case), which generalises Conder's theorem on Hurwitz groups (see Theorem 2.10). Everitt's approach in [25] builds on the coset-diagram methodology developed by Higman and Conder. By applying very different methods, using a combination of character-theoretic and probabilistic tools, Liebeck and Shalev prove the following theorem, which settles Higman's conjecture in full generality (see [47, Theorem 1.7]). In the statement, we use the notation

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

Theorem 2.12 *Let Γ be a Fuchsian group. Then the probability that a random homomorphism in $\mathrm{Hom}_{\mathrm{trans}}(\Gamma, A_n)$ is an epimorphism tends to 1 as $n \to \infty$.*

Numerous extensions are pursued in [48], where A_n is replaced by a different simple group. For example, the following striking result is [48, Theorem 1.6].

Theorem 2.13 *Let Γ be a Fuchsian group of genus $g \geqslant 2$ ($g \geqslant 3$ if non-oriented), and let G be a finite simple group. Then the probability that a randomly chosen homomorphism in $\mathrm{Hom}(\Gamma, G)$ is an epimorphism tends to 1 as $|G| \to \infty$.*

The condition on the genus here is essential, since there are Fuchsian groups of genus 0 or 1 which do not have all large enough finite simple groups as quotients. Indeed, we have already seen that if (a, b, c) is a hyperbolic triple of primes then $\mathrm{L}_2(p^r)$ is a quotient of $T_{a,b,c}$ for just one value of r. For arbitrary Fuchsian groups, the following conjecture is still open (see [48, p.323]).

Conjecture 2.14 (Liebeck & Shalev, 2005) *For any Fuchsian group Γ there is an integer $f(\Gamma)$, such that if G is a finite simple classical group of rank at least $f(\Gamma)$, then the probability that a randomly chosen homomorphism in $\mathrm{Hom}(\Gamma, G)$ is an epimorphism tends to 1 as $|G| \to \infty$.*

3 Spread

In the previous section, we highlighted several strong 2-generation properties of simple groups, which can be viewed as far-reaching generalisations of Theorem 2.1. In this section we study the notions of spread and uniform spread, which provide yet another way to demonstrate the effortless 2-generation of simple groups.

3.1 Definitions

We begin with the following definition, which was introduced by Brenner and Wiegold [8] in the 1970s.

Definition 3.1 Let G be a finite group and let k be a positive integer. Then G has *spread* k if for any non-identity elements $x_1, \ldots, x_k \in G$ there exists $y \in G$ such that $G = \langle x_i, y \rangle$ for all i. We say that G is $\frac{3}{2}$*-generated* if it has spread 1.

One of the main motivations stems from earlier work of Binder [4], who proved that S_n has spread 2 for all $n \geqslant 5$ (in fact, there is an even earlier result of Piccard [66] from the 1930s, which states that both A_n and S_n are $\frac{3}{2}$-generated if $n \geqslant 5$).

Notice that every cyclic group has spread k for all $k \in \mathbb{N}$, so for the remainder of Section 3 we will assume G is non-cyclic. Set

$$s(G) = \max\{k \in \mathbb{N}_0 \,:\, G \text{ has spread } k\}.$$

In practice, it can often be more convenient to work with the more restrictive notion of *uniform spread*, which was formally introduced much more recently in [10].

Definition 3.2 A finite group G has *uniform spread* k if there exists a fixed conjugacy class C of G such that for any non-identity elements $x_1, \ldots, x_k \in G$ there exists $y \in C$ such that $G = \langle x_i, y \rangle$ for all i.

For a non-cyclic group G, set

$$u(G) = \max\{k \in \mathbb{N}_0 : G \text{ has uniform spread } k\}$$

and observe that $u(G) \leqslant s(G) < |G| - 1$. Note that the first inequality can be strict; for example, $u(S_6) = 0$ and $s(S_6) = 2$.

3.2 The spread of simple groups

In [8], Brenner and Wiegold extend the earlier work of Binder and Piccard by investigating the spread of various families of simple groups. Among several interesting results, they prove that $s(A_{2n}) = 4$ for all $n \geqslant 4$ and they show that

$$s(\mathrm{L}_2(q)) = \begin{cases} q-1 & \text{if } q \equiv 1 \pmod 4 \\ q-4 & \text{if } q \equiv 3 \pmod 4 \\ q-2 & \text{if } q \text{ is even} \end{cases}$$

for $q \geqslant 11$ (see [8, Theorems 3.10 and 4.02]). In particular, the spread of a finite simple group can be arbitrarily large.

They also observe that the spread of odd degree alternating groups is radically different. For instance, [8, Theorem 4.01] states that

$$6098892799 \leqslant s(A_{19}) \leqslant 6098892803. \tag{5}$$

Later work by Guralnick and Shalev [31] shows that $s(A_p)$ tends to infinity with p when p is a prime number. More generally, [31, Theorem 1.1] implies that if (G_i) is a sequence of alternating groups such that $G_i = A_{n_i}$ and n_i tends to infinity with i, then $s(G_i) \to \infty$ if and only if $f(n_i) \to \infty$, where $f(n_i)$ is the smallest prime divisor of n_i.

In Steinberg's original paper [70], where he presents a generating pair for each simple group of Lie type, he suggests that these groups may have the much stronger $\frac{3}{2}$-generation property (he is aware of Piccard's result for alternating groups). Steinberg's prediction was eventually verified almost 40 years later (in a stronger form) by Stein [69], and independently by Guralnick and Kantor [29].

Theorem 3.3 *If G is a non-abelian finite simple group, then $u(G) \geqslant 1$.*

Stronger results are established in [29], which turn out to be important for subsequent improvements of the bound in Theorem 3.3. More precisely, it is shown that there is a conjugacy class C of G such that each non-identity element of G generates G with at least $1/10$ of the elements in C, and they also establish some related results for almost simple groups. In later work [10], Breuer, Guralnick and Kantor show that the constant $1/10$ can be improved to $13/42$ (for $G = \Omega_8^+(2)$,

this is best possible), and by excluding a short list of known groups, 1/10 can be replaced by 2/3.

As we shall see below, the fact that the above fraction 1/10 can be replaced by 2/3 in almost all cases is the key ingredient in the proof of the following theorem, which is the main result on the spread of simple groups (see [10, Corollary 1.3]).

Theorem 3.4 *Let G be a non-abelian finite simple group. Then $u(G) \geqslant 2$, with equality if and only if $G \in \{A_5, A_6, \Omega_8^+(2), \mathrm{Sp}_{2m}(2)\,(m \geqslant 3)\}$.*

The proof of Theorem 3.4 uses probabilistic methods, based on fixed point ratio estimates. To describe the main ideas, we need some notation.

Let G be a finite group. For $x, y \in G$, let

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

be the probability that x and a randomly chosen conjugate of y generate G. Set

$$Q(x,y) = 1 - \mathbb{P}(x,y).$$

For a subgroup $H \leqslant G$ and element $x \in G$, let

$$\mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|}$$

be the *fixed point ratio* of x. This is the proportion of fixed points of x under the natural action of G on the set of cosets of H in G. Notice that $\mathrm{fpr}(x, G/H) \leqslant \mathrm{fpr}(x^m, G/H)$ for all $m \in \mathbb{N}$.

Lemma 3.5 *Suppose there exists an element $y \in G$ and a positive integer k such that $Q(x,y) < 1/k$ for all $1 \neq x \in G$. Then $u(G) \geqslant k$.*

Proof Let $x_1, \ldots, x_k \in G$ be non-identity elements and set $E = E_1 \cap \cdots \cap E_k$, where E_i is the event that $G = \langle x_i, z\rangle$ for a randomly chosen conjugate $z \in y^G$. Then

$$\begin{aligned}\mathbb{P}(E) = 1 - \mathbb{P}(\bar{E}) &= 1 - \mathbb{P}(\bar{E}_1 \cup \cdots \cup \bar{E}_k) \\ &\geqslant 1 - \sum_{i=1}^{k} \mathbb{P}(\bar{E}_i) = 1 - \sum_{i=1}^{k} Q(x_i, y) > 1 - k \cdot \frac{1}{k} = 0\end{aligned}$$

and the result follows. □

Notice that if we can find a conjugacy class $C = y^G$ with the property that each non-identity element of G generates G with at least 2/3 of the elements in C, then $Q(x,y) < 1/3$ for all $1 \neq x \in G$ and thus $u(G) \geqslant 3$ by Lemma 3.5. This is the main strategy adopted in the proof of Theorem 3.4.

In order to effectively apply Lemma 3.5, we need to be able to estimate the probability $Q(x,y)$. Here the key result is the following lemma (as before, we define $\mathcal{M}(y)$ to be the set of maximal subgroups of G containing y).

Lemma 3.6 *For $x, y \in G$, we have*

$$Q(x,y) \leqslant \sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H).$$

Proof If $z \in y^G$ then $G \neq \langle x, z\rangle$ if and only if $\langle x', y\rangle \leqslant H$ for some $x' \in x^G$ and $H \in \mathcal{M}(y)$. Therefore,

$$Q(x,y) \leqslant \sum_{H \in \mathcal{M}(y)} \mathbb{P}_x(H),$$

where

$$\mathbb{P}_x(H) = \frac{|x^G \cap H|}{|x^G|} = \mathrm{fpr}(x, G/H)$$

is the probability that a random conjugate of x lies in H. The result follows. □

If we can find an element $y \in G$ and a positive integer k such that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) < \frac{1}{k}$$

for all $x \in G$ of prime order, then by combining Lemmas 3.5 and 3.6 we deduce that $u(G) \geqslant k$. To do this effectively, we need to identify an element $y \in G$ that is contained in very few maximal subgroups of G, and we need to be able to determine the subgroups in $\mathcal{M}(y)$. We then require upper bounds on the appropriate fixed point ratios for elements of prime order. Such bounds are useful in many different contexts and there is an extensive literature to draw upon. For example, if G is a group of Lie type over $\mathbb{F}_q$ then there is the general upper bound $\mathrm{fpr}(x, G/H) \leqslant 4/3q$ due to Liebeck and Saxl [41] (with prescribed exceptions). See [12, 39] and [29, Section 3] for stronger bounds in special cases.

Notice that there is some considerable flexibility in this approach. There is not always an obvious candidate for y, and in practice there may be many valid possibilities (although some choices will require more work than others in estimating the upper bound in Lemma 3.6).

To illustrate some of the main ideas in the proof of Theorem 3.4, let us look at three examples.

Example 3.7 Suppose $G = A_n$, where $n \geqslant 8$ is even. We will use Lemma 3.6 to show that $u(G) \geqslant 3$ (recall that $s(G) = 4$ by [8, Theorem 3.10]). Set $n = 2m$, $k = m - (2, m-1)$ and

$$y = (1, 2, \ldots, k)(k+1, \ldots, n) \in G.$$

First we determine the maximal overgroups in $\mathcal{M}(y)$. To do this, suppose $H \in \mathcal{M}(y)$ and consider the action of H on $\{1, \ldots, n\}$. If H is intransitive, then it is clear that $H = (S_k \cap S_{n-k}) \cap G$ is the only possibility (that is, H has to be the setwise stabiliser in G of $\{1, \ldots, k\}$). Since k and $n-k$ are coprime, it is easy to rule out imprimitive subgroups, so we may assume H is primitive. Here it is

helpful to observe that y^{n-k} is a k-cycle and $1 < k < n/2$, so a classical theorem of Marggraf from 1889 (see [73, Theorem 13.5]) implies that $H = G$ and we reach a contradiction. Therefore, $\mathcal{M}(y) = \{H\}$ with $H = (S_k \cap S_{n-k}) \cap G$, and the action of G on G/H is equivalent to the action of G on the k-element subsets of $\{1, \ldots, n\}$. It is straightforward to show that $\mathrm{fpr}(x, G/H) < 1/3$ for all $x \in G$ of prime order (see the proof of [10, Proposition 6.3]), whence

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) < \frac{1}{3}$$

and thus $u(G) \geqslant 3$ via Lemmas 3.5 and 3.6.

Remark 3.8 The analysis of odd degree alternating groups is more complicated. In this situation, we cannot choose an element $y \in A_n$ with exactly two cycles, so one may be forced to work with an element that is contained in several maximal subgroups. Still, some special cases are easy to handle. For example, if $G = A_{19}$ and y is a 19-cycle, then $\mathcal{M}(y) = \{H\}$ with

$$H = N_G(\langle y \rangle) = \mathrm{AGL}_1(19) \cap G = Z_{19}{:}Z_9$$

and one can check that

$$\mathrm{fpr}(x, G/H) \leqslant \frac{1}{6098892800}$$

for all $x \in G$ of prime order (with equality if $x \in G$ has cycle-shape $[3^6, 1]$). Therefore, $u(G) \geqslant 6098892799$, which agrees with the lower bound on $s(G)$ in (5).

Example 3.9 Suppose $G = E_8(q)$ and let $y \in G$ be a generator of a maximal torus of order $r = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$. By a theorem of Weigel (see case (j) in [72, Section 4]), we have $\mathcal{M}(y) = \{H\}$ with $H = N_G(\langle y \rangle) = Z_r{:}Z_{30}$. Since $|x^G| > q^{58}$ for all $x \in G$ of prime order (minimal if x is a long root element), we deduce that

$$\mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|} < \frac{|H|}{q^{58}} < q^{-44}$$

and thus $u(G) \geqslant q^{44}$.

Example 3.10 Suppose $G = \mathrm{PSp}_{2m}(q)$ is a symplectic group, where $m \geqslant 6$ is even and q is odd. Let V be the natural module for G. Following [10, Proposition 5.10], fix a semisimple element $y \in G$ that preserves an orthogonal decomposition $V = U \perp W$, where U and W are nondegenerate subspaces of dimension 4 and $2m - 4$, respectively. Moreover, assume that y acts irreducibly on both U and W. Since U and W are the only proper nonzero subspaces of V preserved by y, it follows that the stabiliser of U in G (a subgroup of type $\mathrm{Sp}_4(q) \times \mathrm{Sp}_{2m-4}(q)$) is the only reducible subgroup in $\mathcal{M}(y)$.

In order to determine the irreducible subgroups in $\mathcal{M}(y)$, it is very helpful to observe that $|y|$ is divisible by a primitive prime divisor of $q^{2m-4} - 1$ (see Definition

2.8). Recall that the subgroups of classical groups containing such elements are studied in [30], where the analysis is organised according to Aschbacher's subgroup structure theorem (see [1]). By carefully applying the main theorem of [30], it is possible to severely restrict the subgroups in $\mathcal{M}(y)$. Indeed, one can show that there are only two irreducible subgroups in $\mathcal{M}(y)$, both of which are field extension subgroups of type $\mathrm{Sp}_m(q^2)$ (see [10, Proposition 5.10]). We now need to estimate fixed point ratios for the appropriate actions.

Suppose $x \in G$ has prime order. If H is the reducible subgroup of type $\mathrm{Sp}_4(q) \times \mathrm{Sp}_{2m-4}(q)$, then [29, Proposition 3.16] gives

$$\mathrm{fpr}(x, G/H) < 2q^{2-m} + q^{-m} + q^{-2} + q^{4-2m}.$$

Similarly, if H is of type $\mathrm{Sp}_m(q^2)$ then [10, Lemma 3.4] yields

$$\mathrm{fpr}(x, G/H) < q^{3-2m}.$$

Putting all this together, we conclude that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) < 2q^{2-m} + q^{-m} + q^{-2} + q^{4-2m} + 2q^{3-2m} < \frac{1}{3}$$

for all $m \geqslant 6$ and $q \geqslant 3$, whence $u(G) \geqslant 3$.

The spread of sporadic groups has also been the subject of several papers, giving upper and lower bounds (see [5, 6, 26, 27] for example). For example, the best known result on the spread of the Monster $\mathbb{M}$ gives

$$3385007637938037777290624 \leqslant s(\mathbb{M}) \leqslant 579174806851198263694425937 4$$

(see [27, Theorem 1]). It is interesting to note that M_{11} and M_{23} are the only sporadic simple groups for which the exact spread has been computed: we have $s(\mathrm{M}_{11}) = 3$ and $s(\mathrm{M}_{23}) = 8064$.

3.3 Almost simple groups and generating graphs

We can extend the study of spread and uniform spread to the broader class of almost simple groups. Recall that a finite group G is *almost simple* if

$$T \leqslant G \leqslant \mathrm{Aut}(T)$$

for some non-abelian finite simple group T (the socle of G). The following theorem on minimal generation is due to Dalla Volta and Lucchini (see [20, Theorem 1]).

Theorem 3.11 *Let G be an almost simple group with socle T. Then*

$$d(G) = \max\{2, d(G/T)\} \leqslant 3.$$

It is not difficult to see that this bound is best possible. For instance, if we take $G = \mathrm{Aut}(\mathrm{L}_n(q))$, where nq is odd and $q = p^{2f}$ with p a prime, then the elementary abelian group $(Z_2)^3$ is a homomorphic image of G, whence $d(G) = 3$.

Let G be an almost simple group with socle T. In this more general setting, it is still possible to establish a slightly weaker spread-two property. Indeed, [10, Corollary 1.5] states that for any pair of non-identity elements $x_1, x_2 \in G$, there exists $y \in G$ such that $\langle x_i, y\rangle$ contains T, for $i = 1, 2$. Of course, some sort of modified statement is needed because $s(G) = 0$ if G/T is non-cyclic (indeed, if $1 \neq x \in T$ and $G = \langle x, y\rangle$ for some $y \in G$, then $G/T = \langle Ty\rangle$). In view of this observation, it is interesting to consider the spread and uniform spread of almost simple groups of the form $G = \langle T, x\rangle$ for some automorphism x of T.

Further motivation for studying this situation comes from a remarkable conjecture of Breuer, Guralnick and Kantor (see [10, Conjecture 1.8]).

Conjecture 3.12 (Breuer et al., 2008) *Let G be a finite group. Then $s(G) \geqslant 1$ if and only if G/N is cyclic for every nontrivial normal subgroup N of G.*

In recent work, Guralnick has established a reduction of this conjecture to almost simple groups and various special cases have been established. For instance, almost simple sporadic groups are handled in [10], while the desired result for symmetric groups was proved by Binder [4] (as previously noted). More precisely, these results show that $s(G) \geqslant 2$ for every almost simple group G with an alternating or sporadic socle T and cyclic quotient G/T. For groups of Lie type, progress so far has focussed on certain families of classical groups, starting with the main theorem of [13], which shows that $s(G) \geqslant 2$ when $T = \mathrm{L}_n(q)$.

To do this, our initial aim is to establish the bound $u(G) \geqslant 2$ using the same probabilistic approach as before, via Lemmas 3.5 and 3.6. Although the underlying strategy is the same, the details in the almost simple setting are significantly more complicated. Indeed, if our given group is $G = \langle T, x\rangle$ then we have to identify a suitable conjugacy class y^G for some element y in the coset Tx. Here the main challenge is to determine the maximal overgroups of such an element y and various techniques are needed to do this, which depend on the specific type of automorphism x. For instance, if x is a field automorphism, then we use the theory of *Shintani descent* for algebraic groups to identify an appropriate element $y \in Tx$ (see [13, Section 2.6] for further details).

Using similar methods, the results in [13] have recently been extended by Harper [32] to the classical groups with socle $T = \mathrm{PSp}_n(q)$ and $\Omega_n(q)$ (with nq odd in the latter case). Further work to complete the analysis of almost simple groups of Lie type is in progress, with the ultimate goal of completing the proof of Conjecture 3.12.

Finally, to conclude this section we briefly explain how some of the above results can be cast in terms of the *generating graph* of a finite group, which leads to some interesting open problems.

Definition 3.13 Let G be a finite group. The *generating graph* $\Gamma(G)$ is a graph

on the non-identity elements of G so that two vertices x, y are joined by an edge if and only if $G = \langle x, y \rangle$.

For a 2-generated group G, this graph encodes some interesting generation properties of the group. For example, G is $\frac{3}{2}$-generated if and only if $\Gamma(G)$ has no isolated vertices. Similarly, if $s(G) \geqslant 2$ then $\Gamma(G)$ is connected with diameter at most 2. In this way, we obtain an appealing interplay between groups and graphs, leading to a number of natural questions. For instance, what is the (co)-clique number and chromatic number of $\Gamma(G)$? Does $\Gamma(G)$ contain a Hamiltonian cycle (i.e. a cycle that visits every vertex exactly once)? etc. The following theorem brings together some of the main results on the generating graph of a finite simple group.

Theorem 3.14 *Let G be a non-abelian finite simple group and let $\Gamma(G)$ be its generating graph.*

(i) *$\Gamma(G)$ has no isolated vertices.*

(ii) *$\Gamma(G)$ is connected and has diameter 2.*

(iii) *$\Gamma(G)$ contains a Hamiltonian cycle if $|G|$ is sufficiently large.*

Proof Clearly, (ii) implies (i), and (ii) is an immediate corollary of Theorem 3.4. Part (iii) is [11, Theorem 1.2]. □

It is worth noting that the proof of (iii) uses probabilistic methods in the sense that it relies on the proof of Dixon's conjecture (see Conjecture 2.2). Roughly speaking, if $|G|$ is large then $\mathbb{P}_2(G)$ is close to 1, which translates into lower bounds on the degrees of the vertices in $\Gamma(G)$. If these bounds are sufficiently large (relative to $|G|$), then one can appeal to *Pósa's criterion* (in our setting, if $m = |G| - 1$ and $d_1 \leqslant \cdots \leqslant d_m$ are the vertex degrees, then the condition we need is $d_k \geqslant k + 1$ for all $1 \leqslant k < m/2$) to force the existence of a Hamiltonian cycle and this is how the proof of (iii) proceeds in [11].

It is conjectured that the generating graph of *every* non-abelian finite simple group contains a Hamiltonian cycle. In fact, the following stronger conjecture is proposed in [11] (see [11, Conjecture 1.6]).

Conjecture 3.15 (Breuer et al., 2010) *Let G be a finite group with $|G| \geqslant 4$. Then $\Gamma(G)$ contains a Hamiltonian cycle if and only if G/N is cyclic for every nontrivial normal subgroup N of G.*

Notice that the condition on quotients here is identical to the one in Conjecture 3.12. Of course, it is clear that this is a necessary condition for Hamiltonicity, but it is rather striking that it is also conjectured to be sufficient. By [11, Proposition 1.1], the conjecture holds for all soluble groups and it has been verified for the simple groups $\mathrm{L}_2(q)$ (see [9, Section 6]). There has also been recent progress for alternating groups by Erdem [23], who has proved that $\Gamma(A_n)$ is Hamiltonian if $n \geqslant 4100$.

We finish by formulating another conjecture, which combines and strengthens Conjectures 3.12 and 3.15.

Conjecture 3.16 Let G be a finite group with $|G| \geqslant 4$. Then the following are equivalent:

(i) G has spread 1.
(ii) G has spread 2.
(iii) $\Gamma(G)$ has no isolated vertices.
(iv) $\Gamma(G)$ is connected.
(v) $\Gamma(G)$ is connected with diameter at most 2.
(vi) $\Gamma(G)$ contains a Hamiltonian cycle.
(vii) G/N is cyclic for every nontrivial normal subgroup N.

Notice that this conjecture implies that there is no finite group with $s(G) = 1$. It also gives the following remarkable dichotomy for generating graphs: either $\Gamma(G)$ has an isolated vertex, or it is connected with diameter at most 2. Given the proof of Conjecture 3.15 for soluble groups in [11], it is not too difficult to verify the conjecture in the soluble case. However, it is very much an open problem for insoluble groups.

4 Generating subgroups of simple groups

In this final section, we investigate the generation properties of subgroups of simple groups. As we have seen repeatedly in Sections 2 and 3, many questions concerning the generation of simple groups can be reduced to problems involving their maximal subgroups. However, there are very few results in the literature on the generation properties of these subgroups themselves. For example, it is natural to consider the extent to which some of the familiar results for simple groups (such as 2-generation and random generation, as in Dixon's conjecture) can be extended to certain subgroups of interest, with appropriate modifications (if necessary). The goal of this section is to address some of these questions; the main references are [14] and [15].

Let G be a finite group and recall that $d(G)$ denotes the minimal number of generators for G. Notice that d is not a monotonic function, in the sense that a subgroup H of G may require more generators. For instance, if n is even, then the elementary abelian subgroup $\langle (1,2), (3,4), \ldots, (n-1,n) \rangle$ of S_n needs $n/2$ generators, but $S_n = \langle (1,2), (1,2,\ldots,n) \rangle$ is 2-generated. In this setting, there is an attractive theorem of McIver and Neumann (see [57, Lemma 5.2]), which states that $\max\{d(H) : H \leqslant S_n\} = \lfloor n/2 \rfloor$ for all $n \geqslant 4$, so there is some control on the required number of generators for a subgroup of S_n. More generally, we can bound $d(H)$ in terms of $d(G)$ and its index $[G : H]$.

Lemma 4.1 *If G is a finitely generated group and $H \leqslant G$ has finite index, then*

$$d(H) \leqslant [G : H](d(G) - 1) + 1.$$

Proof Let F be the free group on $d(G)$ generators, so $G = F/K$ and $H = L/K$ for some subgroups $K \leqslant L \leqslant F$. Since $[F : L] = [G : H]$ is finite, the Nielsen–Schreier

index formula implies that $d(L) = [F : L](d(F) - 1) + 1$. Therefore

$$d(H) = d(L/K) \leqslant d(L) = [G : H](d(G) - 1) + 1$$

and the result follows. □

The following example shows that the upper bound in Lemma 4.1 is sharp, even for maximal subgroups.

Example 4.2 Let $p \geqslant 3$ be a prime and consider the group $G = (Z_2)^{p+1}{:}Z_p$, where Z_p cyclically permutes the first p copies of Z_2 in the direct product $(Z_2)^{p+1}$. Set $H = (Z_2)^{p+1}$. Then H is a maximal subgroup of G and it is easy to see that $d(G) = 2$ and $d(H) = p + 1 = [G : H] + 1$.

4.1 Maximal subgroups

Let G be an almost simple group with socle T and recall that $d(G) \leqslant 3$ (see Theorem 3.11). We begin our investigation of the generation properties of subgroups of G by starting at the top of the subgroup lattice with the maximal subgroups. The minimal generation of these subgroups is systematically studied in [14] and the main result is the following theorem (see [14, Theorem 2]), which reveals that every maximal subgroup of G can also be generated by very few elements.

Theorem 4.3 *Let G be an almost simple group with socle T and let H be a maximal subgroup of G. Then $d(H \cap T) \leqslant 4$ and $d(H) \leqslant 6$. In particular, every maximal subgroup of a finite simple group is 4-generated.*

It is not too difficult to show that the bound $d(H \cap T) \leqslant 4$ is best possible in the sense that there are infinitely many examples for which equality holds (see Examples 4.4 and 4.8). However, it is possible that the bound $d(H) \leqslant 6$ can be improved. For instance, if T is an alternating group then the proof of Theorem 4.3 already gives $d(H) \leqslant 4$ (see Proposition 4.7 below) and similarly $d(H) \leqslant 3$ if T is a sporadic group. We can construct examples with $d(H) = 5$ when T is a classical group (the author thanks Dr. Gareth Tracey for drawing his attention to the following example).

Example 4.4 Suppose $G = \langle T, x\rangle = T.2$, where $T = \mathrm{P}\Omega_n^+(q)$, $q = q_0^2$ is odd and x is an involutory field automorphism of T. In addition assume $n = a^2$, where $a \geqslant 6$ and $a \equiv 2 \pmod 4$. Then G has a maximal subgroup H of type $O_a^+(q) \wr S_2$ (in the terminology of [37], this is a tensor product subgroup in Aschbacher's $\mathcal{C}_7$ collection) with precise structure

$$H = (\mathrm{P}\Omega_a^+(q) \times \mathrm{P}\Omega_a^+(q)).(Z_2)^5.$$

Clearly, $d(H) \geqslant 5$ and one can check that equality holds. Note that $d(H \cap T) = 4$ in this case, which demonstrates the sharpness of the first bound in Theorem 4.3.

However, it is not known if there are any examples with $d(H) > 5$ when T is a simple group of Lie type.

Conjecture 4.5 *Every maximal subgroup of an almost simple group is* 5*-generated.*

Not surprisingly, subgroup structure theorems for almost simple groups play an essential role in the proof of Theorem 4.3. As previously noted, the 2-generation of finite simple groups is established by inspecting the list of groups provided by the Classification Theorem. The situation for maximal subgroups is not quite as clear-cut because, in general, we cannot consult a complete list of subgroups. However, we do have access to some powerful reduction theorems, such as Aschbacher's theorem [1] for finite classical groups (combined with the detailed structural information in [37] and the comprehensive treatment of the low-dimensional classical groups in [7]) and theorems of Liebeck, Seitz and others for exceptional groups of Lie type (see [42]). These results can be viewed as Lie type analogues of the O'Nan–Scott theorem (see Theorem 4.6), which is the main tool for handling the alternating and symmetric groups. All of these results partition the maximal subgroups of an almost simple group into several families, providing a coherent framework for the proof of Theorem 4.3. It is important to note that for the purposes of this proof, we do not need to worry about any unknown almost simple maximal subgroups because every almost simple group is 3-generated by Theorem 3.11.

Let us sketch a proof of Theorem 4.3 in the case where T is an alternating group. First we recall the O'Nan–Scott theorem, which describes the maximal subgroups of G (see [22, Theorem 4.1A]).

Theorem 4.6 (O'Nan–Scott) *Let $G = A_n$ or S_n, and let H be a maximal subgroup of G. Then one of the following holds:*

(i) *H is intransitive: $H = (S_k \times S_{n-k}) \cap G$, $1 \leqslant k < n/2$;*

(ii) *H is affine: $H = \mathrm{AGL}_d(p) \cap G$, $n = p^d$, p prime, $d \geqslant 1$;*

(iii) *H is imprimitive or wreath-type: $H = (S_k \wr S_t) \cap G$, $n = kt$ or k^t, $k, t \geqslant 2$;*

(iv) *H is diagonal: $H = (A^k.(\mathrm{Out}(A) \times S_k)) \cap G$, A non-abelian simple, $n = |A|^{k-1}$;*

(v) *H is almost simple.*

Proposition 4.7 *Let G be an almost simple group with socle A_n and let H be a maximal subgroup of G. Then $d(H) \leqslant 4$.*

Proof The result can be checked directly if $n = 6$, so we may assume $G = A_n$ or S_n. First we claim that $d(H) \leqslant 3$ in cases (i), (ii), (iii) and (v) of Theorem 4.6. If H is almost simple, then $d(H) \leqslant 3$ by Theorem 3.11. Since $[G : A_n] \leqslant 2$, it suffices to show that $d(L) = 2$ for $L = S_k \times S_{n-k}$, $\mathrm{AGL}_d(p)$ or $S_k \wr S_t$.

(i) For $L = S_k \times S_{n-k}$, it is easy to see that $L = \langle ((1,2), x), (y, (1,2)) \rangle$, where $x = (\alpha, \alpha + 1, \ldots, n-k)$ and $y = (\beta, \beta + 1, \ldots, k)$, with $\alpha = 1$ if $n - k$ is odd, otherwise $\alpha = 2$, and similarly $\beta = 1$ if k is odd, otherwise $\beta = 2$.

(ii) If $L = \mathrm{AGL}_d(p)$ then L has a unique minimal normal subgroup of order p^d and thus the main theorem of [51] implies that $d(L) = \max\{2, d(\mathrm{GL}_d(p))\} = 2$.

(iii) Suppose $L = S_k \wr S_t$ and let $(x_1, \ldots, x_t; y)$ denote a general element of L, where $x_i \in S_k$ and $y \in S_t$. Set $\alpha = 1$ if k is odd, otherwise $\alpha = 2$. If $t = 2$ then $L = \langle x, y \rangle$, where $x = ((1,2), (\alpha, \ldots, k); 1)$ and $y = (1, 1; (1,2))$. Similarly, if $t \geqslant 4$ is even then it is easy to check that $L = \langle x, y \rangle$ where

$$x = ((1,2), 1, \ldots, 1; (2, \ldots, t)),\ y = (1, 1, (\alpha, \ldots, k), 1, \ldots, 1; (1,2)).$$

Similar generators can be given when t is odd.

To complete the proof, we may assume H is a diagonal-type subgroup as in part (iv) of Theorem 4.6. Let Ω be the set of cosets of $\{(a, \ldots, a) : a \in A\}$ in A^k and observe that the embedding of H in G arises from the action of H on Ω.

If $H = A^k.(\mathrm{Out}(A) \times S_k)$ then A^k is the unique minimal normal subgroup of H, so [51] yields $d(H) = \max\{2, d(\mathrm{Out}(A) \times S_k)\}$. The structure of the soluble group $\mathrm{Out}(A)$ is well understood and it is easy to show that $d(\mathrm{Out}(A) \times S_k) \leqslant 4$.

Finally, suppose $G = A_n$ and $[A^k.(\mathrm{Out}(A) \times S_k) : H] = 2$. First assume $k \geqslant 3$. One checks that $(1,2) \in S_k$ induces an even permutation on Ω, so $H = A^k.(J \times S_k)$ with $[\mathrm{Out}(A) : J] = 2$ and we deduce that $d(H) = \max\{2, d(J \times S_k)\} \leqslant 4$. Now assume $k = 2$. Here we calculate that $(1,2) \in S_2$ has precisely $\ell = \frac{1}{2}(|A| - i_2(A) - 1)$ 2-cycles on Ω, where $i_2(A)$ is the number of involutions in A. Now, if ℓ is odd then $H = T^2.\mathrm{Out}(T)$ and thus $d(H) \leqslant d(\mathrm{Aut}(T)) + 1 \leqslant 4$. On the other hand, if ℓ is even then $H = T^2.(J \times S_2)$ with $[\mathrm{Out}(T) : J] = 2$ and as before we conclude that $d(H) = \max\{2, d(J \times S_2)\} \leqslant 4$. □

Example 4.8 We can construct maximal diagonal-type subgroups of alternating groups that need 4 generators, which gives another demonstration of the sharpness of the bound $d(H \cap T) \leqslant 4$ in Theorem 4.3. For example, suppose $A = \mathrm{P}\Omega^+_{12}(p^{2f})$ and $k = 2$ for some prime $p \geqslant 3$ and positive integer f. Then one can show that $H = A^2.(\mathrm{Out}(A) \times S_2)$ is a maximal subgroup of $G = A_n$ (with $n = |A|$) and

$$d(H) = \max\{2, d(\mathrm{Out}(A) \times S_2)\} = d(D_8 \times Z_{2f} \times Z_2) = 4.$$

4.2 Random generation

In the previous section we considered the minimal generation of maximal subgroups of simple (and almost simple) groups, with the aim of extending Theorem 2.1. In a similar spirit, we now turn to the random generation of these subgroups.

Let us recall that the main result on the random generation of simple groups is the verification of Dixon's conjecture (see Conjecture 2.2) and it is natural to ask if an appropriate analogue holds for maximal subgroups of simple groups. It is immediately clear that some modifications are required. Indeed, arbitrarily large maximal subgroups H can have subgroups of bounded index, which prevents $\mathbb{P}_k(H)$ from tending to 1 as $|H| \to \infty$, for any fixed k. For example, $H = S_{n-2}$ is a maximal subgroup of A_n and we have $\mathbb{P}_k(H) \leqslant 1 - 2^{-k}$ since a randomly chosen element of H lies in A_{n-2} with probability $1/2$.

The following result (see [14, Corollary 4]) can be viewed as a best possible analogue of Dixon's conjecture for maximal subgroups of almost simple groups.

Theorem 4.9 *For any given $\epsilon > 0$ there exists an absolute constant $k = k(\epsilon)$ such that $\mathbb{P}_k(H) > 1 - \epsilon$ for any maximal subgroup H of an almost simple group.*

To describe the main steps in the proof, we need some additional notation. Let G be a finite group and set

$$\nu(G) = \min\{k \in \mathbb{N} : \mathbb{P}_k(G) \geqslant 1/e\}.$$

Up to a small multiplicative constant, it is known that $\nu(G)$ is the expected number of random elements generating G (see [62] and [50, Proposition 1.1]). If A is a non-abelian chief factor of G, let $\mathrm{rk}_A(G)$ be the maximal number r such that a normal section of G is the direct product of r chief factors of G isomorphic to A, and let $\ell(A)$ be the minimal degree of a faithful transitive permutation representation of A. Set

$$\delta(G) = \max_A \left\{ \frac{\log \mathrm{rk}_A(G)}{\log \ell(A)} \right\}, \tag{6}$$

where A runs through the non-abelian chief factors of G.

We can now state a remarkable theorem of Jaikin-Zapirain and Pyber [33, Theorem 1.1], which is the key ingredient in the proof of Theorem 4.9.

Theorem 4.10 *There exist absolute constants $\alpha, \beta \in \mathbb{N}$ such that*

$$\alpha(d(G) + \delta(G)) < \nu(G) < \beta d(G) + \delta(G)$$

for any finite group G.

Let H be a maximal subgroup of an almost simple group, so $d(H) \leqslant 6$ by Theorem 4.3. By considering the structure of H (with the aid of the aforementioned subgroup structure theorems), it is not too difficult to show that H has at most three non-abelian chief factors (see [14, Lemma 8.2]) and thus $\delta(H) < 1$. Therefore, Theorem 4.10 implies that $\nu(H) < 6\beta + 1$.

To complete the proof of Theorem 4.9, set $c = 6\beta + 1$ and fix $\epsilon > 0$. Let m be the smallest positive integer such that $(1 - 1/e)^m < \epsilon$ and set $k = cm$. Then

$$1 - \mathbb{P}_k(H) \leqslant (1 - \mathbb{P}_c(H))^m \leqslant (1 - 1/e)^m < \epsilon$$

and thus $\mathbb{P}_k(H) > 1 - \epsilon$ as required.

4.3 Subgroup growth

Let G be a finite group. We define the *depth* of a subgroup H of G to be the maximal length of a chain of subgroups from H to G (with proper inclusions). In particular, H is maximal if and only if it has depth 1. We say that a subgroup of depth 2 is a *second maximal* subgroup of G, and so on. It will be convenient to introduce the following notation:

$$\mathcal{M}_k(G) = \{H : H \leqslant G \text{ has depth } k\}$$
$$m_{k,n}(G) = |\{H \in \mathcal{M}_k(G) : [G : H] = n\}|$$

For example, $m_{1,n}(G)$ is the number of maximal subgroup of G with index n.

For a fixed value of k, it is interesting to consider the growth of $m_{k,n}(G)$ as a function of n. For example, if $\mathcal{G}$ is an infinite family of finite groups (of unbounded order) then we can ask if there is an absolute constant c such that $m_{1,n}(G) < n^c$ for all n and all $G \in \mathcal{G}$. If this condition holds, then we say that the groups in $\mathcal{G}$ have *polynomial maximal subgroup growth*. For example, if p is a prime and $G = (Z_p)^d$ then $m_{1,p}(G) = (p^d - 1)/(p - 1) \sim p^{d-1}$, so elementary abelian p-groups do not have this property.

This growth condition arises naturally in the study of profinite groups. Recall that a profinite group G is *positively finitely generated* (PFG) if $\mathbb{P}_k(G) > 0$ for some positive integer k, where $\mathbb{P}_k(G)$ is defined in terms of topological generation if G is infinite. By a celebrated theorem of Mann and Shalev [54], G is PFG if and only if it has polynomial maximal subgroup growth.

The next result is a combination of [14, Corollaries 5 and 6].

Theorem 4.11 *Almost simple groups have polynomial maximal and second maximal subgroup growth. That is, there exists an absolute constant c such that*

$$\max\{m_{1,n}(G), m_{2,n}(G)\} < n^c$$

for all almost simple groups G and all n.

To prove this, we need the following result, which combines Theorem 4.10 with a result of Lubotzky (see [50, Proposition 1.2]).

Theorem 4.12 *There exists an absolute constant $\gamma \in \mathbb{N}$ such that*

$$m_{1,n}(G) < n^{\gamma d(G)+\delta(G)}$$

for all finite groups G and all $n \in \mathbb{N}$.

Let G be an almost simple group. Then $d(G) \leqslant 3$ by Theorem 3.11 and it is easy to see that $\delta(G) = 0$ (see (6)), so Theorem 4.12 yields

$$m_{1,n}(G) < n^{3\gamma}.$$

As previously noted, $\delta(H) < 1$ for all $H \in \mathcal{M}_1(G)$, so

$$\begin{aligned} m_{2,n}(G) &\leqslant \sum_{a|n} m_{1,a}(G) \max\{m_{1,n/a}(H) \,:\, H \in \mathcal{M}_1(G),\, [G:H] = a\} \\ &< \sum_{a|n} a^{3\gamma}(n/a)^{6\gamma+1} < n^{6\gamma+2} \end{aligned}$$

and thus the bound in Theorem 4.11 holds with $c = 6\gamma + 2$.

The constant γ here can be expressed in terms of the undetermined constant β in Theorem 4.10. It would be desirable to have an effective result with an explicit constant, but it seems rather difficult to extract constants from the proof of Theorem 4.10 in [33].

4.4 Primitive permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with point stabiliser $H = G_\alpha$. Let us consider the relationship between $d(G)$ and $d(H)$. By primitivity, H is a maximal subgroup of G and thus $d(H) \geqslant d(G) - 1$. On the other hand, Lemma 4.1 yields

$$d(H) \leqslant [G : H](d(G) - 1) + 1 \tag{7}$$

and we have observed that equality is possible, even when H is a maximal subgroup of G (see Example 4.2). Of course, if G and H are the groups in Example 4.2 then G does not act faithfully on the cosets of H (indeed, H is a normal subgroup of G), so this example does not come from a primitive group. Therefore, we may ask if it is possible to improve the bound in (7) if we assume H is a *core-free* maximal subgroup. The following result is [14, Theorem 7].

Theorem 4.13 *Let G be a finite primitive permutation group with point stabiliser H. Then*

$$d(G) - 1 \leqslant d(H) \leqslant d(G) + 4.$$

The short proof combines Theorem 4.3 and the O'Nan–Scott theorem (for primitive groups), which describes the structure and action of a primitive permutation group in terms of its socle. Some cases are very easy. For example, if G is an affine group or a twisted wreath product, then G has a regular normal subgroup N, hence $G = HN$, $H \cap N = 1$ and $d(H) = d(G/N) \leqslant d(G)$. If G is almost simple, then $d(H) \leqslant 6$ by Theorem 4.3, so $d(H) \leqslant d(G) + 4$. We refer the reader to [14, Section 10] for the remaining diagonal and product-type cases.

It would be interesting to know if there are any examples in Theorem 4.13 with $d(H) = d(G) + 4$. Note that one would need to prove Conjecture 4.5 in order to rule out any almost simple examples. We refer the reader to [16] for a recent application of Theorem 4.13 to the study of the exchange relation for generating sets of arbitrary finite groups.

4.5 Second maximal subgroups and beyond

Let G be a finite group and recall that $M \leqslant G$ is a *second maximal* subgroup of G if it has depth 2, that is, if M is maximal in a maximal subgroup of G. These subgroups and their overgroups arise naturally in the study of subgroup lattice theory (see Pálfy [63] and Aschbacher [2], for example).

In this final section, our goal is to extend some of the results discussed in the previous section on maximal subgroups of almost simple groups to second maximal subgroups. For example, we have seen that almost simple groups and their maximal subgroups are 3-generated and 6-generated, respectively, so it is natural to ask whether or not this behaviour extends deeper into the subgroup lattice. This question, plus several related problems, is studied in [15] and we will provide a brief overview of the main results.

First let us fix some notation. Let G be an almost simple group and let M be a second maximal subgroup of G, so

$$M < H < G$$

for some maximal subgroup H of G. The following lemma provides an important reduction.

Lemma 4.14 *If either H or M is almost simple, or if $\mathrm{core}_H(M) = 1$, then $d(M) \leqslant 10$.*

Proof If either H or M is almost simple, then $d(M) \leqslant 6$ by Theorems 3.11 and 4.3. If $\mathrm{core}_H(M) = 1$ then H is a primitive permutation group on the set of cosets M in H, so

$$d(M) \leqslant d(H) + 4 \leqslant 10$$

by combining Theorems 4.3 and 4.13. □

If our goal is to investigate the existence of an upper bound of the form $d(M) \leqslant c$ for some absolute constant c, then by the previous lemma we may assume that M contains a non-trivial normal subgroup of H. When viewed in terms of the usual subgroup structure theorems for almost simple groups, this condition on M is rather restrictive. Let us illustrate this with a concrete example.

Example 4.15 Suppose $M < H < G$, where $G = S_n$ and $H = S_k \wr S_t = N.S_t$ with $N = (S_k)^t$ and $k \geqslant 5$ (so $n = kt$ or k^t). Note that $A = (A_k)^t$ is the unique minimal normal subgroup of H. In particular, if $A \not\leqslant M$ then $\mathrm{core}_H(M) = 1$ and thus $d(M) \leqslant 10$ by Lemma 4.14, so let us assume $A \leqslant M$. There are two cases to consider.

(i) $N \leqslant M$: Here the maximality of M in H implies that $M = N.J$ for some maximal subgroup $J < S_t$. Now J has $\ell \leqslant 2$ orbits on $\{1, \ldots, t\}$ (indeed, if J is intransitive, then $J = S_a \times S_{t-a}$ for some a) and Proposition 4.7 implies that $d(J) \leqslant 4$. Therefore,

$$d(M) \leqslant d((S_k)^\ell) + d(J) \leqslant 6.$$

(ii) $N \not\leqslant M$: In this situation, $M = (M \cap N).S_t$ and thus M/A is a maximal subgroup of the wreath product $H/A = S_2 \wr S_t$. One can show that every maximal subgroup of $S_2 \wr S_t$ is 6-generated (see [15, Lemma 2.7]) and thus

$$d(M) \leqslant d(A_k) + 6 = 8.$$

We conclude that $d(M) \leqslant 10$.

The main result on the minimal generation of second maximal subgroups is the following (see [15, Theorem 1]).

Theorem 4.16 *There is an absolute constant c such that $d(M) \leqslant c$ for all second maximal subgroups M of almost simple groups G with*

$$\mathrm{soc}(G) \notin \{\mathrm{L}_2(q), {}^2B_2(q), {}^2G_2(q)\}. \tag{8}$$

Remark 4.17 As noted in [15], we can take $c = 12$ for the constant in Theorem 4.16, unless $\mathrm{soc}(G)$ is a simple exceptional group of Lie type and M is maximal in a parabolic subgroup of G, in which case the conclusion holds with $c = 70$. No doubt these estimates for c could be improved. For example, suppose $G = E_8(q)$ and M is a maximal subgroup of a D_7-parabolic subgroup $H = QL$ of G, where Q is the unipotent radical and L is a Levi factor of H. If M contains Q, then $M = QK_0Z$ where K_0 is a maximal subgroup of $\mathrm{Spin}^+_{14}(q)$, Z is a central torus of rank 1 and Q/Q' is a 64-dimensional spin module for $\mathrm{Spin}^+_{14}(q)$. Since Q' is contained in the Frattini subgroup of Q, Theorem 4.3 implies that

$$d(M) \leqslant d(Q/Q') + d(K_0Z) \leqslant 64 + 6 = 70.$$

To improve this estimate, one would have to study the action of each maximal subgroup of $\mathrm{Spin}^+_{14}(q)$ on the spin module Q/Q' (a complete list of the relevant maximal subgroups is not available in the literature).

Let us look more closely at the groups G excluded in (8). First observe that in each case, G has a maximal Borel subgroup B. If M is a second maximal subgroup and $M \not\leqslant B$, then [15, Theorem 1] states that $d(M) \leqslant c$, where c is the constant in the main statement of Theorem 4.16. However, it is not too difficult to see that certain maximal subgroups of B have radically different generation properties.

Example 4.18 Suppose $G = \mathrm{L}_2(q)$ with $q = p^f$, so $B = (Z_p)^f{:}Z_{q-1}$. If $q - 1$ is a prime, then $M = (Z_p)^f$ is a second maximal subgroup of G with $d(M) = f$. In particular, if we take $q-1$ to be the largest known Mersenne prime, so $q = 2^{74207281}$ at the time of writing, then $M = (Z_2)^{74207281}$ is a second maximal subgroup of $\mathrm{L}_2(q)$ with $d(M) = 74207281$.

This example shows that if there are infinitely many Mersenne primes, which is widely believed to be true, then there is no absolute bound on the number of generators for second maximal subgroups of the groups excluded in (8). In fact, the following result shows that this question is equivalent to a formidable open problem in Number Theory (although this is weaker than the existence of infinitely many Mersenne primes, a proof is still far out of reach).

Theorem 4.19 *There is an absolute constant c such that all second maximal subgroups of almost simple groups are c-generated if and only if*

$$\{r : r \text{ prime and } (q^r - 1)/(q - 1) \text{ is prime for some prime power } q\}$$

is finite.

To finish, let us say a few words on subgroups that lie deeper in the subgroup lattice of an almost simple group G. Firstly, by essentially repeating the argument in the proof of Theorem 4.11, it is easy to show that

$$m_{3,n}(G) < n^{70\gamma+2}$$

for all n (where γ is the constant in Theorem 4.12), assuming the condition on $\mathrm{soc}(G)$ in (8) is satisfied. In fact, by carefully studying the excluded groups in (8), it is possible to show that *all* almost simple groups have polynomial third maximal subgroup growth (see [15, Theorem 6]). Does this growth behaviour extend to fourth maximal subgroups and beyond?

Problem 4.20 For all $k \in \mathbb{N}$, is there a constant $c = c(k) \in \mathbb{N}$ such that $m_{k,n}(G) < n^c$ for all n and all almost simple groups G?

Returning to minimal generation, it is not too difficult to construct third maximal subgroups of almost simple groups that need arbitrarily many generators (without needing to establish any formidably difficult results in Number Theory!).

Example 4.21 Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$. Note that infinitely many primes satisfy this congruence condition, by Dirichlet's theorem. The condition on p implies that S_4 is a maximal subgroup of $\mathrm{PGL}_2(p)$ and this allows us to construct a third maximal subgroup of $S_{2(p+1)}$ via the following chain:

$$S_{2(p+1)} > S_2 \wr S_{p+1} > (S_2)^{p+1}.\mathrm{PGL}_2(p) > (S_2)^{p+1}.S_4 = H.$$

By applying Lemma 4.1 we conclude that $d(H) \geqslant p/24 + 1$.

It would be interesting to seek an appropriate extension of Theorem 4.16 for third maximal subgroups H (and more generally, depth k subgroups) of almost simple groups.

References

[1] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.

[2] M. Aschbacher, *On intervals in subgroup lattices of finite groups*, J. Amer. Math. Soc. **21** (2008), 809–830.

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

[4] G. Binder, *The two-element bases of the symmetric group*, Izv. Vyss. Ucebn. Zaved. Matematika **90** (1970), 9–11.

[5] J.D. Bradley and P.E. Holmes, *Improved bounds for the spread of sporadic groups*, LMS J. Comput. Math. **10** (2007), 132–140.

[6] J.D. Bradley and J. Moori, *On the exact spread of sporadic simple groups*, Comm. Algebra **35** (2007), 2588–2599.

[7] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The Maximal Subgroups of the Low-dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.

[8] J.L. Brenner and J. Wiegold, *Two-generator groups* I, Michigan Math. J. **22** (1975), 53–64.

[9] T. Breuer, *GAP computations concerning Hamiltonian cycles in the generating graphs of finite groups*, preprint, 2012 (arxiv:0911.5589).

[10] T. Breuer, R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups,* II, J. Algebra **320** (2008), 443–494.

[11] T. Breuer, R.M. Guralnick, A. Lucchini, A. Maróti, and G.P. Nagy, *Hamiltonian cycles in the generating graph of finite groups*, Bull. London Math. Soc. **42** (2010), 621–633.

[12] T.C. Burness, *Fixed point ratios in actions of finite classical groups, I*, J. Algebra **309** (2007), 69–79.

[13] T.C. Burness and S. Guest *On the uniform spread of almost simple linear groups*, Nagoya Math. J. **209** (2013), 35–109.

[14] T.C. Burness, M.W. Liebeck and A. Shalev, *Generation and random generation: from simple groups to maximal subgroups*, Adv. Math. **248** (2013), 59–95.

[15] T.C. Burness, M.W. Liebeck and A. Shalev, *Generation of second maximal subgroups and the existence of special primes*, Forum Math. Sigma, to appear.

[16] P.J. Cameron, A. Lucchini and C.M. Roney-Dougal, *Generating sets of finite groups*, Trans. Amer. Math. Soc., to appear.

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

[18] M.D.E. Conder, *An update on Hurwitz groups*, Groups Complex. Cryptol. **2** (2010), 35–49.

[19] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[20] F. Dalla Volta and A. Lucchini, *Generation of almost simple groups*, J. Algebra **178** (1995), 194–223.

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

[22] J.D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Math., vol 163, Springer-Verlag, New York, 1996.

[23] F. Erdem, *On the generating graphs of the symmetric and alternating groups*, PhD thesis, Middle East Technical University, Ankara, 2018.

[24] P. Erdős and P. Turán, *On some problems of a statistical group-theory, II*, Acta. Math. Acad. Sci. Hung. **18** (1967), 151–163.

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

[26] B. Fairbairn, *The exact spread of* M_{23} *is* 8064, Int. J. Group Theory **1** (2012), 1–2.

[27] B. Fairbairn, *New upper bounds on the spreads of the sporadic simple groups*, Comm. Algebra **40** (2012), 1872–1877.

[28] S. Guest, J. Morris, C.E. Praeger and P. Spiga, *On the maximum orders of elements of finite almost simple groups and primitive permutation groups*, Trans. Amer. Math. Soc. **367** (2015), 7665–7694.

[29] R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.

[30] R. Guralnick, T. Pentilla, C.E. Praeger, and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. London Math. Soc. **78** (1999), 167–214.

[31] R.M. Guralnick and A. Shalev, *On the spread of finite simple groups*, Combinatorica **23** (2003), 73–87.

[32] S. Harper, *On the uniform spread of almost simple symplectic and orthogonal groups*, J. Algebra **490** (2017), 330–371.

[33] A. Jaikin-Zapirain and L. Pyber, *Random generation of finite and profinite groups*

and group enumeration, Annals of Math. **173** (2011), 769–814.
[34] S. Jambor, A. Litterick and C. Marion, *On finite simple images of triangle groups*, Israel J. Math., to appear.
[35] W.M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.
[36] C.S.H. King, *Generation of finite simple groups by an involution and an element of prime order*, J. Algebra **478** (2017), 153–173.
[37] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.
[38] M. Larsen, A. Lubotzky and C. Marion, *Deformation theory and finite simple quotients of triangle groups I*, J. Eur. Math. Soc. (JEMS) **16** (2014), 1349–1375.
[39] R. Lawther, M.W. Liebeck and G.M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific J. Math. **205** (2002), 393–464.
[40] M.W. Liebeck, *Probabilistic and asymptotic aspects of finite simple groups*, in Probabilistic group theory, combinatorics, and computing, 1–34, Lecture Notes in Math., 2070, Springer, London, 2013.
[41] M.W. Liebeck and J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of coverings of Riemann surfaces*, Proc. London Math. Soc. **63** (1991), 266–314.
[42] M.W. Liebeck and G.M. Seitz, *A survey of of maximal subgroups of exceptional groups of Lie type*, in Groups, combinatorics & geometry (Durham, 2001), 139–146, World Sci. Publ., River Edge, NJ, 2003.
[43] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.
[44] M.W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky*, J. Algebra **184** (1996), 31–57.
[45] M.W. Liebeck and A. Shalev, *Classical groups, probabilistic methods, and the* $(2,3)$*-generation problem*, Annals of Math. **144** (1996), 77–125.
[46] M.W. Liebeck and A. Shalev, *Random* (r,s)*-generation of finite classical groups*, Bull. London Math. Soc. **34** (2002), 185–188.
[47] 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.
[48] M.W. Liebeck and A. Shalev, *Fuchsian groups, finite simple groups and representation varieties*, Invent. Math. **159** (2005), 317–367.
[49] F. Lübeck and G. Malle, $(2,3)$*-generation of exceptional groups*, J. London Math. Soc. **59** (1999), 109–122.
[50] A. Lubotzky, *The expected number of random elements to generate a finite group*, J. Algebra **257** (2002), 452–459.
[51] A. Lucchini and F. Menegazzo, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Semin. Mat. Univ. Padova **98** (1997), 173–191.
[52] A.M. Macbeath, *Generators of the linear fractional groups*, Proc. Sympos. Pure Math., vol. XII (Amer. Math. Soc., 1969), pp.14–32.
[53] G. Malle, J. Saxl and T. Weigel, *Generation of classical groups*, Geom. Dedicata **49** (1994), 85–116.
[54] A. Mann and A. Shalev, *Simple groups, maximal subgroups, and probabilistic aspects of profinite groups*, Israel J. Math. **96** (1996), 449–468.
[55] C. Marion, *Triangle groups and* $\mathrm{PSL}_2(q)$, J. Group Theory **12** (2009), 689–708.
[56] C. Marion, *On triangle generation of finite groups of Lie type*, J. Group Theory **13** (2010), 619–648.
[57] A. McIver and P. Neumann, *Enumerating finite groups*, Quart. J. Math. Oxford **38**

(1987), 473–488.

[58] N.E. Menezes, M. Quick and C.M. Roney-Dougal, *The probability of generating a finite simple group*, Israel J. Math. **198** (2013), 371–392.

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

[60] L. Morgan and C.M. Roney-Dougal, *A note on the probability of generating alternating or symmetric groups*, Arch. Math. (Basel) **105** (2015), 201–204.

[61] E. Netto, *Substitutionentheorie und ihre Anwendungen auf die Algebra*, Teubner, Leipzig, 1882; English transl. 1892, second edition, Chelsea, New York, 1964.

[62] I. Pak, *On probability of generating a finite group*, preprint, 1999.

[63] P.P. Pálfy, *On Feit's examples of intervals in subgroup lattices*, J. Algebra **116** (1988), 471–479.

[64] M.A. Pellegrini, *The* $(2,3)$*-generation of the special linear groups over finite fields*, Bull. Aust. Math. Soc. **95** (2017), 48–53.

[65] M.A. Pellegrini and M.C. Tamburini, *Finite simple groups of low rank: Hurwitz generation and* $(2,3)$*-generation*, Int. J. Group Theory **4** (2015), 13–19.

[66] S. Piccard, *Sur les bases du groupe symétrique et du groupe alternant*, Math. Ann. **116** (1939), 752–767.

[67] L.L. Scott, *Matrices and cohomology*, Annals of Math. **105** (1977), 473–492.

[68] A. Shalev, *Probabilistic group theory and Fuchsian groups*, in Infinite groups: geometric, combinatorial and dynamical aspects, 363–388, Progr. Math., 248, Birkhäuser, Basel, 2005.

[69] A. Stein, $1\frac{1}{2}$*-generation of finite simple groups*, Beiträge Algebra Geom. **39** (1998), 349–358.

[70] R. Steinberg, *Generators for simple groups*, Canad. J. Math. **14** (1962), 277–283.

[71] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105–145.

[72] T.S. Weigel, *Generation of exceptional groups of Lie-type*, Geom. Dedicata **41** (1992), 63–87.

[73] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York (1964).

[74] A.J. Woldar, *On Hurwitz generation and genus actions of sporadic groups*, Illinois Math. J. **33** (1989), 416–437.

[75] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.