1

Maximal subgroups of finite simple groups: classifications and applications

Colva M. Roney-Dougal

Abstract

This paper surveys what is currently known about the maximal subgroups of the finite simple groups. After briefly introducing the groups themselves, if their maximal subgroups are completely determined then we present this classification. For the remaining finite simple groups our current knowledge is only partial: we describe the state of play, as well as giving some results that apply more generally. We also direct the reader towards computational resources for the construction of maximal subgroups.

After this, we present three sample applications, selected because they combine group theoretical and combinatorial arguments, and because they use either or both of the detailed classifications and the looser statements that can be made about all maximal subgroups. In particular, we discuss results relating to generation, and the generating graph; results concerning bases; and some applications to computational complexity, in particular to graph colouring and other problems with no known polynomial-time solution.

1.1 Introduction

The Classification of Finite Simple Groups was perhaps the most impressive achievement in 20th century mathematics. A simple statement is as follows.

Theorem 1.1 (Classification of Finite Simple Groups) *Let G be a finite simple group. Then G is one of the following:*

(a) *A cyclic group, of prime order.*
(b) *An alternating group* A_n*, of degree* $n \geq 5$*.*
(c) *A group of Lie type, either classical or exceptional.*
(d) *One of 26 sporadic groups.*

After naming the simple groups, two natural questions arise.

1. What is the subgroup structure of these groups?
2. How are these groups represented, by means of permutations or matrices? Phrased differently, what objects have these groups as groups of automorphisms?

These two questions are intimately linked, since any transitive permutation action of a group G is equivalent to the action of G on the set of right cosets of a point stabiliser in G.

A useful first step towards understanding all of the subgroups of a group is to determine its *maximal* subgroups. This paper will describe both what is known about the maximal subgroups of the finite simple groups, and give three examples of areas towards the intersection of group theory and combinatorics where this information has been put to fascinating use.

One might hope that information about the maximal subgroups of the finite simple groups would be sufficient to determine the maximal subgroups of any finite group, but thus turns out not to be the case. However, it is *almost* the case. Each group G acts on itself by conjugation, and this yields a homomorphism ρ from G to the group $\mathrm{Aut}(G)$ of automorphisms of G, where each $g \in G$ is mapped to the automorphism $x \mapsto g^{-1}xg$. The image of ρ is the group $\mathrm{Inn}(G)$ of *inner automorphisms* of G, which can easily be shown to be a normal subgroup of $\mathrm{Aut}(G)$. The kernel of ρ is the centre $Z(G)$ of G, so the first isomorphism theorem shows that $\mathrm{Inn}(G)$ is isomorphic to $G/Z(G)$. It follows that if T is a nonabelian simple group then $T \cong \mathrm{Inn}(T) \trianglelefteq \mathrm{Aut}(T)$, and it is easy to check that T is the unique minimal normal subgroup of $\mathrm{Aut}(T)$.

Definition 1.2 A group G such that $T \trianglelefteq G \leq \mathrm{Aut}(T)$, for some nonabelian simple group T, is an *almost simple group*. The group T is the socle of G, denoted $\mathrm{Soc}(G)$.

If G is almost simple with socle T, and M is a maximal subgroup of G, then $M \cap T \trianglelefteq M$, and so M is a subgroup of $\mathrm{N}_G(M \cap T)$, the normaliser of $M \cap T$ in G. In most cases, $M \cap T$ is a proper subgroup of T, and so is not normal in G, which implies that M is equal to $\mathrm{N}_G(M \cap T)$

(since M is maximal). Often, $M \cap T$ is maximal in T, so many of the maximal subgroups of G are of the form $\mathrm{N}_G(H)$, where H is a maximal subgroup of T. Given such a maximal subgroup H of T, it is relatively straightforward to determine whether $\mathrm{N}_G(H)$ is maximal in G.

However, it is also possible that $M \cap T$ is not maximal in T. For an example of this behaviour, consider the normaliser M of a 7-cycle in the symmetric group S_7, which is a semidirect product $7 \rtimes 6$ of a cyclic group of order 7 by a cyclic group of order 6. It is not too hard to check that M is a maximal subgroup of S_7. However, $M \cap \mathrm{A}_7$ is *not* maximal in A_7, being contained in the representation of $\mathrm{PSL}_3(2)$ as a group of automorphisms of the Fano plane, $\mathrm{PG}_2(2)$.

It turns out that this is the only complication: work of Kovács (57), and of Aschbacher and Scott (4) reduces the problem of finding the maximal subgroups of an arbitrary group to knowing the maximal subgroups of the almost simple extensions of its composition factors, together with solving some cohomological problems, which can be done computationally (25; 34). Thus we shall now describe the maximal subgroups of the almost simple groups.

1.2 The maximal subgroups

The maximal subgroups of the cyclic groups of prime order are trivial. We therefore start this section by describing the maximal subgroups of the alternating groups, then the classical groups of Lie type, the exceptional groups of Lie type, and finally the sporadic groups.

1.2.1 Alternating groups

In this section we discuss the classification of the maximal subgroups of the alternating groups A_n and the symmetric groups S_n, for $n \geq 5$. If $n \neq 6$ then $\mathrm{Aut}(\mathrm{A}_n) = \mathrm{S}_n$, whilst the isomorphism $\mathrm{A}_6 \cong \mathrm{PSL}_2(9)$ means that some additional automorphisms arise naturally: see Subsection 1.2.2.

The first family of maximal subgroups is easy, both to describe and to classify. A permutation group $G \leq \mathrm{S}_n$ is *transitive* if for all $\alpha, \beta \in \{1, \ldots, n\}$ there exists $g \in G$ such that $\alpha^g = \beta$, and *intransitive* otherwise. For $1 \leq k \leq n$, the group A_n is transitive on the k-subsets of $\{1, \ldots, n\}$. Furthermore, stabilising a k-subset is equivalent to stabilising its complement, an $(n-k)$-subset. Hence, for each k in $\{1, \ldots, \lfloor n/2 \rfloor\}$, and for $X \in \{\mathrm{A}_n, \mathrm{S}_n\}$, we find a unique conjugacy class of subgroups of

type $(\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap X$. It is a relatively easy exercise to show that these subgroups are maximal if and only if $k \neq n-k$. Thus, it remains to classify the transitive maximal subgroups of A_n and S_n.

The next family of maximal subgroups is almost as easy. A subset Δ of $\{1, \ldots, n\}$ is a *block* for a permutation group $G \leq \mathrm{S}_n$ if for all $g \in G$ either $\Delta^g \cap \Delta = \emptyset$, or $\Delta^g = \Delta$. That is, each element of G either permutes the elements of Δ amongst themselves, or maps all of them outside Δ. If G is a transitive subgroup of S_n, and there exists a block for G of size greater than one and less than n, then G is *imprimitive*; all other transitive groups are *primitive*.

If Δ is a block for G, then it is easy to check that each translate Δ^g is also a block, so $\ell := |\Delta|$ is a divisor of n. It is not too hard to show that S_n is transitive on all partitions of $\{1, \ldots, n\}$ into parts of size ℓ, so for each proper nontrivial divisor ℓ of n the stabilisers in S_n of such partitions form a single conjugacy class of imprimitive subgroups. One may also with not too much effort show that these imprimitive groups are always maximal in S_n. The group A_n also has a unique conjugacy class of such stabilisers for each value of ℓ, and it turns out that there is a unique non-maximal example, namely the imprimitive groups stabilising four blocks of size two in A_8.

Thus, the main work is to classify the primitive maximal subgroups of A_n and S_n. The first step is the further case distinction given by the O'Nan–Scott Theorem. There are many different versions of this theorem, some giving much more detail than others, but since we are only interested in *maximal* subgroups the following will suffice.

Theorem 1.3 *Let G be a primitive maximal subgroup of $X = \mathrm{S}_n$ or $X = \mathrm{A}_n$, with $n \geq 5$. Then G is one of the following.*

(a) $G = \mathrm{AGL}_k(p) \cap X$, *with $n = p^k$ and p prime: the* affine *case.*
(b) $G = (T^k.(\mathrm{Out}(T) \times \mathrm{S}_k)) \cap X$, *with T a nonabelian simple group, $k \geq 2$ and $n = |T|^{k-1}$: the* diagonal *case.*
(c) $G = (\mathrm{S}_m \wr \mathrm{S}_k) \cap X$, *with $n = m^k$, $m \geq 5$ and $k \geq 2$: the* product action *case.*
(d) $T \trianglelefteq G \leq \mathrm{Aut}(T)$, *with T a nonabelian simple group: the* almost simple *case.*

We shall not give details of the structure of the groups in each of these cases, see textbooks such as (20), (32) or (97) for much more information.

Two questions then arise. Firstly, which of the groups listed above are, in fact, maximal? Secondly, whilst it is clear for which n the groups

of affine, diagonal and product action type arise, the description of the almost simple case gives no indication as to the value of n: what *are* the almost simple primitive groups?

The first of these questions is completely answered by Liebeck, Praeger and Saxl in (61). They show that the group $G = \mathrm{AGL}_k(p)$ is maximal in S_{p^k} whenever G contains an odd permutation (namely, when p is odd), and that $G \cap \mathrm{A}_{p^k}$ is maximal except when $p^k \in \{7, 11, 17, 23\}$. (As an aside, we note that if $n \leq 4$ then $n = p^k$ for a prime p, and S_n is *equal* to the group $\mathrm{AGL}_k(p)$). Furthermore, the groups of diagonal and product action type are maximal whenever they occur. Thus the most detailed work in (61) is to consider the almost simple case, and here the result consists of several pages of tables listing containments of almost simple primitive groups.

Despite the monumental achievement of (61), this still leaves our second question: which almost simple groups actually occur? To answer this, one uses the straightforward result that a transitive permutation group G is primitive if and only if the point stabiliser G_α is maximal in G. Thus, to classify the almost simple primitive groups, we need to classify the maximal subgroups of the almost simple groups! Fortunately, the problem is less circular than it seems, as if G is a maximal subgroup of S_n then certainly $|G| < n!$, so we can bootstrap our solutions.

The classification of the primitive permutation groups of low degree is one of the oldest problems in group theory. We shall only briefly summarise the parts of the history that are most relevant to our current question, namely determining the almost simple maximal subgroups of A_n and S_n: see Short's book (89) for a considerably more detailed exposition. We should also mention that determining the full list of groups of affine type when $n = p^k$ is a very different type of problem to that of determining the other types of maximal subgroup, as this is where by far the greatest number of examples arise.

The earliest significant progress was made by Jordan, who in 1871 counted the primitive permutation groups of degree n for $n \leq 17$, and stated that a transitive group of degree 19 is A_{19}, S_{19}, or a group of affine type (47). By 1912, the classification up to degree 20 had been completed by Martin (79) and Bennet (8). After a long pause, the birth of practical symbolic computation in the 1960s gave rise to new approaches, and by 1970 Sims in (90) had redetermined the primitive groups of degree up to 20. Sims also classified the primitive groups of degree up to 50: this list was never published, but was widely circulated in manuscript

form, and the resulting groups formed one of the earliest databases in computational group theory, eventually becoming part of GAP (36) and MAGMA (11).

The next dramatic leap forward came as a result of the announcement of the Classification of Finite Simple Groups (CFSG), after which Dixon and Mortimer used the O'Nan–Scott Theorem to classify the primitive groups with insoluble socles of degree less than 1000 (31) (these are the non-affine groups). For these degrees, MAGMA can compute the maximal subgroups of A_n and S_n, using the database of primitive groups and the results in (61).

More recently, the author classified all primitive groups of degree up to 2500 in (85), and this was extended to degree 4095 by Coutts, Quick and the author in (28). Both of these classifications are available in both MAGMA and GAP, as part of the primitive groups database. Thus, for any given degree $n \leq 4095$, the interested reader can use the database of primitive groups, together with (61), to determine the maximal subgroups of A_n and S_n. In as yet unpublished work, Ben Stratford has extended the classification to degree $2^{13}-1$, and he is working on a classification of the non-affine primitive groups of degree up to one million.

Thus for all degrees which are likely to be encountered by the average user, the groups are available. In the rest of this subsection we shall therefore concentrate on results which hold for *all* n, and on methods which enable one to prove things about all permutation groups without using such tremendously detailed classifications.

We shall summarize the two types of result we shall present for general n as: the primitive subgroups of A_n and S_n, other than A_n and S_n themselves, are *small* and there are *relatively few* of them. These two facts are often sufficient for many applications. There is a further family of beautiful results that we would love to have discussed, which can be summarised as saying that the majority of the elements of S_n belong to few transitive, and even fewer primitive, subgroups of S_n (permutations belonging to no proper primitive subgroup of S_n other than A_n are called *Jordan elements*). A good starting point for the interested reader is (22).

The question of bounding the order of a proper primitive subgroup of A_n or S_n has a lengthy history. Perhaps the oldest result still in regular use is that of Bochert from 1889 (10), which states that if a primitive group G has index greater than 2 in S_n, then this index is at least $\lfloor (n+1)/2 \rfloor !$. This bound was dramatically improved in 1980, when

Praeger and Saxl proved in (82) that if $G \leq \mathrm{S}_n$ is primitive and does not contain A_n, then $|G| \leq 4^n$.

One especially useful theorem in this field, due to its nice mix of concision and strength, is due to Maróti (78). In Case (a), below, notice that $r = 1$ if and only if G is almost simple, so that the almost simple examples are precisely the actions of A_m and S_m on the cosets of intransitive maximal subgroups.

Theorem 1.4 (78) *Let G be a primitive permutation group of degree n. Then one of the following holds.*

(a) *G is an almost simple or product action subgroup of $\mathrm{S}_m \wr \mathrm{S}_r$, where the action of S_m is on k-subsets of $\{1, \ldots, m\}$, so that G has degree $\binom{m}{k}^r$.*
(b) *G is one of the Mathieu groups M_{11}, M_{12}, M_{23} or M_{24}, with their 4-transitive actions.*
(c) $|G| \leq n \cdot \prod_{i=0}^{\lfloor \log n \rfloor - 1}(n - 2^i) < n^{1+\lfloor \log n \rfloor}$.

(In the above theorem statement, and throughout the paper, all logarithms are to the base 2).

A second extremely useful result, which concerns itself only with almost simple primitive groups, and hence gives a tighter bound, is the following, due to Liebeck in 1984.

Theorem 1.5 (58) *Let G be an almost simple primitive subgroup of S_n, and let $T = \mathrm{Soc}(G)$. Then one of the following holds.*

(a) *$T = \mathrm{A}_m$, acting on k-subsets of $\{1, \ldots, m\}$, or on partitions of $\{1, \ldots, m\}$ into subsets of size $\ell > 1$, where ℓ properly divides m.*
(b) *T is a simple classical group acting on an orbit of subspaces of the natural module, or (if $T = \mathrm{PSL}_d(q)$) on pairs of subspaces of complementary dimensions.*
(c) $|G| < n^9$.

A small number of remarks are in order. Firstly, the groups in Case (a) include the almost simple groups in Case (a) of Maróti's theorem, together with the actions on cosets of imprimitive maximal subgroups. The groups in Case (b) will be examined in more detail in the next subsection, and in particular the natural module for a classical group will be defined. Using results that we shall see in Section 1.4, Liebeck observed (see (20, p116)) that one can replace the 9 in Case (c) with a number just slightly greater than 6, with the precise bound coming from the Mathieu group M_{24} in its natural action on 24 points.

We move on to the idea that there are "few" primitive maximal subgroups, and mention just two asympotic results. The first is due to Liebeck, Martin and Shalev.

Theorem 1.6 (60) *The symmetric group* S_n *has* $n^{o(1)}$ *conjugacy classes of primitive maximal subgroups.*

Here $o(1)$ denotes a number that tends to 0 as n tends to infinity. The author has been unable to find a linear or sublinear bound on the number of conjugacy classes of primitive maximal subgroups that features explicit constants; it would be nice to have one.

Finally, Cameron, Neumann and Teague proved that for almost all n the only primitive groups of degree n are S_n and A_n.

Theorem 1.7 (24) *Let* $e(x)$ *denote the number of integers* $n \leq x$ *such that there exists a primitive group of degree* n*, other than* A_n *or* S_n*. Then* $e(x) \sim 2x/\log x$*.*

1.2.2 Classical groups

We shall give a rather superficial introduction to the classical groups, as this article will require few of their properties. See any of (12), (56), (95) or (97) for significantly more detailed information.

A *classical form* on a finite vector space $V = \mathbb{F}^d$ is a nondegenerate form $\beta : V \times V \to \mathbb{F}$ or $Q : V \to F$ of one of the following types.

1. A *unitary form*: β is linear in the first variable, additive in the second, the order of $\mathbb{F}$ is a square, and $\beta(u, v) = \beta(v, u)^\sigma$ for all $\lambda \in \mathbb{F}$ and $u, v \in V$, where σ is the (unique) field automorphism of $\mathbb{F}$ of order two.
2. A *symplectic form*: β is bilinear, $\beta(u, v) = -\beta(v, u)$ for all $u, v \in V$, and $\beta(v, v) = 0$ for all $v \in V$.
3. A *quadratic form*: $Q(\lambda v) = \lambda^2 Q(v)$ for all $\lambda \in \mathbb{F}$ and $v \in V$, and the associated form β defined by $\beta(u, v) = Q(u) + Q(v) - Q(u + v)$ is bilinear.

A form β is *nondegenerate* if $\beta(x, v) = 0$ for all $v \in V$ implies that $x = 0$, whilst a quadratic form is nondegenerate if its associated form β is nondegenerate. To enable us to speak uniformly about all of the families of classical groups, we often also allow the zero map $\beta : V \times V \to \{0\}$ to count as a classical form.

An *isometry* of a classical form β or Q is an element $g \in \mathrm{GL}(V)$ such

that $\beta(ug, vg) = \beta(u, v)$ or $Q(ug) = Q(u)$, for all $u, v \in V$. It is clear that the set of all such isometries forms a subgroup of $\mathrm{GL}(V)$; notice that if the form β is identically zero then this subgroup is $\mathrm{GL}(V)$ itself.

The term *classical group* is rarely used with a precise definition. It includes the groups of all isometries of each classical form (including the zero form), together with various quotients and extensions by automorphisms of these groups: see (12) or (56) for much more discussion of the various chains of subgroups and quotients that arise. The *natural module* for a classical group is the vector space V, equipped with the corresponding form.

It turns out that the groups of isometries of distinct forms on V of the same type are conjugate in $\mathrm{GL}(V)$, and in particular are isomorphic. This enables the definition of the isometry groups $\mathrm{GL}(V)$ of the zero form, $\mathrm{Sp}(V)$ of a symplectic form, $\mathrm{GU}(V)$ of a unitary form and $\mathrm{GO}^{\varepsilon}(V)$, where $\varepsilon = \{+, -, \circ\}$, of a quadratic form. Here $\varepsilon = \circ$ if and only if the dimension is odd, whilst for even dimension the sign of ε depends on the dimension of a maximal subspace on which the form is identically zero. We warn the reader that notation for the orthogonal groups is unfortunately inconsistent in the literature, and we follow (12).

These isometry groups are not in general simple, but their derived group $\mathrm{SL}(V)$, $\mathrm{Sp}(V)$, $\mathrm{SU}(V)$ or $\Omega^{\varepsilon}(V)$ is usually quasisimple, which means in particular that the quotient of their derived group by its centre is usually simple. There are some exceptions to these assertions for small dimensions and fields: see (26, Chapter 2) or (56, Prop 2.9.2) for the full list.

The simple classical groups therefore act faithfully on projective space, equipped with the corresponding classical form. Since the maximal subgroups of a quasisimple group are in natural bijection with the maximal subgroups of its simple quotient, many authors work with the linear groups, rather than the projective quotients.

The outer automorphism groups of the classical groups are all small and soluble, and are generally formed as a semidirect product of up to three groups, most of which are cyclic. See the Atlas (26) for a brief introduction, or (12) or (56) for a more extensive discussion, including how to pick canonical representatives of the automorphisms.

We shall not give an extensive historical survey of the classification of maximal subgroups of classical groups in this article, as there are already several excellent sources for this history. Firstly, we would like to mention Oliver King's 2005 survey (50), which appeared in the same

series of conference proceedings as the present article. Secondly, there is a useful survey (55) by Kleidman and Liebeck from 1988, which also discusses the alternating and exceptional groups.

The key result when analysing the maximal subgroups, or indeed the full subgroup lattice, of the finite classical groups is Aschbacher's Theorem (1). We shall not give a precise statement of this theorem, as it requires too much technical setup, but in spirit it is similar to the O'Nan–Scott Theorem. It divides the set of *all* subgroups of a finite classical group (other than certain 4-dimensional symplectic groups and 8-dimensional orthogonal groups with $\varepsilon = +$) into nine classes, known as *Aschbacher classes*. Eight of these classes, denoted $\mathcal{C}_1$ to $\mathcal{C}_8$, contain the groups stabilising some natural geometry on the space (V, β) or (V, Q), and so these classes are called *geometric*. The ninth class consists of groups which are almost simple, modulo scalars, and is generally denoted $\mathcal{S}$ or $\mathcal{C}_9$.

The maximal subgroups of the almost simple 4-dimensional symplectic groups are described by Aschbacher in (1), and the maximal subgroups of the almost simple 8-dimensional orthogonal groups with $\varepsilon = +$ are fully classified by Kleidman in (52).

For the geometric subgroups, Aschbacher's Theorem yields restrictions on the dimension d, the field $\mathbb{F}$, and the type of classical form for which the groups arise. For Class $\mathcal{S}$ there is no such information. The Aschbacher classes are not pairwise disjoint, and it is not the case that being the maximal member of one of these classes guarantees maximality in the corresponding classical group.

We are therefore left with the same two questions as we asked for the alternating groups, but with Class $\mathcal{S}$ in place of the almost simple primitive groups.

1. When is a maximal member of one of these classes in fact a maximal subgroup?
2. Which groups actually appear in Class $\mathcal{S}$, for a given classical group?

Let us start by concentrating on the dimensions for which the answers to both questions are known. A classification of the maximal subgroups of the simple classical groups in dimension at most 12 was given in the PhD thesis of Peter Kleidman (51), without full proofs. This was a remarkable achievement, and the list was widely circulated and used by a great many authors. Kleidman intended to publish a subsequent book, which would include complete proofs, and also cover the almost

simple groups, but unfortunately this was not published. However, the task was eventually carried out by Bray, Holt and the author in (12).

In dimension at least 13, the geometric maximal subgroups of the almost simple groups are classified by Kleidman and Liebeck in (56), completely answering our first question for these classes. In (56), Kleidman and Liebeck also give detailed descriptions of the conjugacy class stabilisers in the outer automorphism group, and the structure of the maximal subgroup in the simple group (similar information also appears in (12)).

This leaves Class $\mathcal{S}$. For dimensions 13, 14 and 15 the maximal subgroups in Class $\mathcal{S}$ are classified by Schröder in (88). In dimensions 16 and 17 the maximal subgroups of Class $\mathcal{S}$ are studied by Rogers in (84): for non-orthogonal groups, and for orthogonal groups with $\varepsilon = -$, a complete classification is given, but some small questions remain about maximal subgroups of certain non-simple groups in the exceptional orthogonal cases. The results in (88) and (84) are currently being prepared for publication.

The MAGMA function `ClassicalMaximals` takes as input the type of a classical group, a dimension and a field size, and returns a list of conjugacy class representatives of the maximal subgroups, organised by their Aschbacher class. The geometric maximal subgroups are given by the explicit generating matrices constructed in (44) and (45), whilst many of the groups in Class $\mathcal{S}$ are taken from MAGMA's database of finite quasisimple matrix groups, based on work by Steel (91) and by Hiß and Malle (43). Up to dimension 17, the list returned by `ClassicalMaximals` is guaranteed to be complete, whilst beyond that it returns only the geometric maximal subgroups.

In the remainder of this section we shall discuss what is known, and what remains to be proved, in dimension at least 18. Firstly, papers by Hiß and Malle (43) and by Lübeck (66) provide lists containing all quasisimple groups in class $\mathcal{S}$, for dimension up to 250. Thus in principle the work carried out in (12), (88) and (84) could be continued to higher dimensions, although various issues become harder as the dimension increases.

The very most that one could hope for would be a theorem similar to that of (61): a statement that said that a quasisimple group had maximal normaliser in some almost simple classical group *unless* it was contained in some known list of exceptions. Unfortunately, for the groups in Class $\mathcal{S}$, there are considerably more possible obstructions to maximality than

there are for almost simple primitive permutation groups, and whilst progress is being made, there is long way to go. As an example, we would like to mention (41) and (42) for the analysis of when a member of Class $\mathcal{S}$ can be contained in a member of Class $\mathcal{C}_2$. We refer the reader to (76) for a vision of what might be achieved.

In the absence of such a theorem, there are results of a similar flavour to those discussed in Subsection 1.2.1: groups in Class $\mathcal{S}$ are *small* and there are *few of them*. The order of $\mathrm{GL}_d(q)$ is (approximately) q^{d^2}, and the other classical groups have similar orders, so the bound given in the following theorem, due to Liebeck, is dramatically smaller.

Theorem 1.8 (59) *Let G be a finite almost simple classical group of dimension d over $\mathbb{F}_q$. Let H be a maximal subgroup of G that does not contain $\mathrm{Soc}(G)$, and does not lie in one of the geometric Aschbacher classes. Then either H is isomorphic to A_m or S_m, with $m \in \{d+1, d+2\}$, or $|H| \leq q^{3d}$.*

The representations of A_m and S_m in Theorem 1.8 are not at all mysterious. The group S_m can be represented by *permutation matrices* in $\mathrm{GL}_m(q)$: matrices with a unique 1 in each row and column, and all other entries 0, that permute the ordered basis vectors in the same way as the original permutations act on $\{1, \ldots, m\}$. This action stabilises the subspace $U = \langle (1, 1, \ldots, 1) \rangle$, and also stabilises the subspace S of all vectors of weight 0, which is $(m-1)$-dimensional. If $p \nmid m$ then S gives the required action, but notice that if $p \mid m$ then $U \leq S$, so we find an action of S_m on the $(m-2)$-dimensional space S/U.

There are other versions of Theorem 1.8 which yield smaller bounds than q^{3d}, but at the cost of a larger list of exceptions.

We finish this subsection with a result due to Häsä, which shows that there are not so many maximal subgroups in a classical group.

Theorem 1.9 (39) *Let G be a finite almost simple classical group of dimension d over $\mathbb{F}_q$. Let $m(G)$ denote the number of conjugacy classes of maximal subgroups of G not containing $\mathrm{Soc}(G)$. Then $m(G) < 2d^{5.2} + d \log \log q$.*

1.2.3 Exceptional groups

The remaining finite simple groups of Lie type are known as the *exceptional groups*. Similarly to the classical groups, they are often most eas-

ily constructed via groups of matrices over finite fields, although sometimes constructions over objects other than fields, or as finite subgroups of algebraic groups, are more revealing. The classical groups are each parametrised by two integers, a dimension d and a field size q, but the exceptional groups come with a fixed Lie rank, and only the field size can vary. The Lie rank is used rather than the dimension, since the dimension of the smallest linear representation may depend on the characteristic of the field.

The exceptional groups fall into two main types: the *untwisted* groups are defined over every finite field, whilst the *twisted* groups require the field order to be certain powers, and sometimes also for the field to have a specified characteristic.

The smaller rank groups are subgroups of various classical groups in dimension at most 8, and their maximal subgroups are known. These are as follows.

- The *Suzuki groups* ${}^2\mathrm{B}_2(q)$ (also known as $\mathrm{Sz}(q)$) are defined only for q an odd power of 2, and are subgroups of $\mathrm{Sp}_4(q)$. The maximal subgroups of the simple Suzuki groups were determined by Suzuki himself in (94); the almost simple groups are dealt with in (12).
- The groups $\mathrm{G}_2(q)$ are subgroups of $\mathrm{Sp}_6(q)$ when q is even and of $\Omega_7(q)$ otherwise. The maximal subgroups of almost simple groups G with socle $\mathrm{G}_2(q)$ were determined by Kleidman in (54) for q odd, by Cooperstein in (27) for q even and G simple, and by Aschbacher in (2) otherwise.
- The *small Ree groups* ${}^2\mathrm{G}_2(q)$ (also known as $\mathrm{R}(q)$), are defined only for q an odd proper power of 3, and are subgroups of $\mathrm{G}_2(q)$. Their maximal subgroups were determined by Kleidman in (54).
- The groups ${}^3\mathrm{D}_4(q)$ are defined for q a cube, and are subgroups of $\Omega_8^+(q)$. Their maximal subgroups were determined by Kleidman in (53).

All of these maximal subgroups are described in the tables in (12).

The *big Ree groups* ${}^2\mathrm{F}_4(q)$ are defined only for q an odd power of 2. The maximal subgroups of the almost simple groups with socle ${}^2\mathrm{F}_4(q)$ were determined by Malle in (77). These groups are considerably larger than the previous examples, and first occur in dimension 26.

This leaves only four families of groups: $\mathrm{F}_4(q)$, ${}^2\mathrm{E}_6(q)$ with q a square, and $\mathrm{E}_r(q)$ for $r \in \{6, 7, 8\}$. For these groups, full classifications of maximal subgroups are still not published, but in an exciting, very recent

development, David Craven has just announced a complete classification.

The state of play until earlier this year was as follows. Thanks to a great many papers by a great many people, there are detailed descriptions of the types of maximal subgroups that arise: the survey article by Liebeck and Seitz (62) is a good starting point. The only unknown maximal subgroups had similar properties to Aschbacher Class $\mathcal{S}$ for the classical groups: almost simple, and very small. Thanks to Liebeck, Seitz and many others, it is known which simple groups could be the socles of such groups, but there were no useful bounds on the number of conjugacy classes, and little information about what almost simple extensions arise.

1.2.4 Sporadic groups

In contrast to the rest of this section, the problem of classifying the maximal subgroups of the almost simple sporadic groups is evidently a finite one, and the task is almost complete. An excellent survey of the maximal subgroups of the sporadic groups by Wilson (98) has recently appeared, and we direct the reader there for more details.

The Atlas (26) describes the maximal subgroups of the almost simple sporadic groups, with the exception of seven socle types: the three Fischer groups Fi_{22}, Fi_{23} and Fi_{24}, the Janko group J_4, the Thompson group Th, the baby Monster $\mathbb{B}$ and the Monster $\mathbb{M}$.

Wilson's book (97) lists the maximal subgroups of the almost simple sporadic groups, although (98) points out two mistakes: one in the list of maximal subgroups of $\mathbb{B}$, and one in the list of maximal subgroups of Co_1. The lists re-appear, in somewhat more compressed form, in (98).

The only almost simple sporadic group whose maximal subgroups are not fully determined is $\mathbb{M}$. The published results on maximal subgroups of $\mathbb{M}$ include complete classifications, except for the possibility of maximal subgroups with socle $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_2(16)$ and $\mathrm{PSU}_3(4)$. Of these, $\mathrm{PSL}_2(8)$ and $\mathrm{PSL}_2(16)$ were considered in unpublished work of P. E. Holmes, and papers by Wilson on $\mathrm{PSL}_2(8)$ and $\mathrm{PSU}_3(4)$ are in progress. The most recent case to appear was in (99), which proves that no maximal subgroup of the Monster has socle $\mathrm{PSU}_3(8)$.

1.3 Generation and the generating graph

One of the surprising facts about the finite simple groups is that they can all be generated by only two elements. This is an easy exercise for the alternating groups, was proved by Steinberg (92) for the groups of Lie type, and was shown by Aschbacher and Guralnick in (3) for the sporadic groups. We sadly still have no proof that does not depend on the classification.

Furthermore, Dalla Volta and Lucchini showed in (29) that each almost simple group can be generated by at most three elements, and that an almost simple group G requires three generators if and only if $G/\operatorname{Soc}(G)$ requires three generators. Since these quotients are straightforward to describe, the determination of the *minimal size* of generating sets of the almost simple groups is complete.

The *nature* of the generating sets is still somewhat mysterious. For example, the following landmark result by Liebeck and Shalev in 1995 has created a world of related theorems.

Theorem 1.10 (63) *Let G be an almost simple group, and let $P(G)$ denote the probability that two randomly chosen elements of G generate a subgroup containing* $\operatorname{Soc}(G)$*. Then $P(G) \to 1$ as $|G| \to \infty$.*

Whilst the proof is necessarily complex, and builds on pre-classification work by Dixon (30), who proved the theorem for the case $G = \mathrm{A}_n$, and on a paper (48) by Kantor and Lubotzky, which dealt with the case of G a classical group, the basic idea is quite simple. It uses results in a similar vein to those presented in Section 1.2, although the results used were not exactly the ones we have presented, some of which are much more recent! We now briefly explain the idea.

Let G be nonabelian and simple, for ease of description. If two elements of G *fail* to generate G, then they must both lie in some maximal subgroup M of G. The probability of this happening, for a specific subgroup M, is $|G : M|^{-2}$. Since M is a maximal subgroup of the simple group G, it is equal to its own normaliser in G, so by the Orbit-Stabiliser Theorem there are $|G : M|$ conjugates of M in G. Hence the probability that two elements lie in a common conjugate of M can be bounded above by $|G : M|^{-1}$. Summing over all conjugacy classes of maximal subgroups of G gives an upper bound on $1 - P(G)$, and hence a lower bound on $P(G)$.

As described in Section 1.2, the maximal subgroups of the finite simple groups are either known, and so their orders and numbers of conjugacy

classes can be bounded explicitly, or are known to be small, almost simple, and (excluding until recently the exceptional groups) relatively few. With some effort, and not a little inspiration in the case of the exceptional groups, it is possible to use this insight to bound $P(G)$.

Whilst Theorem 1.10 places no lower bound on the probability, this is given by the following, due to Menezes, Quick and the author.

Theorem 1.11 (80) *Let G be a finite simple group. Then*

$$P(G) \geq 53/90,$$

with equality if and only if G is A_6.

Hence, although we have no classification-free proof that simple groups are 2-generated, in fact they are *overwhelmingly* so – almost any pair of elements will do. However, it is not the case that these generating pairs are spread evenly around the group. Consider, for example, the alternating group A_n, and let x be a 3-cycle. If x is to generate A_n with some other element y, then y must contain a cycle of length at least $n-2$, since $\langle x, y\rangle$ must be transitive. A straightforward counting argument then shows that the probability that a randomly-chosen y generates with x tends rapidly to zero as n grows. Hence, although there are many generating pairs for A_n, very few of them feature x.

One lovely combinatorial object which is used to analyse the structure of the generating pairs is the *generating graph* $\Gamma(G)$, whose definition is due to Liebeck and Shalev in (64). The graph $\Gamma(G)$ has as vertices the nonidentity elements of G, and two vertices form an edge if and only if they generate G. Many algebraic facts about G correspond to nice combinatorial properties of $\Gamma(G)$, and as we shall now see, the original definition was made for this reason.

The *clique number* of a graph Γ is the size of the largest complete induced subgraph. Notice that a clique in $\Gamma(G)$ is a subset S of G such that every pair of distinct elements of S generates G. For a group G, let $m(G)$ denote the minimal index of a proper subgroup of G. In (64), Liebeck and Shalev prove that there exists an absolute constant α such that if G is a finite simple group then

$$1 - \frac{\alpha}{m(G)} \leq P(G).$$

Bounds on $P(G)$ are statements about edge density in $\Gamma(G)$, so Turán's theorem immediately yields that there exists an absolute constant c such

that if G is a nonabelian finite simple group then $\Gamma(G)$ contains a clique of size at least $c \cdot m(G)$.

This lower bound is far from tight, in general. For example, the minimal index of a proper subgroup of A_n is n, but Blackburn showed in (9) that if n is sufficiently large and congruent to 2 modulo 4 then the clique number of $\Gamma(\mathrm{A}_n)$ is 2^{n-2}; he also proved a similar result for S_n. In Stringer's PhD thesis (93), it was shown that "sufficiently large" could be taken to be "at least 22". It would be fascinating to see whether more combinatorial arguments about the structure of graphs $\Gamma(G)$ could be used to prove stronger lower bounds on the clique number, for other simple groups G.

Further *upper* bounds on clique numbers have been proved by using the observation that the clique number of any graph is at most its chromatic number, and in turn the chromatic number of $\Gamma(G)$ is bounded above by $\sigma(G)$, the smallest number of proper subgroups of G whose union is G. This number $\sigma(G)$ is called the *covering number* of G. See (69) and (70) for much more information about these parameters.

A *coclique* in a graph Γ is a subset of the vertices such that no two vertices are adjacent (cocliques are sometimes known as sets of *independent* vertices). In the generating graph $\Gamma(G)$, this corresponds to a subset of G such that every pair of elements generates a proper subgroup of G. There are some obvious cocliques in any generating graph: firstly, the elements of any proper subgroup form a coclique, and (slightly less obviously) since any two involutions generate a dihedral group, if the group G has even order and is not dihedral then the set of all involutions forms a coclique in $\Gamma(G)$. However, it is far from clear whether these cocliques are *maximal*, in the sense that all other vertices of $\Gamma(G)$ are adjacent to at least one vertex in the coclique.

Saunders in (87) completely classfied the cocliques of $\Gamma(\mathrm{PSL}_2(p))$ of size larger than $129(p-1)/2$, where p is prime. It turns out that they are only the maximal subgroups and the set of all involutions. This was done by a detailed analysis of the full subgroup lattice of $\mathrm{PSL}_2(p)$. More recently, Kelsey and the author in (49) considered G equal to S_n or A_n, and showed that for $n > 6$ the maximal intransitive subgroups $G \cap (\mathrm{S}_k \times \mathrm{S}_{n-k})$ are maximal cocliques if and only if $G = \mathrm{A}_n$ or $\gcd(n,k) = 1$. Analysis of the maximal imprimitive subgroups is work in progress, and in general the question of determining the maximal cocliques of $\Gamma(G)$ is wide open.

Much of the inspiration for work on the generating graph was prompted

by questions of connectivity. What can be said about the isolated vertices of $\Gamma(G)$? What can be said about the connected components? If G has a normal subgroup N such that G/N is not cyclic, then no element of N can be in a 2-element generating set, and so each element of N is an isolated vertex of $\Gamma(G)$. In (13), Breuer, Guralnick and Kantor conjectured that the converse is also true, and in dramatic recent progress, this conjecture (and much more) has been proved by Burness, Guralnick and Harper. See their paper (16) for an excellent description of some of the history of the problem, and the key results which go into the proof.

Theorem 1.12 (16) *Let G be a finite group. Then the following are equivalent, for $|G| \geq 3$.*

(a) *Every proper quotient of G is cyclic.*
(b) *$\Gamma(G)$ contains no isolated vertices.*
(c) *$\Gamma(G)$ has diameter at most two.*

It is conjectured that there is another equivalent condition to the one above for $|G| \geq 4$: the graph $\Gamma(G)$ contains a Hamiltonian cycle. This was shown to be the case for sufficiently large simple groups, for sufficiently large symmetric groups, and for almost simple sporadic groups in (14), which is also where this conjecture appears. On a related note, (68) begins the study of when $\Gamma(G)$ is Eulerian, and shows that $\Gamma(\mathrm{A}_n)$ and $\Gamma(\mathrm{S}_n)$ are Eulerian if and only if n and $n-1$ are not equal to a prime congruent to 3 modulo 4.

The above theorem completely answers the question of connectivity when there are no isolated vertices in $\Gamma(G)$. As for the general case, Lucchini showed in (67) that if G is soluble, then the induced subgraph on the nonisolated vertices of $\Gamma(G)$ is connected with diameter at most three, and gives sufficient conditions for the diameter to be two.

There has also been some interesting work on connectivity in the *complement* of $\Gamma(G)$, where two elements are joined if and only if they do *not* generate G. In fact, for nonabelian groups, it makes sense to consider a further refinement. The *commuting graph* has vertices $G \setminus \{1\}$, and an edge between two vertices if and only if they commute; whilst the *non-commuting, non-generating graph* $\Xi(G)$ has vertices $G \setminus Z(G)$, and an edge between two vertices if and only if they do not commute and do not generate G. The union of these two graphs with $\Gamma(G)$ is the complete graph on $G \setminus \{1\}$. Since the identity is not a vertex of the commuting graph, it need not be connected, and Giudici and Parker showed in (37) that the diameter of the commuting graph, if connected, may be un-

bounded. Conversely, Cameron, Freedman and the author have recently shown in (21) that if G is nilpotent then $\Xi(G)$ either has no edges, or the induced subgraph on the nonisolated vertices of $\Xi(G)$ has diameter two or three. Furthermore (21) gives necessary and sufficient conditions for the diameter to be three. This is intriguingly similar to Lucchini's results for $\Gamma(G)$ when G is soluble, from the previous paragraph.

Many other graph-theoretic questions have been studied for $\Gamma(G)$, but we shall conclude this section by asking to what extent $\Gamma(G)$ determines G. If $\Gamma(G)$ has isolated vertices, then possibly not much can be said: for example, it is not too hard to see that the generating graphs of the dihedral and quaternion groups of order 8 are isomorphic, both having one isolated vertex, and the remaining six vertices of degree 4 (the complement of a perfect matching on these six vertices).

Lucchini, Maróti and the author showed in (71) that if H is a sufficiently large simple group, or a symmetric group, and $\Gamma(G) \cong \Gamma(H)$ for some group G, then $G \cong H$. They also show that if $\Gamma(G)$ is sufficiently large and contains no isolated vertices, then $\Gamma(G)$ determines whether or not G is solvable, and if so determines G up to isomorphism.

One way to approach the question of whether $\Gamma(G)$ determines G would be to understand the automorphism group of the graph $\Gamma(G)$. This was not studied much until recently, perhaps because examination of even fairly trivial cases shows that $\mathrm{Aut}(\Gamma(G))$ is exceptionally large: the group $\mathrm{Aut}(\Gamma(\mathrm{A}_5))$ has order $2^{31} \cdot 3^7 \cdot 5$. However, in (23) an explanation is found for this large order, and a description is given of $\mathrm{Aut}(\Gamma(G))$.

The key observation is that in $\Gamma(G)$ there are, in general, many sets of elements with the same neighbours: for example, if g has prime order p, then every nonidentity element of $\langle g \rangle$ generates G with exactly the same other elements as g, and so there is a set of $p-1$ elements with identical neighbours. For $x, y \in G$, we write $N_\Gamma(x)$ for the neighbours of x, and write $x \equiv_\Gamma y$ if $N_\Gamma(x) = N_\Gamma(y)$, i.e. if x and y generate G with the same elements of G. Vertices in the same $\equiv_\Gamma$-equivalence class may be independently permuted by the automorphism group of any graph Γ so $\mathrm{Aut}(\Gamma(G))$ contains a subgroup that is the direct product of various symmetric groups, one for each $\equiv_\Gamma$-equivalence class.

One may define a quotient graph, denoted $\overline{\Gamma}_w(G)$, which has one vertex for each $\equiv_\Gamma$-class $N_\Gamma(x)$, labelled by the size $|N_\Gamma(x)|$, with an edge between $N_\Gamma(x)$ and $N_\Gamma(y)$ if and only if x and y are adjacent in Γ. It is shown in (23) that the group $\mathrm{Aut}(\Gamma(G))$ is completely determined by

the size of the equivalence classes and $\mathrm{Aut}(\overline{\Gamma}_w(G))$ (where we require the automorphisms to preserve the vertex labels). Using this, a complete description is given of $\mathrm{Aut}(\Gamma(G))$ in the case where G is soluble and $\Gamma(G)$ has no isolated vertices. It is asked whether if G is insoluble and $\Gamma(G)$ has no isolated vertices then $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{\Gamma}_w(G))$, and for the same groups G it is conjectured that $x \equiv_\Gamma y$ if and only if x and y belong to exactly the same maximal subgroups of G. This latter conjecture has just been proved by Kelsey and the author in (49), for the case $G \in \{\mathrm{A}_p, \mathrm{S}_p\}$, with p a prime not equal to $(q^d - 1)/(q - 1)$ for any prime power q.

If the reader is interested in further information about questions relating to generation, we highly recommend Burness's excellent survey article (15).

1.4 Base size

For our second application of the results in Section 1.2, we present a variety of recent work relating to the *base size* of a permutation group.

First, the definition. A *base* for a subgroup G of S_n is a sequence $\underline{\beta} = (\alpha_1, \ldots, \alpha_k)$ of points of $\Omega = \{1, \ldots, n\}$ such that the pointwise stabiliser in G of all of the points in $\underline{\beta}$ is trivial. That is,

$$\bigcap_{\alpha \in \underline{\beta}} G_\alpha = 1. \tag{1.1}$$

The size of the smallest possible base for G is called the *base size* of G, and is denoted $b(G)$.

For example, if $G \leq \mathrm{S}_n$ is generated by a single n-cycle, then the stabiliser of any point is the identity, and so we can take $\underline{\beta} = (\alpha)$ for any $\alpha \in \{1, \ldots, n\}$, and the base size is 1. Conversely, if $G = \mathrm{S}_n$ then to reach the identity subgroup we must stabilise $n - 1$ points, as otherwise there are still nontrivial permutations of the remaining points, so $b(G) = n - 1$. As an example where we do not have free choice for the base points, consider the dihedral group of order eight, acting as symmetries of the square. Here, once we have fixed one vertex, the opposite corner of the square is also fixed, but the remaining two vertices can still be interchanged. Hence a base of minimal size consists of two adjacent vertices.

The concept of a base is due to Sims (90), and bases are a key tool in computational group theory, due to the following elementary lemma.

Lemma 1.13 *Let G be a subgroup of S_n, let $\underline{\beta}$ be a base for G, and let $g, h \in G$. If $\alpha^g = \alpha^h$ for all $\alpha \in \underline{\beta}$, then $g = h$.*

That is, the sequence of base images $(\alpha_1^g, \ldots, \alpha_k^g)$ uniquely determines the group element g. This means that (with some additional data structures called strong generating sets which we shall not describe here), when working with a group on a computer it is possible to represent group elements by their sequences of base images, rather than as permutations.

The example of the cyclic group above demonstrates that this can be a much more compact representation of group elements than storing the full permutation. This begs the question: what bounds can be put on the base size, relative to n?

First, we make some combinatorial observations. Fix a base $\underline{\beta}$ for G of size k, say, and let G^i denote the stabiliser in G of the first $i-1$ points of $\underline{\beta}$, so that $G^1 = G$ and $G^{k+1} = 1$. Then $\underline{\beta}$ is called *irredundant* if the index of G^{i+1} in G^i is greater than one, for all i. Since this index is therefore at least two, and a base of minimal size is certainly irredundant, we deduce that if k is the size of an irredundant base then

$$2^{b(G)} \leq 2^k \leq |G|. \tag{1.2}$$

In another direction, since G^{i+1} is a point stabiliser in G^i, it cannot have index greater than n (by the Orbit-Stabiliser Theorem), and so

$$|G| \leq n^{b(G)}. \tag{1.3}$$

Notice that these inequalities immediately tell us that G is small if and only if $b(G)$ is small.

We shall concentrate on the base size of primitive groups, since the base sizes of imprimitive and intransitive groups are somewhat wild. Recalling Theorem 1.4, the following theorem of Liebeck should appear both beautiful and natural (however, note that it appeared nearly two decades before Maróti's result, we are being seriously ahistorical!).

Theorem 1.14 (58) *Let G be a finite primitive group of degree n. Then one of the following holds:*

(a) *G is as described in Case (a) of Theorem 1.4;*
(b) *$b(G) < 9 \log n$.*

In recent work (81), Mosciatiello and the author have improved the upper bound in Case (b) of Theorem 1.14 to say that if G is not the Mathieu

group M_{24} in its natural action on 24 points then $b(G) \leq \lceil \log n \rceil + 1$. Furthermore, we show that that there are infinitely many groups G which attain the bound. That is, either G has a rather precisely described structure, or each element of G is uniquely determined by the image of at most $\lceil \log n \rceil + 1$ points!

However, with a few more definitions under our belt, it is possible to make considerably stronger statements about $b(G)$. A faithful primitive action of an almost simple group G with socle G_0 is *standard* if it is equivalent to one of the following:

(a) G_0 is A_m for some m and the action is on subsets or partitions of $\{1, \ldots, m\}$; or
(b) G_0 is classical with natural module V, and either
   (i). each maximal subgroup M of G_0 containing $G_\alpha \cap G_0$, where G_α is the point stabiliser, is the stabiliser in G_0 of a nondegenerate, totally singular or nonsingular subspace of V; or
   (ii). $G_0 = \mathrm{Sp}_{2d}(q)$, q is even and the point stabiliser is a maximal orthogonal subgroup of G.

Otherwise, G is *non-standard*.

In Case (a) above, the point stabiliser is a maximal intransitive or imprimitive subgroup; whilst in Case (b)(i) the intersection of the point stabiliser and the socle is contained in a member of Aschbacher's Class $\mathcal{C}_1$, and in Case (b)(ii) the point stabiliser is a member of Class $\mathcal{C}_8$. In fact, whilst orthogonal groups in odd dimension $2d + 1$ are usually only defined over fields $\mathbb{F}_q$ of odd order, this is because if q is even then $\mathrm{GO}_{2d+1}(q)$ fixes a 1-dimensional subspace, and is isomorphic to the symplectic group $\mathrm{Sp}_{2d}(q)$. If one permits these orthogonal groups to exist, then Case (b)(ii) above disappears.

In 1993, Cameron and Kantor conjectured in (22) that there exists an absolute constant c such that every non-standard almost simple primitive group G satisfies $b(G) \leq c$. This conjecture was proved in 1999 by Liebeck and Shalev (65). In a sequence of papers, culminating in 2009 paper by Burness, Liebeck and Shalev (18), and a 2011 paper by Burness, Guralnick and Saxl (17), it was shown that one may take the constant c to be 7. Furthermore, there is a unique example with $b(G) = 7$, namely the Mathieu group M_{24} in its natural action on 24 points (which confirms a further conjecture of Cameron in (20)). It is by combining this result with (1.3) that one can deduce the strengthening of Theorem 1.5 that we mentioned.

The next highly influential conjecture regarding base size is due to Laslo Pyber. From (1.3) we deduce that $b(G) \geq (\log |G|)/(\log n)$. In 1993, Pyber conjectured in (83) that there exists a constant c such that for all primitive groups G of degree n,

$$b(G) \leq c\frac{\log |G|}{\log n}.$$

Many authors worked on various cases of this conjecture, we mention just a couple of papers from which the interested reader can find others. The case of groups of diagonal type was settled by Fawcett in (35), and building on work of Benbenishty and the proof of the Cameron-Kantor conjecture, Burness and Seress in (19) completed the proof for all non-affine primitive groups. The conjecture was finally proved in 2018 by Duyan, Halasi and Maróti (33): see their paper for the full list of previous work. Slightly more recently again, in (38) a version was given with all constants explicit: the base size $b(G)$ of a primitive group G of degree n satisfies

$$b(G) \leq 2\frac{\log |G|}{\log n} + 24,$$

and this bound is asymptotically best possible.

1.5 Graph isomorphism and related problems

At the beginning of Section 1.4, we mentioned that a key motivation for studying base size is computational complexity, so let us finish with some discussion of this. It should be intuitively clear that the number of points required to uniquely determine each group element will be a key factor in the running time of a great many algorithms, but rather than enumerating a long list of methods we focus just a few results, of a combinatorial nature.

A *decision problem* is any problem with a yes/no answer. Complexity class P consists of all decision problems that can be solved in time that is bounded above by a polynomial function of the input size. Complexity class NP consists of all decision problems for which the answer "yes" can be *checked* in time polynomial in the input size, given some kind of certificate that the answer is indeed yes. For example, a certificate that a graph is Hamiltonian could be a list of the edges in a Hamiltonian circuit: all we need to do is check that the edges do indeed form such a

circuit. It is clear that $\mathsf{P} \subseteq \mathsf{NP}$, since if the answer can be computed in polynomial time then we can just take an empty certificate, and work from scratch. It is a famous open problem to determine whether $\mathsf{P} = \mathsf{NP}$.

One very well studied example is the *graph isomorphism problem*, which takes as input two graphs, and asks one to determine whether or not they are isomorphic. There is no known polynomial-time solution to this problem, so it is not known to lie in P. (For the purposes of polynomial-time statements, we can take the input size to be the number of vertices.) Conversely, it is clear that the graph isomorphism problem lies in NP, since an explicit bijection between the two graphs can easily be checked in polynomial time. Graph isomorphism is not known to be NP-complete (the NP-complete problems are the hardest problems in NP), and indeed if the graph isomorphism problem is not in P then it is thought to be one of the easier problems in $\mathsf{NP} \setminus \mathsf{P}$.

In 1982, Luks showed in (73) that the graph isomorphism problem is polynomial-time reducible to a somewhat more general problem, known as the *string isomorphism problem*, which is as follows. One is given two functions f and g from a finite set Ω to a set Σ, and a permutation group $G \leq \mathrm{Sym}(\Omega)$, and one is asked to determine whether there exists an element σ of G such that $f^\sigma = g$, where the action is $f^\sigma(\alpha) = f(\alpha^{\sigma^{-1}})$. If so, then we return all such σ. The action of σ on f may look a little odd, but if one represents f and g by $|\Omega|$-tuples of elements of Σ then σ is just permuting the coordinates.

Let's see how the graph isomorphism problem can be reduced to the string isomorphism problem. Suppose we have two graphs, Γ_1 and Γ_2, both with vertex set $\{1, \ldots, m\}$ (if the vertex sets have different sizes then the problem is easy!). We let Ω be the set of 2-subsets of $\{1, \ldots, m\}$, let $\Sigma = \{0, 1\}$, and let f and g be the characteristic functions of the edge sets of Γ_1 and Γ_2. That is, f and g return 1 if $\{i, j\}$ is an edge in their graph, and 0 otherwise. We let G be the subgroup of the symmetric group on Ω given by the natural action of G on 2-subsets of $\{1, \ldots, m\}$, so that G is the automorphism group of the complete graph K_m. Then each graph isomorphism from Γ_1 to Γ_2 is an element σ of G, and this element σ naturally induces a string isomorphism from f to g. Hence the graph isomorphism problem reduces in polynomial time to the string isomorphism problem.

Theorem 1.15 (73) *Fix an integer k, and let Ξ be the set of all*

graphs of degree at most k. Then the graph isomorphism problem for graphs in Ξ can be solved in polynomial time.

Luks proved this theorem by showing that if a permutation group G has no composition factor of order greater than k, for some fixed k, then the string isomorphism problem is solvable in polynomial time.

We give a very brief sketch of some of the ideas in Luks' solution to the string isomorphism problem; a slightly more detailed exposition is given in (40). First, one reduces to the case of G being transitive on Ω, since otherwise one can recursively solve the problem for the restriction of G to an orbit Δ of Ω, and then solve a slightly modified problem for the action of the pointwise stabiliser $G_{(\Delta)}$ on $\Omega \setminus \Delta$. Gluing these two solutions together is comparatively straightforward.

Next, one considers a minimal block system $\mathcal{B}$, and the (primitive) induced action $G^{\mathcal{B}}$. We shall use the following 1982 theorem of Babai, Cameron and Palfy, which we state in somewhat less generality than it was proved.

Theorem 1.16 (7) *Fix an integer m. Then there exists a constant $c(m)$ such that if $H \leq \mathrm{S}_n$ is primitive and has no nonabelian composition factor of order greater than m, then $|H| \leq n^{c(m)}$.*

Let K be the kernel of the action of G on $\mathcal{B}$. Since $G^{\mathcal{B}}$ is primitive, it follows from Theorem 1.16 and our assumption on the composition factors of G that there are only polynomially many cosets of K in G. Furthermore, K is intransitive, and we have already seen how to solve the problem for intransitive groups. Carefully defining the strings to be examined, and then gluing these recursive solutions together, gives the result.

In a dramatic breakthrough, Babai in (5; 6) proved that the string isomorphism problem, and hence the graph isomorphism problem, can be solved in *quasipolynomial time*: time $2^{O((\log n)^c)}$, for some absolute constant c. Babai did so by replacing the polynomial bound in Theorem 1.16 by the bound $2^{\log n(\log n+1)}$ in Theorem 1.4(c), and then performing an *extremely* careful analysis of the groups in Theorem 1.4(a). Helfgott then re-analysed Babai's approach, and was able to show that one can take $c = 3$, see (40).

Luks in (74) had studied other permutation problems believed to lie strictly between P and NP, and developed what is now called the *Luks*

hierarchy. When analysing the complexity of permutation group algorithms, each subgroup of S_n is input via a set of generating permutations; any such generating set can be taken to have size at most $O(n^2)$, by Sims' work on bases and strong generating sets. Thus we measure the complexity as a function of n.

The easiest problem in the Luks hierarchy is the graph isomorphism problem. At least as difficult as the graph isomorphism problem, and all equivalent to each other, are three permutation group problems: the problem of finding the intersection of two subgroups of S_n; the problem of finding the setwise stabiliser of some subset Δ of $\{1, \ldots, n\}$ in a group $G \leq \mathrm{S}_n$; and the problem of finding the centraliser in a group $G \leq \mathrm{S}_n$ of an element $x \in \mathrm{S}_n$. These three problems (and others which are equally difficult) form what is known as the *Luks class*. At least as hard as all of these is the *normaliser problem*: given two subgroups G and H of S_n, find $\mathrm{N}_H(G)$. A special case of the normaliser problem, whose difficulty relative to the Luks class is unknown, is the problem of computing $\mathrm{N}_{\mathrm{S}_n}(G)$, that is the case $H = \mathrm{S}_n$.

The setwise stabiliser problem is readily seen to be a special case of the string isomorphism problem: given $G \leq \mathrm{S}_n$, and a subset Δ of $\{1, \ldots, n\}$, take $f = g$ to be the characteristic function of Δ (so $f(\alpha) = 1$ if and only if $\alpha \in \Delta$). Thus Babai's result shows that all of the problems in the Luks class can be solved in quasipolynomial time.

There are two obvious open problems left. One is to try to reduce Helfgott's constant down from $c = 3$ to $c = 1$ (which would be a polynomial-time solution) or, conversely and somewhat more dramatically, to show that no such reduction is possible (which would prove that $\mathsf{P} \neq \mathsf{NP}$). The other, which seems more tractable, is the normaliser problem.

For a long time, it was not even known whether the normaliser problem could be solved in time that was simply exponential in n, since a naive algorithm involves looking through up to all $2^{n \log n}$ elements of S_n for normalising elements. However, Wiebking in (96) has recently shown that the normaliser problem can be solved in time $2^{O(n)}$.

One way to look for more tractable special cases is to restrict the group H. In this vein, Luks and Miyazaki in (75) used somewhat similar ideas to those of (73) to show the following. Let Γ_d be the class of permutation groups for which every nonabelian composition factor is a subgroup of S_d (this is closely related to the class of groups considered in Theorem 1.16, but includes imprimitive and intransitive groups as well; in particular

all soluble groups are in Γ_d). Then Luks and Miyazaki showed that for fixed d, if $H \in \Gamma_d$ then $N_H(G)$ can be computed in polynomial time.

The other way to look for more tractable special cases is to restrict the group G. Since Babai showed in particular that the intersection problem can be solved in quasipolynomial time, if all one seeks is a *quasipolynomial* solution to the normaliser problem, it suffices to study the special case $\mathrm{N}_{\mathrm{S}_n}(G)$. In very recent work the author and Siccha used this observation to prove the following.

Theorem 1.17 (86) *Let $G \leq \mathrm{S}_n$ be primitive. Then one can compute $\mathrm{N}_{\mathrm{S}_n}(G)$, and hence $\mathrm{N}_H(G)$, in time $2^{O((\log n)^3)}$.*

One key tool in the proof is the fact, due to Derek Holt and the author in (46), that a subnormal subgroup of a primitive group G of degree $n > 3$ can be generated by at most $\log n$ elements (one could instead use the asymptotic result due to Lucchini, Menegazzo and Morigi in (72) that such a G can be generated by $O(\log n/(\sqrt{\log \log n}))$ elements).

Special methods are developed to compute the normaliser of groups lying in Case (a) of Theorem 1.14. For groups in Case (b) of the theorem, one first observes that an element σ of S_n lies in $\mathrm{N}_{\mathrm{S}_n}(G)$ if and only if σ conjugates each of the $O(\log n)$ generators of G to elements of G. Next, notice that by Theorem 1.14, one can test whether an element g^σ lies in G by looking at $9 \log n$ base point images of g^σ, so one can test whether $\sigma \in \mathrm{N}_{\mathrm{S}_n}(G)$ without completely describing the permutation σ.

Acknowledgements The author would like to thank Derek Holt and Veronica Kelsey for carefully reading a draft of this article, and making many helpful suggestions. The author would also like to thank the anonymous referee, whose thoughtful comments greatly improved the paper.

References

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

[2] M. Aschbacher. Chevalley groups of type G_2 as the group of a trilinear form. *J. Algebra* **109** (1987), 193–259.

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

[4] M. Aschbacher and L. Scott. Maximal subgroups of finite groups. *J. Algebra* **92** (1985), 44–80.

[5] L. Babai. Graph isomorphism in quasipolynomial time. arXiv e-print 1512.03547.
[6] L. Babai. Graph isomorphism in quasipolynomial time. In *Proceedings of STOC'16*, (ACM, New York, 2016), 684–697.
[7] L. Babai, P. J. Cameron and P. P. Pálfy. On the orders of primitive groups with restricted nonabelian composition factors. *J. Algebra* **79** (1982), 161–168.
[8] E. R. Bennett. Primitive groups with a determination of the primitive groups of degree 20. *Amer. J. Math.* **34** (1912), 1–20.
[9] S. R. Blackburn. Sets of permutations that generate the symmetric group pairwise. *J. Combin. Theory Ser. A* **113** (2006), 1572–1581.
[10] A. Bochert. Über die Transitivitätsgrenze der Substitutionengruppen, welche die Alternierende ihres Grades nicht einhalt. *Math. Ann.* **33** (1889), 572–583.
[11] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997), 235–265.
[12] J. N. Bray, D. F. Holt and C. M. Roney-Dougal. The maximal subgroups of the low-dimensional finite classical groups. Lond. Math. Soc. Lecture Note Ser. **407**. *Cambridge Univ. Press, Cambridge*, 2013.
[13] T. Breuer, R. M. Guralnick and W. M. Kantor. Probabilistic generation of finite simple groups II. *J. Algebra* **320** (2008), 443–494.
[14] T. Breuer, R. M. Guralnick, A. Lucchini, A. Maróti and G. P. Nagy. Hamiltonian cycles in the generating graphs of finite groups. *Bull. Lond. Math. Soc.* **42** (2010), 621–633.
[15] T. C. Burness. Simple groups, generation and probabilistic methods. In *Groups St Andrews 2017 in Birmingham*, London Math. Soc. Lecture Note Ser. **455** (Cambridge Univ. Press, Cambridge), 2019, 200–229.
[16] T. C. Burness, R. M. Guralnick and S. Harper. The spread of a finite group. arXiv e-print. 2006.01421.
[17] T. C. Burness, R. M. Guralnick and J. Saxl. On base sizes for symmetric groups. *Bull. Lond. Math. Soc.* **43** (2011), 386–391.
[18] T. C. Burness, M. W. Liebeck and A. Shalev. Base sizes for simple groups and a conjecture of Cameron, *Proc. Lond. Math. Soc.* **98** (2009), 116–162.
[19] T. C. Burness and A. Seress. On Pyber's base size conjecture. *Trans. Amer. Math. Soc.* **367** (2015), 5633–5651.
[20] P. J. Cameron. Permutation groups. Lond. Math. Soc. Student Texts **45**. *Cambridge Univ. Press, Cambridge*, 1999.
[21] P. J. Cameron, S. D. Freedman and C. M. Roney-Dougal. The non-commuting, non-generating graph of a nilpotent group. arXiv e-print 2008.09291.
[22] P. J. Cameron and W. M. Kantor. Random permutations: some group-theoretic aspects. *Combin. Probab. Comput.* **2** (1993), 257–262.
[23] P. J. Cameron, A. Lucchini and C. M. Roney-Dougal. Generating sets of finite groups. *Trans. Amer. Math. Soc.* **370** (2018), 6751–6770.
[24] P. J. Cameron, P. M. Neumann and D. N. Teague. On the degrees of primitive permutation groups. *Math. Z.* **180** (1982), 141–149.

[25] J. Cannon and D. F. Holt. Computing maximal subgroups of finite groups. *J. Symbolic Comput.* **37** (2004), 589–609.

[26] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson. An ATLAS of Finite Groups. *Clarendon Press, Oxford*, 1985; reprinted with corrections 2003.

[27] B. N. Cooperstein. Maximal subgroups of $G_2(2^n)$. *J. Algebra* **70** (1981), 23–36.

[28] H. J. Coutts, M. R. Quick and C. M. Roney-Dougal. The primitive groups of degree less than 4096. *Comm. Algebra* **39** (2011), 3526–3546.

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

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

[31] J. D. Dixon and B. Mortimer. The primitive permutation groups of degree less than 1000. *Math. Proc. Cambridge Philos. Soc.* **103** (1988), 213–238.

[32] J. D. Dixon and B. Mortimer. Permutation Groups. Graduate Texts in Mathematics **163**. *Springer-Verlag, New York*, 1996.

[33] H. Duyan, Z. Halasi and A. Maróti. A proof of Pyber's base size conjecture. *Adv. Math.* **331** (2018), 720–747.

[34] B. Eick and A. Hulpke. Computing the maximal subgroups of a permutation group. I. In *Groups and computation, III (Columbus, OH, 1999)*, (de Gruyter, Berlin (2001)), 155–168.

[35] J. B. Fawcett. The base size of a primitive diagonal group. *J. Algebra* **375** (2013), 302–321.

[36] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.0*; 2020, `https://www.gap-system.org`.

[37] M. Giudici and C. Parker. There is no upper bound for the diameter of the commuting graph of a finite group. *J. Combin. Theory Ser. A* **120** (2013), 1600–1603.

[38] Z. Halasi, M. W. Liebeck and A. Maróti. Base sizes of primitive groups: bounds with explicit constants. *J. Algebra* **521** (2019), 16–43.

[39] J. Häsä, Growth of cross-characteristic representations of finite quasisimple groups of Lie type. *J. Algebra* **407** (2014), 275–306.

[40] H. A. Helfgott. Isomorphismes de graphes en temps quasi-polynomial (d'après Babai et Luks, Weisfeiler-Leman). *Astérisque*, **407** (2019), 135–182.

[41] G. Hiß, W. J. Husen and K. Magaard. Imprimitive irreducible modules for finite quasisimple groups. *Mem. Amer. Math. Soc.* **234** (2015).

[42] G. Hiß and K. Magaard. Imprimitive irreducible modules for finite quasisimple groups. II. *Trans. Amer. Math. Soc.* **371** (2019), 833–882.

[43] G. Hiß and G. Malle. Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math.* **4** (2001), 22–63. Corrigenda: *LMS J. Comput. Math.* **5** (2002), 95–126.

[44] D. F. Holt and C. M. Roney-Dougal. Constructing maximal subgroups of classical groups. *LMS J. Comput. Math.* **8** (2005), 46–79.

[45] D. F. Holt and C. M. Roney-Dougal. Constructing maximal subgroups of orthogonal groups. *LMS J. Comput. Math.* **13** (2010), 164–191.

[46] D. F. Holt and C. M. Roney-Dougal. Minimal and random generation of permutation and matrix groups. *J. Algebra* **387** (2013), 195–214.

[47] C. Jordan. Traité des substitutions et des equations algébriques. *Gauthier-Villers, Paris*, 1871.

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

[49] V. Kelsey and C. M. Roney-Dougal. Maximal cocliques in the generating graphs of the alternating and symmetric groups. arXiv e-print 2007.12021.

[50] O. H. King. The subgroup structure of finite classical groups in terms of geometric configurations. In *Surveys in combinatorics, 2005* (ed. B. S. Webb), Lond. Math. Soc. Lecture Note Ser. **327** (Cambridge Univ. Press, Cambridge, 2005), 29–56.

[51] P. B. Kleidman. The maximal subgroups of the low-dimensional classical groups. PhD Thesis, University of Cambridge, 1987.

[52] P. B. Kleidman. The maximal subgroups of the finite 8-dimensional orthogonal groups $\mathrm{P}\Omega_8^+(q)$ and of their automorphism groups. *J. Algebra* **110** (1987), 173–242.

[53] P. B. Kleidman. The maximal subgroups of the Steinberg triality groups ${}^3\mathrm{D}_4(q)$ and of their automorphism groups. *J. Algebra* **115** (1988), 182–199.

[54] P. B. Kleidman. The maximal subgroups of the Chevalley groups $\mathrm{G}_2(q)$ with q odd, the Ree groups ${}^2\mathrm{G}_2(q)$, and their automorphism groups. *J. Algebra* **117** (1988), 30–71.

[55] P. B. Kleidman and M. W. Liebeck. A survey of the maximal subgroups of the finite simple groups. *Geom. Dedicata* **25** (1988), 375–389.

[56] P. B. Kleidman and M. W. Liebeck. The subgroup structure of the finite classical groups. Lond. Math. Soc. Lecture Note Ser. **129**. *Cambridge Univ. Press, Cambridge*, 1990.

[57] L. G. Kovács. Maximal subgroups in composite finite groups. *J. Algebra* **99** (1986), 114–131.

[58] M. W. Liebeck. On minimal degrees and base sizes of primitive permutation groups. *Arch. Math. (Basel)* **43** (1984), 11–15.

[59] M. W. Liebeck. On the orders of maximal subgroups of the finite classical groups. *Proc. London Math. Soc. (3)* **50** (1985), 426–446.

[60] 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.

[61] M. W. Liebeck, C. E. Praeger and J. Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra* **111** (1987), 365–383.

[62] M. W. Liebeck and G. M. Seitz. A survey of maximal subgroups of exceptional groups of Lie type. In *Groups, combinatorics & geometry (Durham, 2001)*, (World Sci. Publ., River Edge, NJ, 2003), 139–146.

[63] M. W. Liebeck and A. Shalev. The probability of generating a finite simple group. *Geom. Dedicata* **56** (1995), 103–113.
[64] M. W. Liebeck and A. Shalev. Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra* **184** (1996), 31–57.
[65] M. W. Liebeck and A. Shalev. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.* **12** (1999), 497–520.
[66] F. Lübeck. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.* **4** (2001), 135–169.
[67] A. Lucchini. The diameter of the generating graph of a finite soluble group. *J. Algebra* **492** (2017), 28–43.
[68] A. Lucchini and C. Marion. Alternating and symmetric groups with Eulerian generating graph. *Forum Math. Sigma* **5** (2017), 30pp.
[69] A. Lucchini and A. Maróti. Some results and questions related to the generating graph of a finite group. In *Ischia group theory 2008*, (World Sci. Publ., Hackensack, NJ, 2009), 183–208.
[70] A. Lucchini and A. Maróti. On the clique number of the generating graph of a finite group. *Proc. Amer. Math. Soc.* **137** (2009), 3207–3217.
[71] A. Lucchini, A. Maróti and C. M. Roney-Dougal. On the generating graph of a simple group. *J. Aust. Math. Soc.* **103** (2017), 91–103.
[72] A. Lucchini, F. Menegazzo and M. Morigi. Asymptotic results for primitive permutation groups and irreducible linear groups. *J. Algebra* **223** (2000), 154–170.
[73] E. M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comput. System Sci.* **25** (1982), 42–65.
[74] E. M. Luks. Permutation groups and polynomial-time computation. In *Groups and Computation, 1991* (eds L. Finkelstein and W. M. Kantor), DIMACS Ser. Discrete Math. Theoret. Comput. Sci **11** (Amer. Math. Soc., Providence, RI, 1993), 139–175.
[75] E. M. Luks and T. Miyazaki. Polynomial-time normalizers. *Discrete Math. Theor. Comput. Sci.* **13** (2011), 61–96.
[76] K. Magaard. Some remarks on maximal subgroups of finite classical groups. In *Finite simple groups: thirty years of the atlas and beyond*, Contemp. Math. **694** (Amer. Math. Soc., Providence, RI 2017), 123–137.
[77] G. Malle. The maximal subgroups of ${}^2\mathrm{F}_4(q^2)$. *J. Algebra* **139** (1991), 52–69.
[78] A. Maróti. On the orders of primitive groups. *J. Algebra* **258** (2002), 631–640.
[79] E. N. Martin. On the imprimitive substitution groups of degree fifteen and the primitive substitution groups of degree eighteen. *Amer. J. Math.* **23** (1901), 259–286.
[80] 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.
[81] M. Mosciatello and C. M. Roney-Dougal. Base sizes of primitive permutation groups. *In preparation.*
[82] C. E. Praeger and J. Saxl. On the orders of primitive permutation groups. *Bull. London Math. Soc.* **12** (1980), 303–307.

[83] L. Pyber. Asymptotic results for permutation groups. In *Groups and Computation, 1991* (eds L. Finkelstein and W. M. Kantor), DIMACS Ser. Discrete Math. Theoret. Comput. Sci **11** (Amer. Math. Soc., Providence, RI, 1993), 197–219.

[84] D. Rogers. Maximal subgroups of classical groups in dimensions 16 and 17. PhD Thesis, University of Warwick, 2017.

[85] C. M. Roney-Dougal. The primitive groups of degree less than 2500. *J. Algebra* **292** (2005), 154–183.

[86] C. M. Roney-Dougal and S. Siccha. Normalisers of primitive permutation groups in quasipolynomial time. *Bull. Lond. Math. Soc.* **52** (2020), 358–366.

[87] J. Saunders. Maximal cocliques in $\mathrm{PSL}_2(q)$. *Comm. Algebra* **47** (2019), 3921–3931.

[88] A. K. Schröder. The maximal subgroups of the Classical Groups in Dimension 13, 14 and 15. PhD Thesis, University of St Andrews, 2015.

[89] M. W. Short. The primitive soluble permutation groups of degree less than 256. Lecture Notes in Mathematics **1519**. *Springer-Verlag, Berlin–Heidelberg*, 1992.

[90] C. C. Sims. Computational methods for permutation groups. In *Computational Problems in Abstract Algebra* (ed. J. Leech), (Pergamon, 1970), 169–183.

[91] A. K. Steel. Construction of ordinary irreducible representations of finite groups. PhD Thesis, University of Sydney, 2012.

[92] R. Steinberg. Lectures on Chevalley Groups. *Yale University Mathematics Department*, 1968.

[93] L. Stringer. Pairwise generating sets for the symmetric and alternating groups. PhD Thesis, Royal Holloway University of London, 2008.

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

[95] D. E. Taylor. The geometry of the classical groups. Sigma Series in Pure Mathematics **9**. *Heldermann Verlag, Berlin*, 1992.

[96] D. Wiebking. Normalizers and permutational isomorphisms in simply-exponential time. arXiv e-print 904.10454.

[97] R. A. Wilson. The Finite Simple Groups. Graduate Texts in Mathematics **251**. *Springer-Verlag London, Ltd., London*, 2009.

[98] R. A. Wilson. Maximal subgroups of sporadic groups. In *Finite simple groups: thirty years of the* Atlas *and beyond*, Contemp. Math. **694**, (Amer. Math. Soc., Providence, RI 2017), 57–72.

[99] R. A. Wilson. The uniqueness of $\mathrm{PSU}_3(8)$ in the Monster. *Bull. Lond. Math. Soc.* **49** (2017), 877–880.