Simple groups, fixed point ratios and applications

Timothy C. Burness

School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

Abstract. The study of fixed point ratios is a classical topic in permutation group theory, with a long history stretching back to the origins of the subject in the 19th century. Fixed point ratios arise naturally in many different contexts, finding a wide range of applications. In this survey article we focus on fixed point ratios for simple groups of Lie type, highlighting some of the main results, applications and related problems.

1. Introduction

The study of fixed point ratios is a classical topic in permutation group theory, with a long history stretching all the way back to the early days of group theory in the 19th century. The concept arises naturally in many different contexts, finding a wide range of interesting (and often surprising) applications. One of the main aims of this survey article is to highlight some of these applications. For instance, we will explain how fixed point ratios play a key role in the study of some remarkable generation properties of finite groups. We will also see how probabilistic methods, based on fixed point ratio estimates, have revolutionised the search for small bases of primitive permutation groups. In a completely different direction, we will also describe how bounds on fixed point ratios can be used to investigate the structure of monodromy groups of coverings of the Riemann sphere.

In this introductory section we start by recalling some basic properties of fixed point ratios and we present several standard examples that will be useful later. We also highlight connections to some classical notions in permutation group theory, such as minimal degree, fixity and derangements. To whet the appetite of the reader, we close the introduction by presenting three very different group-theoretic problems. It is interesting to note that none of these problems have an obvious connection to fixed point ratios, but we will show later that recent advances in our understanding of fixed point ratios (in particular, recent results for (almost) simple groups of Lie type) play an absolutely essential role in their solution.

Some of the main theorems on fixed point ratios will be highlighted in Section 2, where we focus on the simple groups of Lie type. Finally, in Sections 3, 4 and 5 we will discuss the three motivating problems mentioned above. Here we will explain the connection to fixed point ratios and we will sketch some of the main ideas. In particular, we will see how some of the results presented in Section 2 play a key role, and we will report on more recent developments and open problems.

Finally, we have also included an extensive bibliography, which we hope will serve as a useful guide for further reading.

Acknowledgments. This article is based on a lecture series I gave at the workshop *Some problems in the theory of simple groups* at the Centre Interfacultaire Bernoulli at the École Polytechnique Fédérale de Lausanne in September 2016. This workshop was part of the semester programme *Local representation theory and simple groups* at the CIB. It is a pleasure to thank the organisers of this programme for inviting me to participate and for their

generous hospitality. I would also like to thank Gunter Malle and Donna Testerman for their helpful comments on an earlier version of this article.

1.1. Preliminaries. We start with some preliminary definitions. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω. For $\alpha \in \Omega$ we will write $G_\alpha = \{x \in G \,:\, \alpha^x = \alpha\}$ for the stabiliser of α in G. Similarly, the set of fixed points of $x \in G$ will be denoted by

$$C_\Omega(x) = \{\alpha \in \Omega \,:\, \alpha^x = \alpha\}.$$

Definition 1.1. The *fixed point ratio* of $x \in G$, denoted by $\mathrm{fpr}(x,\Omega) = \mathrm{fpr}(x)$, is the proportion of points in Ω fixed by x, i.e.

$$\mathrm{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|}.$$

Notice that $\mathrm{fpr}(x)$ is the *probability* that a randomly chosen element of Ω is fixed by x (with respect to the uniform distribution on Ω). This viewpoint is often useful for applications. Indeed, in recent years probabilistic methods have been used to solve many interesting problems in finite group theory. Typically, the aim is to establish an existence result through a probabilistic approach (rather than an explicit construction, for example) – this has been a standard technique in combinatorics, number theory and other areas for many years. As we will see later, bounds on fixed point ratios play a central role in several applications of this flavour.

It is also worth noting that a fixed point ratio is a special type of *character ratio*; if $\pi : G \to \mathbb{C}$ is the corresponding permutation character, then

$$\mathrm{fpr}(x) = \frac{\pi(x)}{\pi(1)}.$$

The following lemma records some basic properties.

Lemma 1.2. *Let G be a permutation group on a finite set Ω and let x be an element of G.*

(i) $\mathrm{fpr}(x) = \mathrm{fpr}(y)$ *for all* $y \in x^G$.

(ii) $\mathrm{fpr}(x) \leqslant \mathrm{fpr}(x^m)$ *for all* $m \in \mathbb{Z}$.

(iii) *If G is transitive with point stabiliser H, then*

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

(iv) *If the derived subgroup G' is transitive, then there is a non-linear irreducible constituent χ of the permutation character such that*

$$\mathrm{fpr}(x) \leqslant \frac{1+|\chi(x)|}{1+\chi(1)}.$$

Proof. Parts (i) and (ii) are trivial.

(iii) For $\beta \in \Omega$, $g \in G$ define $(\beta, g) = 1$ if $\beta^g = \beta$, otherwise $(\beta, g) = 0$. Then

$$\begin{aligned}|x^G|\,|C_\Omega(x)| = \sum_{g \in x^G} |C_\Omega(g)| &= \sum_{g \in x^G} \left(\sum_{\beta \in \Omega} (\beta, g) \right) \\ &= \sum_{\beta \in \Omega} \left(\sum_{g \in x^G} (\beta, g) \right) = \sum_{\beta \in \Omega} |x^G \cap G_\beta|,\end{aligned}$$

which is equal to $|\Omega|\,|x^G \cap H|$ by the transitivity of G.

(iv) Set $f = \mathrm{fpr}(x)$ and write $\pi = 1 + \chi_1 + \cdots + \chi_t$ with $\chi_i \in \mathrm{Irr}(G)$. Note that the transitivity of G' implies that each χ_i is non-linear. If $1 + |\chi_i(x)| < f(1 + \chi_i(1))$ for all i then

$$\begin{aligned} f|\Omega| = 1 + \sum_i \chi_i(x) \leqslant 1 &+ \sum_i |\chi_i(x)| \\ &= \sum_i (1 + |\chi_i(x)|) - (t-1) \\ &< f\left(\sum_i (1 + \chi_i(1)) \right) - (t-1) \\ &= f|\Omega| - (1-f)(t-1), \end{aligned}$$

which is a contradiction. □

The formula in part (iii) of the previous lemma is a key tool for computing fixed point ratios for transitive groups. Indeed, it essentially reduces the problem to determining the fusion of H-classes in G, which may be more tractable.

EXAMPLE 1.3. $\mathrm{Sym}(n)$ *on* 2*-sets.*

Let $G = \mathrm{Sym}(n)$ be the symmetric group of degree $n \geqslant 5$, let $x = (1,2,3) \in G$ and let Ω be the set of 2-element subsets of $\{1, \ldots, n\}$. Then $|\Omega| = \binom{n}{2}$ and the action of G is transitive, with point stabiliser $H = \mathrm{Sym}(n-2) \times \mathrm{Sym}(2)$. We compute $\mathrm{fpr}(x)$ in three different ways:

a. *Direct calculation.* We have $C_\Omega(x) = \{\{a,b\} : a, b \in \{4, \ldots, n\}\}$, so $|C_\Omega(x)| = \binom{n-3}{2}$ and thus

$$\mathrm{fpr}(x) = \frac{(n-3)(n-4)}{n(n-1)}. \tag{1.1}$$

b. *Permutation character.* Let π be the permutation character. The action of G on Ω has rank 3 (that is, H has three orbits on Ω) and by *Young's Rule* we have

$$\pi = 1 + \chi^{(n-1,1)} + \chi^{(n-2,2)},$$

where χ^λ is the character of the irreducible *Specht module* S^λ corresponding to the partition λ of n (see [**61**, Section 14], for example). By applying the *Hook Formula* for dimensions and the *Murnaghan-Nakayama Rule* for character values (see [**61**, Sections 20 and 21]), we calculate that

$$\chi^{(n-1,1)}(x) = \chi^{(n-4,1)}(1) = n-4$$

and

$$\chi^{(n-2,2)}(x) = \chi^{(n-5,2)}(1) = (n-3)(n-6)/2$$

if $n \geqslant 7$ (one can check that $\chi^{(3,2)}(x) = -1$ and $\chi^{(4,2)}(x) = 0$), so

$$\mathrm{fpr}(x) = \frac{1+(n-4)+(n-3)(n-6)/2}{n(n-1)/2} = \frac{(n-3)(n-4)}{n(n-1)}.$$

c. *Conjugacy classes.* All the 3-cycles in G are conjugate, so $x^G \cap H$ is the set of 3-cycles in H. This gives

$$|x^G \cap H| = |x^H| = 2\binom{n-2}{3}, \quad |x^G| = 2\binom{n}{3}$$

and thus Lemma 1.2(iii) implies that (1.1) holds.

Example 1.4. $\mathrm{GL}_n(q)$ *on vectors.*

Consider the action of $G = \mathrm{GL}_n(q)$ on its natural module $V = \mathbb{F}_q^n$. For $x \in G$ we have $\mathrm{fpr}(x) = q^{d-n}$, where d is the dimension of the 1-eigenspace of x on V.

Example 1.5. $\mathrm{PGL}_n(q)$ *on* 1*-spaces.*

Similarly, we can consider the transitive action of $G = \mathrm{PGL}_n(q) = \mathrm{GL}_n(q)/Z$ on the set of 1-dimensional subspaces of V. Suppose q is odd and set $x = \hat{x}Z \in G$, where $\hat{x} \in \mathrm{GL}_n(q)$ is the block-diagonal matrix $[-I_1, I_{n-1}]$ with respect to a basis $\{e_1, \ldots, e_n\}$ for V (here, and elsewhere, we use I_m to denote the $m \times m$ identity matrix). Then x fixes $\langle e_1 \rangle$ and every 1-space in $\langle e_2, \ldots, e_n \rangle$, and no others, so

$$\mathrm{fpr}(x) = \frac{1+\frac{q^{n-1}-1}{q-1}}{\frac{q^n-1}{q-1}} = \frac{q^{n-1}+q-2}{q^n-1} \sim \frac{1}{q}.$$

Alternatively, note that a point stabiliser $H = q^{n-1}{:}(\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q))/Z$ is a maximal parabolic subgroup of G and one checks that $x^G \cap H$ is a union of two H-classes. More precisely,

$$|x^G \cap H| = q^{n-1} + q \cdot \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{GL}_{n-2}(q)||\mathrm{GL}_1(q)|}, \quad |x^G| = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-1}(q)||\mathrm{GL}_1(q)|}$$

which provides another way to compute $\mathrm{fpr}(x)$ via Lemma 1.2(iii).

1.2. Problems. It is natural to consider the following problems, either in the context of a specific permutation group, or more typically for an interesting family of permutation groups, such as primitive groups and almost simple groups.

1. Given a permutation group G and $x \in G$, compute $\mathrm{fpr}(x)$.
2. Obtain upper and lower bounds on $\mathrm{fpr}(x)$ (in terms of parameters depending on G and x).

3. Compute (or bound) the minimal and maximal fixed point ratios $\min\{\mathrm{fpr}(x) : x \in G\}$ and $\max\{\mathrm{fpr}(x) : 1 \neq x \in G\}$.
4. We can also consider "local" versions. For example, given a (normal) subset $S \subseteq G \setminus \{1\}$, compute (or bound) $\min\{\mathrm{fpr}(x) : x \in S\}$ and $\max\{\mathrm{fpr}(x) : x \in S\}$.

   For instance, we may be interested in the case where S is the set of elements of prime order in G, or the set of involutions, etc. Note that $\max\{\mathrm{fpr}(x) : 1 \neq x \in G\}$ and $\max\{\mathrm{fpr}(x) : x \in G, |x| \text{ prime}\}$ are equal by Lemma 1.2(ii).

As we will see later, bounds on fixed point ratios (in particular, *upper* bounds) are often sufficient for the applications we have in mind.

The above problems are closely related to some classical notions in permutation group theory. To see the connection, let us fix a permutation group $G \leqslant \mathrm{Sym}(\Omega)$ of degree n.

a. *Minimal degree:* The minimal degree $\mu(G)$ of G is defined to be the smallest number of points moved by any non-identity element, i.e.

$$\mu(G) = \min_{1 \neq x \in G} (n - |C_\Omega(x)|) = n\left(1 - \max_{1 \neq x \in G} \mathrm{fpr}(x)\right).$$

For example, $\mu(\mathrm{Sym}(n)) = 2$ and $\mu(\mathrm{Alt}(n)) = 3$. This is a classical invariant studied by Jordan, Bochert, Manning and others (see Section 2.2).

b. *Fixity:* Similarly, the largest number of fixed points of a non-identity element is called the *fixity* of G, denoted by

$$f(G) = n\left(\max_{1 \neq x \in G} \mathrm{fpr}(x)\right) = n - \mu(G).$$

In addition, $\max_{1 \neq x \in G} \mathrm{fpr}(x)$ is sometimes referred to as the *fixity ratio*. This has been studied by Liebeck, Saxl, Shalev and others.

If we take S to be the set of involutions in G, then $n\left(\max_{x \in S} \mathrm{fpr}(x)\right)$ is the *involution fixity* of G. This concept was studied by Bender in the early 1970s, who classified the transitive groups with involution fixity 1 (for example, the 3-transitive action of $\mathrm{PSL}_2(2^m)$ on the projective line has this property). See [**32, 35, 82**] for more recent results in the context of almost simple primitive groups.

c. *Derangements:* An element $x \in G$ is a *derangement* if $\mathrm{fpr}(x) = 0$, so

$$\min_{1 \neq x \in G} \mathrm{fpr}(x) = 0 \iff G \text{ contains a derangement.}$$

The existence and abundance of derangements has been intensively studied for many years, finding a wide range of applications. We refer the reader to [**25**, Chapter 1], and the references therein.

1.3. Applications. The above problems have an intrinsic interest in their own right, but much of the motivation for studying fixed point ratios stems from the wide range of applications. In order to motivate some of these applications, we close this introduction by presenting three very different problems involving simple groups where fixed point ratios play a key role. We will return to these problems in Sections 3, 4 and 5.

1. *Generating graphs.*

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 $G = \langle x, y \rangle$.

PROBLEM A. *Let G be a nonabelian finite simple group. Prove that $\Gamma(G)$ is a connected graph with diameter 2.*

2. *Monodromy groups.*

Let g be a non-negative integer and let $\mathcal{E}(g)$ be the set of nonabelian non-alternating composition factors of monodromy groups of branched coverings $f : X \to \mathbb{P}^1(\mathbb{C})$ of the Riemann sphere, where X is a compact connected Riemann surface of genus g.

PROBLEM B. *Prove that $\mathcal{E}(g)$ is finite.*

3. *Bases.*

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group. A subset $B \subseteq \Omega$ is a *base* for G if the pointwise stabiliser of B in G is trivial. The *base size* $b(G)$ of G is the minimal size of a base for G.

PROBLEM C. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive nonabelian finite simple group with point stabiliser H satisfying the following conditions:*

(i) *If $G = \mathrm{Alt}(m)$, then H acts primitively on $\{1, \ldots, m\}$.*

(ii) *If G is a classical group, then H acts irreducibly on the natural module.*

Prove that $b(G) \leqslant 7$, with equality if and only if G is the Mathieu group M_{24} in its natural action on 24 points.

2. Simple groups

In this section we focus on fixed point ratios for primitive simple groups of Lie type. We start with a brief discussion of primitivity in Section 2.1, before turning our attention to the connection between fixed point ratios and the classical notion of minimal degree. In Section 2.3 we introduce a theorem of Liebeck and Saxl (see Theorem 2.6), which provides an essentially best possible upper bound on fixed point ratios for simple groups of Lie type. For the remainder of the section, we look at ways in which this theorem can be strengthened in special cases of interest. For example, we will explain how much stronger bounds have been established for so-called *non-subspace* actions of classical groups – later we will see that these improved fixed point ratio estimates are essential for the applications we have in mind.

Finally, a word or two on notation. For the remainder of this article we will adopt the notation for simple groups used by Kleidman and Liebeck (see [**68**, Section 5.1]). Notice that this differs slightly from the notation in the Atlas [**34**]. For instance, we will write $\mathrm{P}\Omega_n^{\epsilon}(q)$ for a simple orthogonal group (where $\epsilon = \pm$ when n is even) and $\mathrm{O}_n^{\epsilon}(q)$ is the isometry group of the underlying quadratic form.

2.1. Primitivity. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group, with orbits Ω_i, $i \in I$. Then G induces a transitive permutation group G^{Ω_i} on each Ω_i; these are called the *transitive constituents* of G. In some sense, G is built from its transitive constituents; indeed, G is a subdirect product of the G^{Ω_i} (that is, the corresponding projection maps $G \to G^{\Omega_i}$ are surjective). For example, $G = \{1, (1,2)(3,4)\}$ has orbits $\Omega_1 = \{1,2\}$ and $\Omega_2 = \{3,4\}$ on $\Omega = \{1,2,3,4\}$, and G is a proper subdirect product of $G^{\Omega_1} = \{1,(1,2)\}$ and $G^{\Omega_2} = \{1,(3,4)\}$. For the purposes of studying fixed point ratios, it is natural to assume that G is transitive.

In turn, the transitive constituents themselves may be built from smaller permutation groups in a natural way. This leads us to the notion of *primitivity.* This is an important irreducibility condition that allows us to define the *primitive groups*, which are the basic building blocks of all permutation groups.

Definition 2.1. A transitive group $G \leqslant \mathrm{Sym}(\Omega)$ is *imprimitive* if Ω admits a nontrivial G-invariant partition, otherwise G is *primitive.*

Here the trivial partitions are $\{\Omega\}$ and $\{\{\alpha\} : \alpha \in \Omega\}$. It is an easy exercise to show that G is primitive if and only if a point stabiliser $H = G_\alpha$ is a maximal subgroup of G, which is a useful characterisation. For instance, the action of $G = \mathrm{Sym}(n)$ on the set of k-element subsets of $\{1,\ldots,n\}$ is primitive for all $1 \leqslant k < n$, $k \neq n/2$ (note that G is imprimitive if $k = n/2$ since $G_\alpha < \mathrm{Sym}(n/2) \wr \mathrm{Sym}(2) < G$). Any transitive group of prime degree is primitive and all 2-transitive groups are primitive.

It turns out that the abstract structure of a finite primitive group G is rather restricted (observe that transitivity alone imposes no structural restrictions whatsoever). For example, the socle of G (denoted $\mathrm{soc}(G)$) is a direct product of isomorphic simple groups (recall that the *socle* of a group is the product of its minimal normal subgroups). In fact, we can say much more. The main result is the *O'Nan-Scott theorem* (see [**38**, Chapter 4], for example), which describes the structure and action of a primitive group in terms of its socle. This is a very powerful tool for studying primitive groups. Indeed, in many situations it can be used to reduce a general problem to a much more specific problem concerning almost simple groups, at which point one can appeal to the *Classification of Finite Simple Groups* (CFSG) and the vast literature on simple groups and their subgroups, conjugacy classes and representations. (Recall that a finite group G is *almost simple* if $\mathrm{soc}(G) = G_0$ is a nonabelian simple group, so $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.)

In view of these observations, in this article we will focus our attention on fixed point ratios for almost simple primitive permutation groups.

2.2. Minimal degree. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group of degree n. Recall that

$$\mu(G) = \min_{1 \neq x \in G}(n - |C_{\Omega}(x)|) = n\left(1 - \max_{1 \neq x \in G} \mathrm{fpr}(x)\right)$$

is the *minimal degree* of G. This invariant has been studied since the 19th century. In particular, a classical problem is to find lower bounds on $\mu(G)$ in terms of n, assuming $G \neq \mathrm{Alt}(n), \mathrm{Sym}(n)$, which is equivalent to finding upper bounds on $\max_{1 \neq x \in G} \mathrm{fpr}(x)$. We record some results:

- Jordan [**62**], 1871: $\mu(G)$ tends to infinity as n tends to infinity. In particular, there are only finitely many primitive groups with a given minimal degree bigger than 3.
- Bochert [**12**], 1892: $\mu(G) \geqslant n/4 - 1$ if G is 2-transitive.
- Babai [**7, 8**], 1981/2: $\mu(G) \geqslant (\sqrt{n} - 1)/2$ (independent of CFSG).
- Liebeck & Saxl [**75**], 1991: $\mu(G) \geqslant 2(\sqrt{n} - 1)$ (using CFSG).

Remark 2.2. The bounds obtained by Babai and Liebeck & Saxl are essentially best possible. To see this, consider the primitive *product action* of $G = \mathrm{Sym}(m) \wr \mathrm{Sym}(2)$ on $n = m^2$ points (with $m \geqslant 3$), so

$$(\gamma_1, \gamma_2)^{(x_1,x_2)\pi} = \begin{cases} ((\gamma_1)^{x_1}, (\gamma_2)^{x_2}) & \text{if } \pi = 1 \\ ((\gamma_2)^{x_2}, (\gamma_1)^{x_1}) & \text{if } \pi = (1,2) \end{cases}$$

for all $\gamma_1, \gamma_2 \in \{1, \ldots, m\}$ and $(x_1, x_2)\pi \in G$. One checks that every non-identity element $x \in G$ moves at least $2m$ points, with equality if and only if x is of the form $(y, 1)$ or $(1, y)$ in the base group $\mathrm{Sym}(m)^2$, where y is a transposition. Therefore $\mu(G) = 2\sqrt{n}$.

The following theorem of Guralnick and Magaard is a simplified version of [**52**, Theorem 1]; it is the best known result on the minimal degree of primitive groups.

Theorem 2.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group of degree n with $\mu(G) < n/2$. Then one of the following holds:*

(i) $G = \mathrm{Sym}(n)$ *or* $\mathrm{Alt}(n)$*;*

(ii) $G \leqslant L \wr \mathrm{Sym}(r)$ *acts with its product action on $\Omega = \Gamma^r$ for some $r \geqslant 1$, where $L \leqslant \mathrm{Sym}(\Gamma)$ is an almost simple primitive group with socle L_0 and either*

  (a) $L_0 = \mathrm{Alt}(m)$ *and Γ is the set of k-element subsets of* $\{1, \ldots, m\}$ *for some $k \geqslant 1$; or*

  (b) $L_0 = \Omega_m^{\epsilon}(2)$ *is an orthogonal group over $\mathbb{F}_2$ and Γ is a set of 1-dimensional subspaces of the natural L_0-module.*

By carefully analysing the cases arising in (b), Guralnick and Magaard establish the following striking corollary (see [**52**, Corollary 1]).

Corollary 2.4. *Let G be a finite primitive group and assume that the socle of G is not a product of alternating groups. Then*

$$\max_{1 \neq x \in G} \mathrm{fpr}(x) \leqslant \frac{4}{7}.$$

Remark 2.5.

(i) The upper bound in Corollary 2.4 is best possible. For example, suppose

$$G = \mathrm{O}_7(2) \cong \mathrm{Sp}_6(2), \;\; H = G_\alpha = \mathrm{O}_6^-(2)$$

and $x \in G$ is a transvection (in other words, x is an involution with Jordan form $[J_2, J_1^4]$ on the natural module for $\mathrm{Sp}_6(2)$, where J_i denotes a standard unipotent Jordan block of size i). All the transvections in H (and also in G) are conjugate, so

$$|x^G \cap H| = |x^H| = \frac{|\mathrm{O}_6^-(2)|}{2|\mathrm{Sp}_4(2)|} = 36, \;\; |x^G| = \frac{|\mathrm{Sp}_6(2)|}{2^5|\mathrm{Sp}_4(2)|} = 63$$

and thus $\mathrm{fpr}(x) = 36/63 = 4/7$ (the respective centraliser orders can be read off from [**6**, Sections 7 and 8], noting that x is a b_1-type involution in both H and G).

(ii) Note that the conclusion is false if we allow groups whose socle is a product of alternating groups. For instance, in Example 1.3 we observed that

$$\lim_{n\to\infty}\left(\max_{1\neq x\in G}\mathrm{fpr}(x)\right) = 1$$

for the action of $G = \mathrm{Sym}(n)$ on 2-sets.

We refer the reader to [**66**] for results on the minimal degree of arbitrary finite permutation groups and some interesting applications to quantum computing.

2.3. Fixed point ratios for simple groups. In this section we discuss fixed point ratios for almost simple groups of Lie type. With a view towards applications, we are primarily interested in obtaining upper bounds, so it is natural to focus on primitive actions and prime order elements.

We start by recalling a theorem of Liebeck and Saxl [**75**, Theorem 1], which is the most general result in this area.

Theorem 2.6. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive almost simple group of Lie type over $\mathbb{F}_q$ with socle G_0 and point stabiliser H. Assume $G_0 \neq \mathrm{PSL}_2(q)$. Then either*

$$\max_{1\neq x\in G}\mathrm{fpr}(x) \leqslant \frac{4}{3q} \tag{2.1}$$

or $G_0 \in \{\mathrm{PSL}_4(2), \mathrm{PSp}_4(3), \mathrm{P}\Omega_4^-(3)\}$.

Remark 2.7.

(i) This is a simplified version of [**75**, Theorem 1], which includes the case $G_0 = \mathrm{PSL}_2(q)$ and gives a precise description of the triples (G, H, x) with $\mathrm{fpr}(x) > 4/3q$.

(ii) The upper bound is essentially best possible. For instance, in Example 1.5 ($G = \mathrm{PGL}_n(q)$ on 1-spaces) we observed that there are elements $x \in G$ with $\mathrm{fpr}(x) \sim 1/q$.

(iii) Consider the special case $G_0 = \mathrm{PSL}_4(2) \cong \mathrm{Alt}(8)$ appearing in the statement of the theorem. If $G = G_0.2 = \mathrm{Sym}(8)$, $|\Omega| = 8$ and $x = (1,2)$, then $\mathrm{fpr}(x) = 6/8 > 4/6$.

The proof of Theorem 2.6 proceeds by induction, with the ultimate goal of eliminating the existence of a minimal counterexample (minimal with respect to the order of the group). The details of the argument are somewhat complicated by the fact that there are a small number of groups for which the bound in (2.1) is false. To give a flavour of the main ideas, we provide a brief sketch to show that (2.1) holds when $G = \mathrm{PSL}_n(q)$ with $n \geqslant 6$. Below we use the notation P_m for the stabiliser in G of an m-dimensional subspace of the natural module V for G.

Sketch proof of Theorem 2.6 ($G = \mathrm{PSL}_n(q)$, $n \geqslant 6$). Suppose $\mathrm{fpr}(x) > 4/3q$ for some $1 \neq x \in G$. Set $H = G_\alpha$ and write $x = \hat{x}Z$, where $\hat{x} \in \mathrm{SL}_n(q)$ and $Z = Z(\mathrm{SL}_n(q))$. In view of Lemma 1.2, we may assume that H is maximal (so G is primitive) and x has prime order r, so x is either semisimple (if $r \neq p$) or unipotent (if $r = p$), where p is the characteristic of $\mathbb{F}_q$. Replacing x by a suitable conjugate, if necessary, we may assume that $x \in H$. Note that

$$|\Omega| < \frac{3q|C_G(x)|}{4} \tag{2.2}$$

by Lemma 1.2(iii).

Our first goal is to reduce to the case where x stabilises a nontrivial decomposition $V = V_1 \oplus V_2$. Suppose otherwise.

If x is semisimple then it acts irreducibly on V and we deduce that $|C_G(x)| \leqslant (q^n-1)/(q-1)$. In view of (2.2), this implies that $H = P_1$ (the smallest permutation representation of G has degree $(q^n-1)/(q-1)$), which means that x fixes a 1-space. This is incompatible with the irreducibility of x. Similarly, if x is unipotent then it must be regular (i.e. it has Jordan form $[J_n]$ on V) and by considering $|C_G(x)|$ we again deduce that $H = P_1$. But a regular unipotent element fixes a unique 1-dimensional subspace of V, so $|C_\Omega(x)| = 1$ and once again we have reached a contradiction.

Let $V = V_1 \oplus V_2$ be a nontrivial decomposition fixed by x with $1 \leqslant a_1 \leqslant a_2$, where $a_i = \dim V_i$. Assume a_1 is minimal. We claim that $a_1 \leqslant 2$.

Suppose $a_1 \geqslant 3$. Set $A_i = \mathrm{SL}_{a_i}(q)$, $B_i = \mathrm{GL}_{a_i}(q)$ and write $\hat{x} = (\hat{x}_1, \hat{x}_2) \in B_1 \times B_2$. Let

$$X = \langle A_1 \times A_2, \hat{x} \rangle \leqslant \mathrm{SL}_n(q).$$

Let x_i be the automorphism of the simple group $A_i/Z(A_i)$ induced by $\hat{x}_i$. The minimality of a_1 implies that neither $\hat{x}_1$ nor $\hat{x}_2$ is a scalar, so each x_i is nontrivial.

The key step in the proof is to study the orbits $\Omega_1, \ldots, \Omega_k$ of X on Ω, together with the action of A_1 and A_2 on each orbit. The case where $H = P_{a_1}$ can be handled directly, so assume otherwise. For convenience, let us also assume that neither $A_1/Z(A_1)$ nor $A_2/Z(A_2)$ are exceptions to the statement of the main theorem. Then using induction and a technical lemma [**75**, Lemma 2.8] one can show that $|C_{\Omega_j}(x)| \leqslant 4|\Omega_j|/3q$ for each j, which implies that $\mathrm{fpr}(x) \leqslant 4/3q$, a contradiction.

We now have $a_1 \leqslant 2$ and $a_2 \geqslant 4$ since $n \geqslant 6$. By considering the orbits of A_2 on Ω and applying induction, one can reduce to the case where $A_2 \leqslant H$. From here it follows that $H = P_1$ or P_2 (using work of Kantor [**64**], given the fact that H contains long root elements of G), and it is not too difficult to eliminate these two possibilities. □

Theorem 2.6 plays a central role in the proof of [**75**, Theorem 2], which yields the aforementioned lower bound $\mu(G) \geqslant 2(\sqrt{n}-1)$ on the minimal degree of a primitive group G of degree n that does not contain $\mathrm{Alt}(n)$. To derive this bound, it suffices to show that $\mu(G) \geqslant n/3$ unless G satisfies the conditions in part (ii)(a) of Theorem 2.3. We briefly sketch the argument.

Consider a counterexample $G \leqslant \mathrm{Sym}(\Omega)$ of minimal order, with point stabiliser H. Fix $x \in H$ of prime order such that $\mathrm{fpr}(x) > 2/3$. By applying the O'Nan-Scott theorem, we can reduce to the case where G is almost simple. For example, if G is either an affine group or a twisted wreath product, then $N = \mathrm{soc}(G)$ is regular (that is, $H \cap N = 1$), so

$$|C_\Omega(x)| = |C_N(x)| \leqslant \frac{|N|}{2} = \frac{n}{2}$$

and thus $\mathrm{fpr}(x) \leqslant 1/2$, a contradiction.

Now assume G is almost simple with socle G_0. If G_0 is a simple group of Lie type over $\mathbb{F}_q$ then Theorem 2.6 immediately gives $\mu(G) > n/2$ if $q > 2$, and $\mu(G) \geqslant n/3$ if $q = 2$. If G_0 is a sporadic group and $\mu(G) > n/2$ then Lemma 1.2(iv) implies that

$$1 + |\chi(x)| \geqslant \frac{1+\chi(1)}{2}$$

for some non-linear character $\chi \in \mathrm{Irr}(G)$. By inspecting the relevant character tables in the Atlas [**34**], one checks that no such character exists.

Finally, suppose $G_0 = \mathrm{Alt}(m)$ is an alternating group and consider the action of H on $\Gamma = \{1, \ldots, m\}$. The situation where H is intransitive or imprimitive on Γ can be handled directly, working with a concrete description of the action of G on subsets or partitions. Suppose H is primitive. The minimality of $|G|$ implies that $\mu(H) \geqslant m/3$ with respect to the action of H on Γ. This immediately translates into a lower bound of the form $|x^G| \geqslant f(m)$ for some function f and thus $|H| > \frac{2}{3}f(m)$ since $\mathrm{fpr}(x) > 2/3$. But H is a primitive group of degree m, so $|H| < g(m)$ for some function g (for instance, we can take $g(m) = 4^m$ by a theorem of Praeger and Saxl [**91**]). Together, these bounds imply that $m \leqslant 750$ and by inspecting lists of small degree primitive groups one can reduce this to $m \leqslant 24$. The remaining possibilities can be eliminated one-by-one.

2.4. Classical groups. As observed in Remark 2.7, the upper bound in Theorem 2.6 is essentially best possible. However, it would be desirable to have bounds on $\mathrm{fpr}(x)$ that depend on the element x in some way. We might also try to establish stronger bounds, at the expense of excluding some specific actions. In this section we report on recent work in this direction for almost simple classical groups.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive classical group over $\mathbb{F}_q$ with socle G_0 and point stabiliser H. Let V be the natural module for G_0 and set $n = \dim V$. Write $q = p^f$ with p prime. The possibilities for G_0 are recorded in Table 2.1. Note that we may assume the given conditions on n and q due to several exceptional isomorphisms among the low-dimensional classical groups (see [**68**, Proposition 2.9.1] for example).

Type	Notation	Conditions
Linear	$\mathrm{PSL}_n(q)$	$n \geqslant 2,\ (n,q) \neq (2,2),(2,3)$
Unitary	$\mathrm{PSU}_n(q)$	$n \geqslant 3,\ (n,q) \neq (3,2)$
Symplectic	$\mathrm{PSp}_n(q)'$	$n \geqslant 4$ even
Orthogonal	$\Omega_n(q)$	nq odd, $n \geqslant 7$
	$\mathrm{P}\Omega_n^{\pm}(q)$	$n \geqslant 8$ even

TABLE 2.1. The finite simple classical groups

Since G is primitive, H is a maximal subgroup of G with $G = G_0H$. The possibilities for H are described by a fundamental theorem of Aschbacher. In [**2**], Aschbacher introduces eight *geometric* families of subgroups of G, denoted by $\mathcal{C}_1, \ldots, \mathcal{C}_8$, which are defined in terms of the underlying geometry of V. For example, these collections include the stabilisers of certain types of subspaces of V, and the stabilisers of appropriate direct sum and tensor product decompositions. Roughly speaking, Aschbacher's main theorem implies that H is either contained in one of the $\mathcal{C}_i$ collections, or H is almost simple and the socle of H acts absolutely irreducibly on V. Following [**68**], we use $\mathcal{S}$ to denote the latter collection of *non-geometric* subgroups. In turn, we write $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$ where a subgroup $H \in \mathcal{S}$ is in $\mathcal{S}_1$ if its socle is a group of Lie type in the defining characteristic p. A brief description of these subgroup collections is presented in Table 2.2.

Some further conditions are imposed on the subgroups in $\mathcal{S}$ to avoid containment in a geometric subgroup collection. For instance, suppose $G_0 = \mathrm{PSL}_n(q)$ and $H \in \mathcal{S}$ has socle H_0. Let

$$\rho : \widehat{H}_0 \to \mathrm{GL}(V)$$

be the corresponding absolutely irreducible representation (where $\widehat{H}_0$ is the full covering group of H_0). Then $\rho(\widehat{H}_0)$ does not fix a non-degenerate form on V and the representation cannot be realised over a proper subfield of $\mathbb{F}_q$ (see [**68**, p.3] for a complete list of the conditions satisfied by $\rho(\widehat{H}_0)$).

It turns out that a small additional subgroup collection (denoted by $\mathcal{N}$) arises when $G_0 = \mathrm{PSp}_4(q)'$ (with q even) or $\mathrm{P}\Omega_8^+(q)$, due to the existence of certain exceptional automorphisms (the maximal subgroups in the latter case have been determined by Kleidman [**67**]).

The definitive reference for information on the structure, maximality and conjugacy of the geometric subgroups is the book by Kleidman and Liebeck

$\mathcal{C}_1$	Stabilisers of subspaces, or pairs of subspaces, of V
$\mathcal{C}_2$	Stabilisers of decompositions $V = \bigoplus_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathcal{C}_3$	Stabilisers of prime degree extension fields of $\mathbb{F}_q$
$\mathcal{C}_4$	Stabilisers of decompositions $V = V_1 \otimes V_2$
$\mathcal{C}_5$	Stabilisers of prime index subfields of $\mathbb{F}_q$
$\mathcal{C}_6$	Normalisers of symplectic-type r-groups, $r \neq p$
$\mathcal{C}_7$	Stabilisers of decompositions $V = \bigotimes_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathcal{C}_8$	Stabilisers of nondegenerate forms on V
$\mathcal{S}$	Almost simple absolutely irreducible subgroups
$\mathcal{N}$	Novelty subgroups ($G_0 = \mathrm{P}\Omega_8^+(q)$ or $\mathrm{PSp}_4(q)'$ ($p = 2$), only)

Table 2.2. Aschbacher's subgroup collections

[**68**]. More recently, the maximal subgroups of the low-dimensional classical groups with $n \leqslant 12$ have been completely determined by Bray, Holt and Roney-Dougal in [**14**].

Example 2.8. If $G_0 = \mathrm{PSL}_6(q)$ then the subgroups comprising the geometric $\mathcal{C}_i$ collections are described below (note that the $\mathcal{C}_6$ and $\mathcal{C}_7$ collections are empty). Here we refer to the *type* of a subgroup H, which provides an approximate description of the group-theoretic structure of H (the precise structure is presented in [**14, 68**]).

$\mathcal{C}_1$: Parabolic subgroups P_m with $m \in \{1,2,3,4,5\}$, where $P_m = G_U$ for an m-dimensional subspace U of V.

In addition, if G contains a graph (or graph-field) automorphism τ of G_0 then $\mathcal{C}_1$ also includes the stabilisers of the form $G_{U,W}$, where U, W are non-zero subspaces of V with $6 = \dim U + \dim W$ and either $U \subset W$ or $V = U \oplus W$. (Note that if $G = \langle G_0, \tau \rangle$ and $m \neq 3$ then $P_m < G_0 < G$ since $\dim U^{\tau} = 6 - m$.)

$\mathcal{C}_2$: Stabilisers of direct sum decompositions of the form $V = V_1 \oplus V_2$ or $V = U_1 \oplus U_2 \oplus U_3$, where $\dim V_i = 3$ and $\dim U_i = 2$. These subgroups are of type $\mathrm{GL}_3(q) \wr \mathrm{Sym}(2)$ and $\mathrm{GL}_2(q) \wr \mathrm{Sym}(3)$, respectively.

$\mathcal{C}_3$: Field extension subgroups of type $\mathrm{GL}_3(q^2)$ and $\mathrm{GL}_2(q^3)$.

$\mathcal{C}_4$: Tensor product subgroups of type $\mathrm{GL}_3(q) \otimes \mathrm{GL}_2(q)$.

$\mathcal{C}_5$: Subfield subgroups of type $\mathrm{GL}_6(q_0)$, where $q = q_0^k$ for some prime k.

$\mathcal{C}_8$: Classical subgroups of type $\mathrm{Sp}_6(q)$ and $\mathrm{O}_6^{\pm}(q)$ (with q odd in the latter case), and also type $\mathrm{GU}_6(q_0)$ if $q = q_0^2$.

In addition, the possible socles of the subgroups in $\mathcal{S}$ are as follows (see [**14**, Table 8.25]):

$$\mathrm{Alt}(6),\ \mathrm{Alt}(7),\ \mathrm{PSL}_2(11),\ \mathrm{M}_{12},\ \mathrm{PSL}_3(4),\ \mathrm{PSU}_4(3),\ \mathrm{PSL}_3(q).$$

Note that the latter subgroup arises from the symmetric-square representation $S^2(W)$ of $\mathrm{SL}_3(q)$, where W is the natural module for $\mathrm{SL}_3(q)$.

When studying fixed point ratios for classical groups, it is natural to distinguish between those actions which permute subspaces of the natural module and those which do not. This leads us naturally to the following definition.

Definition 2.9. Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive classical group over $\mathbb{F}_q$ with socle G_0, natural module V and point stabiliser H. The action of G on Ω is a *subspace action* if one of the following holds for each maximal subgroup M of G_0 containing $H \cap G_0$:

(i) M is the stabiliser in G_0 of a proper non-zero subspace U of V, where U is totally singular, non-degenerate or, if G_0 is orthogonal and q is even, a non-singular 1-space (U can be any subspace if $G_0 = \mathrm{PSL}_n(q)$).

(ii) $M = \mathrm{O}_n^{\pm}(q)$ if $G_0 = \mathrm{Sp}_n(q)$ and q is even.

Example 2.10. If $G_0 = \mathrm{PSp}_6(q)$ then the subspace actions correspond to the following maximal subgroups H of G:

$\mathcal{C}_1$: $H = P_m = G_U$ is a maximal parabolic subgroup, where U is a totally singular m-space and $m \in \{1,2,3\}$.

$\mathcal{C}_1$: $H = G_W$ is of type $\mathrm{Sp}_4(q) \times \mathrm{Sp}_2(q)$, where W is a non-degenerate 2-space.

$\mathcal{C}_8$: H is of type $\mathrm{O}_6^+(q)$ or $\mathrm{O}_6^-(q)$, and q is even.

Note that a subgroup H of the latter type is the stabiliser of a non-degenerate quadratic form on V. However, if we consider the isomorphism $\mathrm{Sp}_6(q) \cong \mathrm{O}_7(q)$ (where $\mathrm{O}_7(q)$ is the isometry group of a non-singular quadratic form on a 7-dimensional space over $\mathbb{F}_q$), then H corresponds to the stabiliser of an appropriate non-degenerate 6-space. This explains why we include these subgroups in Definition 2.9.

In general, notice that subspace actions correspond to maximal subgroups in the collection $\mathcal{C}_1$ (in addition to the special $\mathcal{C}_8$-subgroups that arise when G is a symplectic group in even characteristic).

As previously remarked, it is sensible to make a distinction between subspace and non-subspace actions when studying fixed point ratios for classical groups. In general, the stabilisers for subspace actions tend to be large subgroups, such as maximal parabolic subgroups, so it is natural to expect that $\mathrm{fpr}(x) = |x^G \cap H|/|x^G|$ will also be large in this situation. For example, we demonstrated the sharpness of Theorem 2.6 by considering the action of $\mathrm{PGL}_n(q)$ on 1-spaces. Therefore, it is reasonable to expect that better bounds can be established if we exclude subspace actions. In addition, we have a very concrete description of subspace actions, which may permit direct calculation, so it also makes sense to treat them separately from this point of view.

2.5. Subspace actions of classical groups.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ in a subspace action with socle G_0 and natural module V. Fix an element $x \in G \cap \mathrm{PGL}(V)$ and write $x = \hat{x}Z$, where $\hat{x} \in \mathrm{GL}(V)$ and Z denotes the centre of $\mathrm{GL}(V)$. Since we can identify Ω with a collection of subspaces (or pairs of subspaces) of V, it is natural to expect that $\mathrm{fpr}(x)$ will reflect certain properties of the action of x on V. For instance, in Example 1.4 we observed that $\mathrm{fpr}(x) = q^{d-n}$ for the natural action of $\mathrm{GL}_n(q)$ on $V = \mathbb{F}_q^n$, where $d = \dim C_V(x)$ is the dimension of the 1-eigenspace of x on V. To formalise this, we introduce the following notation (recall that if $y \in \mathrm{GL}(W)$, then $[W, y]$ is the subspace of W spanned by the vectors of the form $w - wy$, for $w \in W$).

Definition 2.11. For $x \in \mathrm{PGL}(V)$, let $\hat{x}$ be a pre-image of x in $\mathrm{GL}(V)$ and define

$$\nu(x) = \min\{\dim[\bar{V}, \lambda\hat{x}] \,:\, \lambda \in K^{\times}\},$$

where $\bar{V} = V \otimes K$ and K is the algebraic closure of $\mathbb{F}_q$. Note that $\nu(x)$ is equal to the codimension of the largest eigenspace of $\hat{x}$ on $\bar{V}$.

Example 2.12. Consider the action of $G = \mathrm{PSp}_n(q)$ on the set Ω of 2-dimensional non-degenerate subspaces of V. Assume q is odd and set $x = \hat{x}Z$, where $\hat{x} = [-I_m, I_{n-m}]$ and $0 < m < n/2$ with respect to an appropriate symplectic basis of V. The eigenspaces U and W of $\hat{x}$ are non-degenerate, so $m = \dim U = \nu(x)$ is even and x stabilises the orthogonal decomposition $V = U \perp W$. Since G acts transitively on Ω we have

$$|\Omega| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_2(q)||\mathrm{Sp}_{n-2}(q)|} \sim q^{2(n-2)}.$$

Clearly, x fixes a non-degenerate 2-space if and only if it is contained in either U or W, so

$$\begin{aligned}|C_\Omega(x)| = \frac{|\mathrm{Sp}_m(q)|}{|\mathrm{Sp}_2(q)||\mathrm{Sp}_{m-2}(q)|} + \frac{|\mathrm{Sp}_{n-m}(q)|}{|\mathrm{Sp}_2(q)||\mathrm{Sp}_{n-m-2}(q)|} &\sim q^{2(m-2)} + q^{2(n-m-2)} \\ &\sim q^{2(n-m-2)}\end{aligned}$$

and thus $\mathrm{fpr}(x) \sim q^{-2m} = q^{-2\nu(x)}$.

The most general result for subspace actions is the following theorem of Frohardt and Magaard [**44**], which shows that the previous example is typical for all subspace actions.

Theorem 2.13. *Fix $\epsilon > 0$ and let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ with natural module V, where Ω is an appropriate set of k-subspaces of V. Then there exists an integer $N = N(q, \epsilon)$ such that if $\dim V \geqslant N$ then*

$$\mathrm{fpr}(x) < q^{-\nu(x)k} + \epsilon$$

for all $1 \neq x \in G \cap \mathrm{PGL}(V)$.

This is a somewhat simplified version of their main result. Indeed, [**44**] provides a suitably modified version of the theorem that holds for all non-identity elements in G, together with explicit upper and lower bounds on $\mathrm{fpr}(x)$. For instance, [**44**, Theorem 1] states that if $G_0 = \mathrm{PSL}_n(q)$, $n \geqslant 5$ and Ω is the set of k-dimensional subspaces of V, then either

(a) $\mathrm{fpr}(x) \leqslant 9q^{-(n-1)/2}$, or

(b) $x \in G \cap \mathrm{PGL}(V)$, $\nu(x) \leqslant n/2k$ and

$$q^{-\nu(x)k} - q^{-n} \leqslant \mathrm{fpr}(x) \leqslant q^{-\nu(x)k} + 11q^{-n/2}.$$

We also refer the reader to [**51**, Section 3] for some alternative upper bounds on $\max_{1\neq x\in G}\mathrm{fpr}(x)$ for subspace actions (this work of Guralnick and Kantor was motivated by very different applications, which we will discuss in Section 3).

2.6. Non-subspace actions of classical groups. Now let us turn to the non-subspace actions of classical groups. Here it is natural to distinguish between geometric and non-geometric actions. For geometric actions, we have a rather concrete description of the embedding of $H = G_\alpha$ in G, which permits a detailed analysis of the conjugacy classes in H and, more importantly, their fusion in G. In this way, it is possible to compute accurate fixed point ratio estimates for geometric actions.

EXAMPLE 2.14. Suppose $G = \mathrm{PSp}_{12}(q)$ and H is a $\mathcal{C}_2$-subgroup of G of type $\mathrm{Sp}_4(q) \wr \mathrm{Sym}(3)$, so H is the stabiliser of an orthogonal decomposition $V = V_1 \perp V_2 \perp V_3$ and each V_i is a nondegenerate 4-space. Let Z denote the centre of $\mathrm{Sp}_{12}(q)$. Assume $q \equiv 1 \pmod 3$ and set $x = \hat{x}Z \in G$ where $\hat{x} = [I_6, \lambda I_3, \lambda^2 I_3]$ and $\lambda \in \mathbb{F}_q$ is a primitive cube root of unity (here we are thinking of $\hat{x}$ as a diagonal matrix, with respect to an appropriate basis). Since two semisimple elements in a symplectic group are conjugate if and only if they have the same eigenvalues (in a splitting field), we see that $x^G \cap H = x_1^H \cup x_2^H$ where $\hat{x}_1, \hat{x}_2 \in \mathrm{Sp}_4(q)^3$ are as follows:

$$\hat{x}_1 = ([I_4], [I_2, \lambda, \lambda^2], [\lambda I_2, \lambda^2 I_2]),\;\; \hat{x}_2 = ([I_2, \lambda, \lambda^2], [I_2, \lambda, \lambda^2], [I_2, \lambda, \lambda^2]).$$

Therefore

$$\begin{aligned}|x^G \cap H| &= 3! \cdot \frac{|\mathrm{Sp}_4(q)|}{|\mathrm{Sp}_2(q)||\mathrm{GL}_1(q)|} \cdot \frac{|\mathrm{Sp}_4(q)|}{|\mathrm{GL}_2(q)|} + \left(\frac{|\mathrm{Sp}_4(q)|}{|\mathrm{Sp}_2(q)||\mathrm{GL}_1(q)|}\right)^3 \\ &\sim 6q^{12} + q^{18}\end{aligned}$$

and

$$|x^G| = \frac{|\mathrm{Sp}_{12}(q)|}{|\mathrm{Sp}_6(q)||\mathrm{GL}_3(q)|} \sim q^{48},$$

so $\mathrm{fpr}(x) \sim q^{-30} \sim |x^G|^{-5/8}$ (we refer the reader to [**25**, Chapter 3] for detailed information on the centralisers of elements of prime order in finite classical groups).

We require different methods to handle the non-geometric actions of classical groups. Indeed, in general we are unable to determine the maximal subgroups $H \in \mathcal{S}$ for a given classical group G. Of course, we do not even know the dimensions of the irreducible representations of simple groups, let alone information on the embedding of H in G that might allow us to understand the fusion of the relevant conjugacy classes! However, as described below in Section 2.7, there are ways to overcome these obstacles for the purposes of estimating fixed point ratios.

A key result on non-subspace actions is the following theorem of Liebeck and Shalev [**81**], which plays a major role in several important applications. A nice feature of this result is that the upper bound depends on the size of the conjugacy class of the element.

Theorem 2.15. *There is an absolute constant $\epsilon > 0$ such that*

$$\mathrm{fpr}(x) < |x^G|^{-\epsilon}$$

for all $x \in G$ of prime order and for every primitive almost simple classical group G in a non-subspace action.

It is easy to see that this result does *not* extend to subspace actions. For example, if we consider the action of $G = \mathrm{PGL}_n(q)$ on 1-spaces and we choose $x \in G$ with $\nu(x) = 1$ then $|x^G| \sim q^{2n-2}$ but $\mathrm{fpr}(x) \sim q^{-1}$. In particular, Theorem 2.15 implies that $\mathrm{fpr}(x)$ tends to 0 as $|G|$ tends to infinity (for classical groups acting on subspaces of a fixed dimension, we only get this limiting behaviour as the field size tends to infinity).

The constant ϵ in Theorem 2.15 is undetermined and with applications in mind it is desirable to pin down an explicit estimate. The main theorem of [**19**] implies that $\epsilon \sim 1/2$ is optimal.

Theorem 2.16. *Let G be a primitive almost simple classical group in a non-subspace action with point stabiliser H and natural module of dimension n. Then*

$$\mathrm{fpr}(x) < |x^G|^{-\frac{1}{2}+\eta}$$

for all $x \in G$ of prime order, where $\eta \to 0$ as $n \to \infty$.

This is a simplified version of [**19**, Theorem 1], which is proved in the sequence of papers [**20, 21, 22**]. Indeed, one can take $-1/2 + 1/n + \delta$ for the exponent, where $\delta = 0$, or (G, H, δ) is one of a small number of known exceptions (in every case, $\delta \to 0$ as $n \to \infty$). The next example shows that there is not much room for improvement in this exponent.

Example 2.17. Suppose $G = \mathrm{PSL}_n(q)$ and H is a $\mathcal{C}_8$-subgroup of type $\mathrm{O}_n^+(q)$, so n is even and q is odd. Let $x \in G$ be an involution such that $\hat{x} = [-I_m, I_{n-m}]$ with m even. Then

$$|x^G \cap H| = \frac{|\mathrm{O}_n^+(q)|}{|\mathrm{O}_m^+(q)||\mathrm{O}_{n-m}^+(q)|} + \frac{|\mathrm{O}_n^+(q)|}{|\mathrm{O}_m^-(q)||\mathrm{O}_{n-m}^-(q)|} \sim q^{m(n-m)}$$

and

$$|x^G| = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_m(q)||\mathrm{GL}_{n-m}(q)|} \sim q^{2m(n-m)}$$

so $\mathrm{fpr}(x) \sim q^{-m(n-m)} \sim |x^G|^{-1/2}$.

There are many other examples that demonstrate the accuracy of the bound in Theorem 2.16. For instance, if $q = q_0^2$ and H is a subfield subgroup of G defined over $\mathbb{F}_{q_0}$ then $|x^G \cap H| \sim |x^G|^{1/2}$ for all $x \in G$ with fixed points, so $\mathrm{fpr}(x) \sim |x^G|^{-1/2}$.

The proof of Theorem 2.16 is given in [**20, 21, 22**]. To handle the relevant geometric actions we combine detailed information on the structure of the maximal geometric subgroups in [**68**] (which is organised according to the subgroup collections arising in Aschbacher's theorem) with a careful analysis of the conjugacy classes and fusion of elements of prime order.

A different approach is needed to deal with the non-geometric actions corresponding to the maximal subgroups in the collection $\mathcal{S}$. We will briefly describe the main ingredients in the next section.

2.7. $\mathcal{S}$-actions of classical groups. Let G, H and n be given as in the statement of Theorem 2.16. Let G_0 be the socle of G, which is a simple classical group over $\mathbb{F}_q$ (for $q = p^f$, p prime) with natural module V of dimension n. Assume $H \in \mathcal{S}$ has socle H_0 and let $\rho : \widehat{H}_0 \to \mathrm{GL}(V)$ be the corresponding absolutely irreducible representation.

If n is small, say $n \leqslant 5$, then the possibilities for (G, H, ρ) are well known (see [**14**]) and it is straightforward to work directly with the representation ρ (and its Brauer character) to obtain sufficient information on the fusion of H-classes in G to compute (or accurately estimate) fixed point ratios.

Now assume $n \geqslant 6$. Let us write $H \in \mathcal{A}$ if $q = p$, $H_0 = \mathrm{Alt}(m)$ is an alternating group and V is the fully deleted permutation module for H_0 over $\mathbb{F}_q$ (in which case $n = m - 2$ or $m - 1$). We can now state the following result, which combines the main theorem of [**73**] with [**54**, Theorem 7.1].

Theorem 2.18. *Let G be a primitive almost simple classical group over $\mathbb{F}_q$ with socle G_0, point stabiliser $H \in \mathcal{S} \setminus \mathcal{A}$ and natural module V of dimension $n \geqslant 6$. Let $\rho : \widehat{H}_0 \to \mathrm{GL}(V)$ be the corresponding representation. Then the following hold:*

(i) *$|H| < q^{3n\alpha}$, where $\alpha = 2$ if G_0 is unitary, otherwise $\alpha = 1$;*

(ii) *Either $\nu(x) > \max\{2, \sqrt{n}/2\}$ for all $1 \neq x \in H \cap \mathrm{PGL}(V)$, or $n \leqslant 10$ and (G, H, ρ) belongs to a short list of known exceptions.*

Remark 2.19.

(a) The bound in part (i) of the theorem can be sharpened, at the expense of some additional (known) exceptions. For instance, see [**73**, Theorem 4.2] and [**27**, Theorem 2.10] for improvements with $q^{3n\alpha}$ replaced by $q^{(2n+4)\alpha}$ and q^{2n+4}, respectively (for example, the case $(G, H) = (\mathrm{PSL}_{27}(q), E_6(q))$ is an exception to the bound $|H| < q^{2n+4}$).

(b) We can view the bound in (ii) as a linear analogue of the aforementioned bounds of Babai, Liebeck and Saxl on the minimal degree of a primitive permutation group (with irreducibility in place of primitivity); see Section 2.2.

(c) The bound in (ii) is close to best possible if we impose the condition that the only exceptions occur in small dimensions. To see this, suppose $n = m^2$ where $m \geqslant 3$ is odd. If q is chosen appropriately then $G = \mathrm{PSL}_n(q)$ has a maximal subgroup $H \in \mathcal{S}$ with socle $H_0 = \mathrm{PSL}_m(q^2)$, which is embedded in G via the module $W \otimes W^{(q)}$ for $\widehat{H}_0 = \mathrm{SL}_m(q^2)$, where W is the natural module for H_0 and $W^{(q)}$ is the q-power Frobenius twist of W. If we take $x = [-I_{m-1}, I_1] \in H_0$ then it is easy to check that $\nu(x) = 2m - 2 < 2\sqrt{n}$.

The proof of Theorem 2.15 also uses the bound in part (i) of Theorem 2.18, but the bound in (ii) is a crucial new ingredient in the proof of Theorem 2.16. The cases in $\mathcal{A}$, and also the small number of low-dimensional exceptions arising in part (ii) of Theorem 2.18, are well understood embeddings and they can be handled directly.

Generically, Theorem 2.18 tells us that H is small *and* the elements in $H \cap \mathrm{PGL}(V)$ have relatively small eigenspaces on V. In particular, the latter property yields a lower bound $|x^G| \geqslant f(n,q)$ for all $x \in H \cap \mathrm{PGL}(V)$ of prime order, so we get

$$\mathrm{fpr}(x) = \frac{|x^G \cap H|}{|x^G|} < \frac{|H|}{|x^G|} < \frac{q^{3n\alpha}}{f(n,q)}. \tag{2.3}$$

Note that if $x \in H \setminus \mathrm{PGL}(V)$ has prime order then x is either a field, graph or graph-field automorphism of G_0 and it is straightforward to check that the inequality $|x^G| \geqslant f(n,q)$ still holds, so (2.3) is valid for all $x \in H$ of prime order.

EXAMPLE 2.20. Suppose $G = \mathrm{PSL}_n(q)$, $H \in \mathcal{S} \setminus \mathcal{A}$ and $n > 10$. Let $x \in H$ be an element of prime order with $\nu(x) = s$, so $s \geqslant \lceil \sqrt{n}/2 \rceil = \beta$ by Theorem 2.18(ii). It is not too difficult to show that

$$|x^G| > \frac{1}{2}q^{2\beta(n-\beta)}$$

(see [**20**, Corollary 3.38]) so we get $\mathrm{fpr}(x) < |x^G|^{-1/2}$ if

$$q^{6n} < \frac{1}{2}q^{2\beta(n-\beta)}.$$

One checks that this inequality holds if $n > 36$, so we may assume that $n \leqslant 36$. In fact, if we replace the bound in part (i) of Theorem 2.18 by $|H| < q^{2n+4}$ (at the expense of a small number of known exceptions (see [**73**, Theorem 4.2]), which can be handled separately), then we can reduce to the case where $n \leqslant 16$. At this point we can turn to results of Lübeck [**84**] (in defining characteristic) and Hiss and Malle [**59, 60**] (in non-defining characteristic) to determine the possibilities for (G, H, ρ) and we can then work directly with these cases.

2.8. Exceptional groups. Finally, let us say a few words on fixed point ratios for exceptional groups. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple exceptional group of Lie type over $\mathbb{F}_q$ with socle G_0 and point stabiliser H. Recall that Theorem 2.6 gives

$$\max_{1 \neq x \in G} \mathrm{fpr}(x) \leqslant \frac{4}{3q}$$

and it is natural to ask if this upper bound can be improved.

In [**46**], Frohardt and Magaard obtain close to best possible upper bounds in the special case where the rank of G is at most 2. For example, they prove that

$$\max_{1 \neq x \in G} \mathrm{fpr}(x) = \begin{cases} \frac{1}{q^2-q+1} & \text{if } G_0 \in \{G_2(q), {}^2G_2(q)\} \text{ and } q > 4, \\ \frac{1}{q^4-q^2+1} & \text{if } G_0 = {}^3D_4(q). \end{cases}$$

In [**71**], using different methods, Lawther, Liebeck and Seitz present a detailed analysis of fixed point ratios for all the exceptional groups. For instance, [**71**, Theorem 1] gives

$$\max_{1 \neq x \in G} \mathrm{fpr}(x) \leqslant \begin{cases} \frac{1}{q^8(q^4-1)} & \text{if } G_0 = E_8(q) \\ \frac{1}{q^6-q^3+1} & \text{if } G_0 \in \{E_7(q), {}^2E_6(q)\} \\ \frac{1}{q^4-q^2+1} & \text{if } G_0 \in \{E_6(q), F_4(q)\}, \end{cases}$$

with equality if $G_0 = E_6(q)$, ${}^2E_6(q)$ or $F_4(q)$. More detailed bounds are given in [**71**, Theorem 2], which depend not only on G, but also on the choice of H and x to some extent. For example, if $G = E_8(q)$ and H does not contain a maximal torus of G, then [**71**, Theorem 2] states that $\mathrm{fpr}(x) \leqslant q^{-48}$ for all non-identity semisimple elements $x \in G$.

As for classical groups, the proofs rely on detailed information on the subgroup structure and conjugacy classes of the finite exceptional groups. In particular, there is a fundamental reduction theorem for subgroups due to Liebeck and Seitz, which plays a similar role to Aschbacher's theorem for classical groups (see [**77**, Theorem 8], for example). We finish by highlighting two other important ingredients in [**71**].

2.8.1. *Parabolic actions.* The special case where H is a maximal parabolic subgroup is studied using tools from the character theory of finite groups of Lie type, such as the Deligne-Lusztig theory and Green functions. These sophisticated techniques can be used to obtain very precise fixed point ratio estimates.

For example, suppose $G = E_8(q)$, $H = P_8$ and $x \in G$ is unipotent (here our notation indicates that H corresponds to the 8-th node in the Dynkin diagram of G, labelled in the usual way, so the Levi factor of H is of type $E_7(q)$). Then $|\Omega| \sim q^{57}$ and one can show that the corresponding permutation character admits the decomposition

$$\begin{aligned} 1_H^G(x) &= \sum_{\phi \in \widehat{W}} n_\phi R_\phi(x) \\ &= R_{\phi_{1,0}}(x) + R_{\phi_{8,1}}(x) + R_{\phi_{35,2}}(x) + R_{\phi_{112,3}}(x) + R_{\phi_{84,4}}(x), \end{aligned}$$

where $\widehat{W} = \mathrm{Irr}(W)$ and W is the Weyl group of G. The R_ϕ are almost characters of G and the coefficients are given by $n_\phi = \langle 1_{W_P}^W, \phi \rangle$, where W_P is the corresponding parabolic subgroup of W. The restriction of the R_ϕ to unipotent elements $x \in G$ are called *Green functions*; each $R_\phi(x)$ is a polynomial in q with non-negative coefficients. Lübeck has implemented an algorithm of Lusztig to compute the relevant Green functions (modulo a sign issue for certain elements) and his calculations yield very precise estimates for $\mathrm{fpr}(x)$ (see [**71**, Section 2] for more details). For example, if $x \in G$ is a long root element then $1_H^G(x)$ can be computed precisely in this way; we get a certain monic polynomial in q of degree 45, which implies that $\mathrm{fpr}(x) \leqslant 1/q^8(q^4-1)$. This turns out to be the largest fixed point ratio for any non-identity element of G.

2.8.2. *Algebraic groups.* Results on the dimensions of fixed point spaces for primitive actions of exceptional algebraic groups also play a key role in [**71**]. In the general set up, $\bar{G}$ is a simple algebraic group over the algebraic closure $K = \bar{\mathbb{F}}_q$ and σ is a Frobenius morphism of $\bar{G}$ such that G_0 is the derived subgroup of $\bar{G}_\sigma = \{x \in \bar{G} : x^\sigma = x\}$. Let $\bar{H}$ be a σ-stable closed subgroup of $\bar{G}$ and let $\Gamma = \bar{G}/\bar{H}$ be the corresponding coset variety, which is naturally a $\bar{G}$-variety over K. Then the fixed point space $C_\Gamma(x)$ is a subvariety for each $x \in \bar{G}$, and we may compare the dimensions of Γ and $C_\Gamma(x)$. In analogy with Lemma 1.2(iii), we have

$$\dim C_\Gamma(x) - \dim \Gamma = \dim(x^{\bar{G}} \cap \bar{H}) - \dim x^{\bar{G}}$$

for all $x \in \bar{H}$ (see [**70**, Proposition 1.14]). Moreover, if we set $H = \bar{H}_\sigma$ then

$$\mathrm{fpr}(x) = \frac{|x^G \cap H|}{|x^G|} \sim q^{\dim(x^{\bar{G}} \cap \bar{H}) - \dim x^{\bar{G}}}$$

for all $x \in H$ (see [**71**, Lemma 4.5], for example). In this way, if H corresponds to a σ-stable closed subgroup of $\bar{G}$, then it is possible to use dimension bounds at the algebraic group level to study fixed point ratios for the finite group G.

This interplay between finite and algebraic groups is applied repeatedly in [**71**], using results obtained for primitive actions of exceptional algebraic groups in the companion paper [**70**]. Similar considerations also play a role in the analysis of geometric actions of finite classical groups in the proof of Theorem 2.16, using results for classical algebraic groups in [**18**].

3. Generation and random generation

In this section we discuss applications of fixed point ratios to problems concerning the generation and random generation of finite groups. In particular, we will explain how fixed point ratios play a key role in the solution to Problem A on generating graphs of simple groups stated in the introduction.

3.1. Simple groups. Recall that a group is *n-generated* if it can be generated by n elements. For instance, dihedral and symmetric groups are 2-generated, e.g. we have $\mathrm{Sym}(n) = \langle (1,2), (1,2,\ldots,n) \rangle$. The following theorem (essentially due to Steinberg [**98**]) is the starting point for the investigation of many interesting problems.

Theorem 3.1. *Every finite simple group is* 2*-generated.*

The proof relies on CFSG. The alternating groups are easy:

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

In [**98**], Steinberg presents explicit generating pairs for each simple group of Lie type. For instance, $\mathrm{PSL}_2(q) = \langle xZ, yZ \rangle$, where $Z = Z(\mathrm{SL}_2(q))$ and

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

with $\mathbb{F}_q^\times = \langle \mu \rangle$. In [**4**], Aschbacher and Guralnick complete the proof of the theorem by showing that every sporadic group is 2-generated.

Remark 3.2. By a theorem of Dalla Volta and Lucchini [**36**], every almost simple group is 3-generated (there are such groups that really need 3 generators, e.g. take $G = \mathrm{Aut}(\mathrm{PSL}_n(q))$ with nq odd and $q = p^{2f}$ with p prime).

In view of Theorem 3.1, it is natural to consider the abundance of generating pairs in a finite simple group (or a sequence of such groups), or the existence of generating pairs with special properties (such as prescribed orders). Problems of this flavour have been intensively investigated in recent years.

3.2. Random generation. Let G be a finite group, let k be a positive integer and let

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

be the probability that k randomly chosen elements generate G.

Conjecture 3.3 (Netto [**88**], 1882). *"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 our terminology, Netto is claiming that $\lim_{n\to\infty} \mathbb{P}(\mathrm{Alt}(n),2) = 1$. This remarkable conjecture was proved by Dixon [**37**] in a highly influential paper published in 1969, which relies in part on the pioneering work of Erdös and Turán in the mid-1960s 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 3.4. *Let (G_n) be any sequence of finite simple groups such that $|G_n|$ tends to infinity with n. Then* $\lim_{n\to\infty} \mathbb{P}(G_n,2) = 1$.

Dixon's conjecture was eventually proved in the 1990s. In [**65**], Kantor and Lubotzky establish the conjecture for classical groups and low rank exceptional groups, and the remaining exceptional groups were handled by Liebeck and Shalev [**78**].

In both papers, the strategy of the proof is based on an elementary observation. Let $\mathcal{M}$ be the set of maximal subgroups of G and let $x, y \in G$ be randomly chosen elements. If $G \neq \langle x,y\rangle$ then $x,y \in H$ for some $H \in \mathcal{M}$. The probability of this event is $|G:H|^{-2}$, so

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

By carefully studying $\mathcal{M}$, using recent advances in our understanding of the subgroup structure of the simple groups of Lie type (such as Aschbacher's theorem for classical groups), one shows that $Q(G) \to 0$ as $|G|$ tends to infinity, and the result follows.

Note that this probabilistic approach shows that every sufficiently large finite simple group is 2-generated, without the need to explicitly construct a pair of generators. Many interesting related results have been established in more recent years. For example, the following result is [**87**, Theorem 1.1].

Theorem 3.5. *We have $\mathbb{P}(G,2) \geqslant 53/90$ for every finite simple group G, with equality if and only if $G = \mathrm{Alt}(6)$.*

3.3. Spread. The following 2-generation property was introduced by Brenner and Wiegold [**15**] in the 1970s.

Definition 3.6. Let G be a finite group and let k be a positive integer. Then G has *spread at least 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 at least 1.

We will also be interested in the more restrictive notion of *uniform spread*, which was introduced more recently in [**16**].

Definition 3.7. We say that G has *uniform spread at least* 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.

Clearly, every cyclic group has uniform spread at least k for all $k \in \mathbb{N}$, so for the remainder of this discussion let us assume G is non-cyclic. Set

$$\begin{aligned} s(G) &= \max\{k \in \mathbb{N}_0 \, : \, G \text{ has spread at least } k\} \\ u(G) &= \max\{k \in \mathbb{N}_0 \, : \, G \text{ has uniform spread at least } k\} \end{aligned}$$

(so $u(G) = 0$ if G does not have uniform spread at least 1, etc.). Note that $u(G) \leqslant s(G) < |G| - 1$ and there are examples with $u(G) < s(G)$. For example, if $G = \mathrm{Sym}(6)$ then $u(G) = 0$ and $s(G) = 2$. Note that G is $\frac{3}{2}$-generated if and only if $s(G) \geqslant 1$.

In [**15**], Brenner and Wiegold study the spread of the simple groups $\mathrm{Alt}(n)$ and $\mathrm{PSL}_2(q)$. Among other things, they prove that $s(\mathrm{Alt}(2m)) = 4$ if $m \geqslant 4$ and $s(\mathrm{PSL}_2(q)) = q - 2$ if q is even.

The following theorem of Breuer, Guralnick and Kantor is the main result on the spread of simple groups (see [**16**, Corollary 1.3]).

Theorem 3.8. *Let G be a nonabelian finite simple group. Then $u(G) \geqslant 2$, with equality if and only if*

$$G \in \{\mathrm{Alt}(5), \mathrm{Alt}(6), \Omega_8^+(2), \mathrm{Sp}_{2m}(2)\, (m \geqslant 3)\}. \tag{3.1}$$

It turns out that $u(G) = s(G) = 2$ for each of the groups in (3.1).

Remark 3.9. The weaker bound $u(G) \geqslant 1$ was originally obtained by Stein [**97**], and independently by Guralnick and Kantor [**51**]. In the latter paper, the authors prove 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 [**16**], the constant $1/10$ is replaced by $13/42$ (for $G = \Omega_8^+(2)$, this is best possible). In fact, with the exception of a known finite list of small groups, plus the family of symplectic groups over $\mathbb{F}_2$, $1/10$ can be replaced by $2/3$ (see [**16**, Theorem 1.1]). As explained below, this result is the key ingredient in the proof of Theorem 3.8. We also note that in an earlier paper, Guralnick and Shalev proved that $u(G) \geqslant 2$ for all sufficiently large simple groups G (see [**55**, Theorem 1.2]).

Fixed point ratios play a central role in the proof of Theorem 3.8. Let us explain the connection. 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

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

Lemma 3.10. *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 $x_1,\dots,x_k \in G$ be non-identity elements and let E denote the event $E_1 \cap \cdots \cap E_k$, where E_i is the event that $G = \langle x_i, z\rangle$ for a randomly chosen conjugate $z \in y^G$. Let $\mathbb{P}(E)$ be the probability that E occurs and let $\bar{E}$ be the complementary event (and similarly for $\mathbb{P}(E_i)$ and $\bar{E}_i$). We need to show that $\mathbb{P}(E) > 0$. To see this, we note that

$$\mathbb{P}(E) = 1 - \mathbb{P}(\bar{E}) = 1 - \mathbb{P}(\bar{E}_1 \cup \cdots \cup \bar{E}_k) \geqslant 1 - \sum_{i=1}^{k} \mathbb{P}(\bar{E}_i) = 1 - \sum_{i=1}^{k} Q(x_i, y)$$

so $\mathbb{P}(E) > 1 - k \cdot \frac{1}{k} = 0$ and the result follows. □

Let $\mathcal{M}(y)$ be the set of maximal subgroups of G containing y. The following result is the main tool in the proof of Theorem 3.8.

Corollary 3.11. *Suppose there is 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 elements $x \in G$ of prime order. Then $u(G) \geqslant k$.

Proof. In view of Lemma 3.10, it suffices to show that

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

for all $1 \neq x \in G$. Fix a non-identity element $x \in G$ and let $z \in y^G$. Then $G \neq \langle x, z\rangle$ if and only if $\langle x', y\rangle \leqslant H$ for some $x' \in x^G$ and $H \in \mathcal{M}(y)$, so we have

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

where $\mathbb{P}_x(H)$ is the probability that a randomly chosen conjugate of x lies in H. Now

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

and the result follows. □

The key step in applying Corollary 3.11 is to carefully choose $y \in G$ so that it belongs to very few maximal subgroups of G, with the essential extra property that we can explicitly determine the subgroups in $\mathcal{M}(y)$, or at least a collection of maximal subgroups containing $\mathcal{M}(y)$ that is not too much bigger. This means that there is some flexibility in the approach – the optimal choice of y is not always obvious (in practice, it seems that there are many valid possibilities, but some will require more work than others).

Example 3.12. Let's use this approach to prove that $u(\mathrm{Alt}(5)) \geqslant 2$. Set $G = \mathrm{Alt}(5)$ and $y = (1,2,3,4,5) \in G$. The maximal subgroups of G are isomorphic to $\mathrm{Sym}(3)$, $\mathrm{Alt}(4)$ and D_{10}, and it is easy to see that $\mathcal{M}(y) = \{K\}$ with

$$K = \langle (1,2,3,4,5), (1,2)(3,5)\rangle = D_{10}.$$

We now compute

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G/K) = \begin{cases} 1/3 & |x| = 2 \\ 0 & |x| = 3 \\ 1/6 & |x| = 5 \end{cases}$$

and thus $u(G) \geqslant 2$ by Corollary 3.11. In fact, we have $u(G) = 2$ (see Theorem 3.8), which shows that the strictness of the inequality in Corollary 3.11 is essential. As an aside, one can check that the class of 3-cycles has the uniform spread 1 property, but not spread 2.

Example 3.13. We claim that $u(G) \geqslant 3$ if $G = \mathrm{Alt}(n)$ and $n \geqslant 8$ is even (recall the result of Brenner and Wiegold, which states that $s(G) = 4$). To see this, set $n = 2m$ and $k = m - (2, m-1)$. Fix $y \in G$ with cycle-shape $[k, n-k]$ and note that $(k, n-k) = 1$. We claim that $\mathcal{M}(y)$ consists of a single intransitive subgroup H of type $\mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$. It is clear that H is the only intransitive subgroup in $\mathcal{M}(y)$, so assume $M \in \mathcal{M}(y)$ is transitive. The cycle-shape of y implies that M is primitive, but $\langle y \rangle$ contains a k-cycle and thus $M = G$ by a classical result of Marggraf (1892), which is a contradiction (Marggraf's theorem implies that the only primitive groups of degree n containing a cycle of length $\ell < n/2$ are $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$; see [**101**, Theorem 13.5]). This justifies the claim. It remains to estimate fixed point ratios with respect to the action of G on k-sets. A straightforward combinatorial argument shows that $\mathrm{fpr}(x) < 1/3$ for all $x \in G$ of prime order (see the proof of [**16**, Proposition 6.3]) and the result follows.

Remark 3.14. The analysis of odd degree alternating groups is slightly more complicated. In this situation, no elements have precisely two cycles, so one is forced to work with n-cycles, which may belong to several maximal subgroups.

Remark 3.15. By a theorem of Guralnick and Shalev [**55**, Theorem 1.1], if $G_i = \mathrm{Alt}(n_i)$ and n_i tends to infinity with i, then $s(G_i)$ tends to infinity if and only if $p(n_i)$ tends to infinity, where $p(n_i)$ is the smallest prime divisor of n_i.

Let us also comment on the proof of Theorem 3.8 for classical groups, which require the most work. To illustrate some of the main ideas, we will assume that $G = \mathrm{PSL}_n(q)$ and $n \geqslant 13$ is odd. Following [**16**], fix a semisimple element $y \in G$ preserving a decomposition $V = U \oplus W$ of the natural module, where $\dim U = k = (n-1)/2$ and y acts irreducibly on U and W. We claim that $\mathcal{M}(y) = \{G_U, G_W\}$, which quickly implies that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) = 2 \cdot \mathrm{fpr}(x, G/G_U) < \frac{1}{3}$$

for all $x \in G$ of prime order (note that the actions of G on k-subspaces and $(n-k)$-subspaces of V are permutation isomorphic and $\mathrm{fpr}(x, G/G_U) = \mathrm{fpr}(x, G/G_W)$ for all $x \in G$). For example, if $q \geqslant 8$ then $\mathrm{fpr}(x, G/G_U) \leqslant 1/6$ by Theorem 2.6. In particular, we conclude that $u(G) \geqslant 3$.

In order to determine the subgroups in $\mathcal{M}(y)$, it is very helpful to observe that $|y|$ is divisible by a *primitive prime divisor* of $q^{n-k} - 1$ (that is, a prime r such that $n-k$ is the smallest positive integer i such that r divides $q^i - 1$;

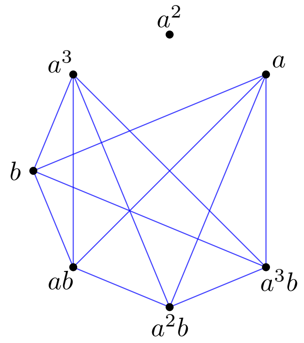

FIGURE 3.1. The generating graph of $D_8 = \langle a, b \mid a^4 = b^2 = 1,\, a^b = a^{-1}\rangle$

a classical theorem of Zsigmondy (1892) establishes the existence of such primes if $n - k \geqslant 3$ and $(n - k, q) \neq (6, 2)$). The subgroups of classical groups containing such ppd elements are studied in [**53**], where the analysis is organised according to Aschbacher's subgroup structure theorem. The main theorem of [**53**] severely limits the possible subgroups in $\mathcal{M}(y)$, and many of these possibilities can be ruled out by considering the order of y (which is roughly $(q^n - 1)/(q - 1)$ since $(k, n - k) = 1$). We refer the reader to the proof of [**16**, Proposition 5.23] for the details.

3.4. Generating graphs. The following notion first appeared in a paper by Liebeck and Shalev [**80**] on random generation.

DEFINITION 3.16. 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 $G = \langle x, y\rangle$.

This graph encodes many interesting generation properties of the group. For example,

$$\begin{aligned} G \text{ is 2-generated} &\iff \text{The edge-set of } \Gamma(G) \text{ is non-empty} \\ G \text{ has spread 1} &\iff \Gamma(G) \text{ has no isolated vertices} \\ G \text{ has spread 2} &\implies \Gamma(G) \text{ is connected with diameter at most 2} \end{aligned}$$

Moreover, the interplay between groups and graphs suggests many natural problems. For instance, what is the (co)-clique number and chromatic number of $\Gamma(G)$? Does $\Gamma(G)$ contain a Hamiltonian cycle?

In view of Theorem 3.1, it makes sense to study the generating graphs of finite simple groups. Moreover, the fact that simple groups are strongly 2-generated (in the probabilistic sense of Netto and Dixon (see Conjecture 3.4), for example, or in the sense of spread, as in Theorem 3.8) suggests that the corresponding generating graphs should have lots of edges and therefore strong connectivity properties.

EXAMPLE 3.17. If $G = \mathrm{Alt}(5)$ then $\Gamma(G)$ has 59 vertices and one checks that there are 1140 edges. It also has clique number 8, chromatic number

9 and coclique number 15 (for example, a maximal coclique is given by the set of 15 elements of order 2).

The following result summarises some of the main results on generating graphs for simple groups.

Theorem 3.18. *Let G be a nonabelian 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 3.8. Part (iii) is one of the main results in [**17**] and we briefly sketch the argument in the case where G is a group of Lie type. The three main ingredients are as follows:

(a) By the proof of Dixon's conjecture, we know that $\mathbb{P}(G,2) \to 1$ as $|G|$ tends to infinity. More precisely, a theorem of Liebeck and Shalev (see [**80**, Theorem 1.6]) states that there is a positive constant c_1 such that
$$\mathbb{P}(G,2) \geqslant 1 - \frac{c_1}{m(G)}$$
for any nonabelian finite simple group G, where $m(G)$ is the minimal index of a proper subgroup of G. Note that $G \leqslant \mathrm{Sym}(m(G))$, so $m(G)$ tends to infinity with $|G|$.

(b) Set $|G| = m+1$ (so m is odd) and let d_i be the degree of the i-th vertex of $\Gamma(G)$, where the vertices are labelled so that $d_i \leqslant d_{i+1}$ for all i. By a theorem of Fulman and Guralnick [**48**], there is a positive constant c_2 such that
$$d_1 \geqslant c_2(m+1)$$
(the constant c_2 is independent of the choice of G).

(c) *Pósa's criterion*: $\Gamma(G)$ has a Hamiltonian cycle if $d_k \geqslant k+1$ for all $k < m/2$ (see [**83**, Exercise 10.21(b)]).

If $d_i > m/2$ for all i then Pósa's criterion immediately implies that $\Gamma(G)$ has a Hamiltonian cycle, so assume otherwise. Let t be maximal such that $d_t < m/2$ and observe that
$$(m+1)^2 \cdot \mathbb{P}(G,2) = \sum_{i=1}^{m} d_i < \frac{1}{2}(m-1)t + (m-t)(m+1) < (m+1)^2 - \frac{1}{2}(m+1)t.$$
Therefore, applying (a) we get
$$1 - \frac{c_1}{m(G)} \leqslant \mathbb{P}(G,2) \leqslant 1 - \frac{t}{2(m+1)}$$
and thus
$$t \leqslant \frac{2c_1(m+1)}{m(G)} \leqslant c_2(m+1) - 1$$
if $|G|$ is sufficiently large, where c_2 is the constant in (b). It follows that if $1 \leqslant k \leqslant t$ then
$$d_k \geqslant d_1 \geqslant c_2(m+1) \geqslant t+1 \geqslant k+1.$$

Similarly, if $t+1 \leqslant k < m/2$ then $d_k \geqslant (m+1)/2 \geqslant k+1$. Therefore, Pósa's criterion is satisfied and we conclude that $\Gamma(G)$ has a Hamiltonian cycle. □

Let G be a 2-generated finite group and let N be a nontrivial normal subgroup of G. Observe that if $\Gamma(G)$ has no isolated vertices, then G/N is cyclic (indeed, if $1 \neq x \in N$ and $G = \langle x, y \rangle$ for some $y \in G$, then $G/N = \langle yN \rangle$ is cyclic). The following conjecture is a combination (and strengthening) of conjectures in [**16, 17**]:

Conjecture 3.19. *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.*

Remark 3.20. Some comments on the status of this conjecture:

(a) Note that any of the first six statements implies (vii). The following implications are also obvious:

$$\text{(i)} \iff \text{(iii)},\ \text{(ii)} \implies \text{(v)},\ \text{(vi)} \implies \text{(iv)} \implies \text{(iii)},$$
$$\text{(v)} \implies \text{(iv)} \implies \text{(iii)}$$

(b) By [**17**, Proposition 1.1], (vi) and (vii) are equivalent for soluble groups.

(c) The conjectured equivalence of (i) and (vii) is [**16**, Conjecture 1.8], and that of (vi) and (vii) is [**17**, Conjecture 1.6].

Notice that if the conjecture is true, then there is no finite group with spread 1, but not spread 2.

Let us focus on the following weaker conjecture of Breuer, Guralnick and Kantor.

Conjecture 3.21. *Let G be a finite group. Then G has spread 1 if and only if G/N is cyclic for every nontrivial normal subgroup N of G.*

As noted above, Conjecture 3.21 has been verified for soluble groups. More importantly, Guralnick has recently established the following reduction theorem.

Theorem 3.22. *It is sufficient to prove Conjecture 3.21 for almost simple groups.*

In view of this result, we focus our attention on almost simple groups G of the form $G = \langle G_0, x \rangle$, where G_0 is simple and $x \in \mathrm{Aut}(G_0)$. The goal is to prove that G has spread 1 (in fact, we aim for $s(G) \geqslant 2$). This is work in progress:

- $G_0 = \mathrm{Alt}(n)$ or sporadic: $s(G) \geqslant 2$ by results in [**16**].

- $G_0 = \mathrm{PSL}_n(q)$: $s(G) \geqslant 2$ by the main theorem of [**26**].
- $G_0 \in \{\mathrm{PSp}_n(q), \Omega_n(q)\ (nq \text{ odd})\}$: $s(G) \geqslant 2$ by work of Scott Harper (2016) in his PhD thesis (see [**58**]).

The goal is to use Corollary 3.11 to show that $u(G) \geqslant 2$. To do this, we need to find a suitable element $y \in G_0x$ so that we can determine the maximal overgroups $\mathcal{M}(y)$ and estimate

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

for all $x \in G$ of prime order (to get spread 1, recall that we need to show that this sum is less than 1). The set-up here is complicated by the fact that we have to choose y in the coset G_0x, where x is typically a field or graph automorphism of G_0. The following example illustrates some of the main ideas in the situation where x is a field automorphism.

Example 3.23 (Harper). Let $G_0 = \mathrm{Sp}_n(q)$, where $q = q_0^e$ is even, $e \geqslant 5$ and $n = 2m$ with $m \geqslant 3$ odd. Let $X = \mathrm{Sp}_n(K)$ be the ambient simple algebraic group over the algebraic closure $K = \bar{\mathbb{F}}_q$ and let $\sigma : X \to X$ be a Frobenius morphism such that $X_{\sigma^e} = G_0$. Set $H_0 = X_\sigma = \mathrm{Sp}_n(q_0) < G_0$.

Suppose $G = \langle G_0, x\rangle$, where x is the restriction of σ to G_0 (this is a field automorphism of order e). By the *Lang-Steinberg theorem* (see [**99**, Theorem 10.1]), for each sx in the coset G_0x there exists $a \in X$ such that $s = a^{-\sigma}a$. This allows us to define a map

$$f : \{G_0\text{-classes in } G_0x\} \to \{H_0\text{-classes in } H_0\} \tag{3.2}$$

by sending $(sx)^{G_0}$ to $(a(sx)^e a^{-1})^{H_0}$. One checks that f is well-defined and bijective (this map is sometimes called the *Shintani correspondence*). One can also show that f has nice fixed point properties for suitable actions of G and H_0 (see [**26**, Theorem 2.14], for example).

The strategy is to choose an element $z \in H_0$ so that the maximal overgroups of z in H_0 are somewhat restricted; hopefully this will allow us to control the maximal subgroups of G containing a representative $y \in G_0x$ of the corresponding G_0-class in the coset G_0x. To do this, we take a semisimple element of the form $z = [A, B] \in H_0$, where $A \in \mathrm{Sp}_2(q_0)$ and $B \in \mathrm{Sp}_{n-2}(q_0)$ are irreducible (so z preserves an orthogonal decomposition $V_0 = U \perp W$ of the natural module V_0 for H_0, with $\dim U = 2$). Fix an element $y \in G_0x$ such that $f(y^{G_0}) = z^{H_0}$.

We need to determine the maximal subgroups of G containing y. To do this, it is helpful to observe that $(|A|, |B|) = 1$ so $\nu(y^\ell) = 2$ for some positive integer ℓ. This quickly rules out maximal subgroups in the collections $\mathcal{C}_3$, $\mathcal{C}_4$ and $\mathcal{C}_7$, and [**54**, Theorem 7.1] (cf. Theorem 2.18) can be used to further restrict the possibilities for H. By exploiting some additional properties of the bijection in (3.2) one can show that there is a unique reducible subgroup in $\mathcal{M}(y)$ (of type $\mathrm{Sp}_2(q) \times \mathrm{Sp}_{n-2}(q)$) and also a unique $\mathcal{C}_8$-subgroup of type $\mathrm{O}_n^{\pm}(q)$.

By carefully studying the subgroups in $\mathcal{C}_2 \cup \mathcal{C}_5$, and by applying the fixed point ratio bounds in Theorems 2.6 and 2.16, one can show that

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

for all $x \in G$ of prime order, where

$$\alpha = 2 \cdot \frac{4}{3q} + \Big(1 + 2^{(m-1,e)} + (\log(e)+1)(q_0+1)(q_0^{m-1}+1)\Big) \cdot \frac{(4q+4)^{1/2-1/2m}}{q^{m-1}}$$

Now $q \geqslant 32$ since $q = q_0^e$ with $e \geqslant 5$, and it is straightforward to show that $\alpha < 1/3$. Therefore $u(G) \geqslant 3$ by Corollary 3.11.

4. Monodromy groups

In this section we turn to an application of fixed point ratios in the study of coverings of Riemann surfaces, focussing on the solution to Problem B stated in the introduction.

4.1. Preliminaries. Let X be a compact connected Riemann surface of genus $g \geqslant 0$ and let $Y = \mathbb{P}^1(\mathbb{C})$ be the Riemann sphere. Let $f : X \to Y$ be a branched covering of degree n. This means that f is a meromorphic function with a finite set of branch points $B = \{y_1, \ldots, y_k\} \subset Y$ (with $k \geqslant 2$) such that the restriction of f to $X^0 = X \setminus f^{-1}(B)$ is a covering map of degree n (that is, $|f^{-1}(y)| = n$ for all $y \in Y^0 = Y \setminus B$, so generically f is an "n-to-1" mapping).

Fix $y_0 \in Y^0$ and let $\Omega = f^{-1}(y_0) = \{x_1, \ldots, x_n\}$ be the fibre of y_0. Let γ be a loop in Y^0 based at y_0. For each $x_i \in \Omega$, we can lift γ via f to a path $\tilde{\gamma}_i$ in X beginning at x_i. The endpoint $\tilde{\gamma}_i(1)$ is also in Ω and the corresponding map $\sigma_\gamma : x_i \mapsto \tilde{\gamma}_i(1)$ is a permutation of Ω, which is independent of the homotopy type of γ. In this way, we obtain a homomorphism

$$\varphi : \pi_1(Y^0, y_0) \to \mathrm{Sym}(\Omega), \quad [\gamma] \mapsto \sigma_\gamma$$

from the fundamental group of Y^0 with base point y_0. The image of this map is a permutation group of degree n. Moreover, the path connectedness of Y^0 implies that the group we obtain in this way is independent of the choice of base point $y_0 \in Y^0$, up to permutation isomorphism. This allows us to make the following definition.

Definition 4.1. The *monodromy group* $\mathrm{Mon}(X, f)$ of f is defined to be the image of φ.

Since X has genus g, we refer to $\mathrm{Mon}(X, f)$ as a *monodromy group of genus g*. The connectedness of X implies that $\mathrm{Mon}(X, f)$ is a transitive permutation group.

Example 4.2. Let $n \geqslant 2$ be an integer and consider the map $f : X \to Y$ given by $f(z) = z^n$, where $X = Y = \mathbb{P}^1(\mathbb{C})$. This is a branched covering of degree n with branch points $B = \{0, \infty\}$ and $\Omega = f^{-1}(1) = \{e^{2\pi i k/n} : k = 0, 1, \ldots, n-1\}$. Here the monodromy group is cyclic of order n, generated by the permutation $\alpha \mapsto \zeta\alpha$ of Ω, with $\zeta = e^{2\pi i/n}$.

There is a natural generating set $\{\gamma_1, \ldots, \gamma_k\}$ for $\pi_1(Y^0, y_0)$, where γ_i is a loop that encircles the i-th branch point y_i (and no other branch point) with the property that the γ_i only meet at y_0. Moreover, by relabelling if necessary, one can show that the product $\gamma_1 \cdots \gamma_k$ is homotopy equivalent to the trivial loop based at y_0, so $\gamma_1 \cdots \gamma_k = 1$ and by a theorem of Hurwitz (1891) we have

$$\pi_1(Y^0, y_0) = \langle \gamma_1, \dots, \gamma_k \mid \gamma_1 \cdots \gamma_k = 1 \rangle.$$

This implies that $\mathrm{Mon}(X, f) = \langle \sigma_1, \dots, \sigma_k \rangle$ and $\sigma_1 \cdots \sigma_k = 1$, where $\sigma_i = \sigma_{\gamma_i}$ as above.

Question. *Which transitive permutation groups $G \leqslant \mathrm{Sym}(\Omega)$ of degree n occur as the monodromy group of a branched covering $f : X \to \mathbb{P}^1(\mathbb{C})$ of genus g and degree n?*

A necessary and sufficient condition is provided by the *Riemann Existence Theorem* below (see [**100**] for a modern treatment). In the statement, recall that $\mathrm{ind}(x) = n - t$ is the *index* of a permutation $x \in \mathrm{Sym}(\Omega)$, where t is the number of cycles of x on Ω. Equivalently, $\mathrm{ind}(x)$ is the minimal ℓ such that x is a product of ℓ transpositions. Note that if $x_1, \dots, x_k$ are permutations of Ω with $x_1 \cdots x_k = 1$, then $\sum_i \mathrm{ind}(x_i)$ is even.

Theorem 4.3 (Riemann Existence Theorem). *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive group of degree n. Then G is isomorphic to a monodromy group $\mathrm{Mon}(X, f)$ for some compact connected Riemann surface X of genus g and branched covering $f : X \to \mathbb{P}^1(\mathbb{C})$ if and only if G has a generating set $\{g_1, \dots, g_k\}$ such that $g_1 \cdots g_k = 1$ and*

$$\sum_{i=1}^{k} \mathrm{ind}(g_i) = 2(n + g - 1). \tag{4.1}$$

This fundamental result allows us to translate questions about monodromy groups to purely group-theoretic problems concerning finite permutation groups. One of the main problems is to understand the structure of monodromy groups of genus g, specifically in terms of the composition factors of such groups. This is formalised in a highly influential conjecture of Guralnick and Thompson from 1990 [**56**], which we will discuss below.

Remark 4.4. There is a well understood connection between branched covers of $\mathbb{P}^1(\mathbb{C})$ and finite extensions of the field $\mathbb{C}(t)$. More precisely, if $f : X \to \mathbb{P}^1(\mathbb{C})$ is a branched covering then $\mathbb{C}(X)/\mathbb{C}(t)$ is a finite extension, where $\mathbb{C}(X)$ and $\mathbb{C}(t)$ denote the function fields of X and $\mathbb{P}^1(\mathbb{C})$, respectively. It turns out that the Galois group of the normal closure of this extension is the monodromy group $\mathrm{Mon}(X, f)$. Therefore, Theorem 4.3 can be interpreted in terms of the inverse Galois problem. In particular, this viewpoint permits natural generalisations in which $\mathbb{C}$ is replaced by some other algebraically closed field (of any characteristic). We will return to this more general set-up at the end of the section.

4.2. The Guralnick-Thompson conjecture. Motivated by the discussion above, we define the *genus* of a finite group as follows.

Definition 4.5. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite transitive permutation group and let $E = \{g_1, \dots, g_k\}$ be a generating set for G with $g_1 \cdots g_k = 1$. Define the genus $g = g(G, \Omega, E)$ as in (4.1) and define $g(G, \Omega)$ to be the minimal value of $g(G, \Omega, E)$ over all such generating sets E (for any k). We say that a finite group G has *genus g* if it has a faithful transitive G-set Ω such that $g(G,\Omega) \leqslant g$.

Example 4.6. Let $G = \langle g_1 \rangle$ be a cyclic group of order n. Set $E = \{g_1, g_1^{-1}\}$ and consider the regular action of G on itself. Then $\mathrm{ind}(g_1) = \mathrm{ind}(g_1^{-1}) = n-1$, so (4.1) implies that G has genus zero.

Example 4.7. Let $G = \mathrm{Sym}(n) = \langle g_1, g_2, g_2^{-1}g_1^{-1} \rangle$, where $g_1 = (1,2)$ and $g_2 = (1,2,\ldots,n)$, and consider the natural action of G of degree n. The indices of the respective generators are 1, $n-1$ and $n-2$, hence G has genus zero. Similarly, every alternating group has genus 0.

Fix a non-negative integer g and let $\mathcal{C}(g)$ be the set of composition factors of groups of genus g. Note that $\mathcal{C}(0) \subseteq \mathcal{C}(g)$. In view of the above examples, it follows that $\mathcal{C}(g)$ contains every simple cyclic and alternating group. Therefore we focus on $\mathcal{E}(g)$, which is the set of nonabelian, non-alternating composition factors of groups of genus g.

The following theorem establishes a conjecture of Guralnick and Thompson [**56**], which we stated as Problem B in the introduction.

Theorem 4.8. *$\mathcal{E}(g)$ is finite for each g.*

Sketch proof. We briefly sketch the main steps, highlighting the central role played by fixed point ratios.

Step 1. Reduction to almost simple primitive groups.

By work of Aschbacher, Guralnick, Neubauer, Thompson and others [**3, 49, 56, 89**], it is sufficient to show that there are only finitely many primitive almost simple groups of Lie type of genus g. The key ingredient in this highly nontrivial reduction is the Aschbacher-O'Nan-Scott theorem (as formulated in [**5**]) on the structure of finite groups with a core-free maximal subgroup. See [**49**, Section 5] for more details.

Step 2. Fixed point ratio estimates.

The next result provides the connection to fixed point ratios (see [**49**, Corollary 2]).

Proposition 4.9. *Let $\mathcal{X}$ be the set of nonabelian, non-alternating finite simple groups such that*

$$\max_{1 \neq x \in G} \mathrm{fpr}(x,\Omega) \leqslant \frac{1}{86} \tag{4.2}$$

for every almost simple primitive group $G \leqslant \mathrm{Sym}(\Omega)$ with socle $G_0 \in \mathcal{X}$. Then $\mathcal{X} \cap \mathcal{E}(g)$ is finite for every non-negative integer g.

Proof. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple group of degree n with socle $G_0 \in \mathcal{X}$, so (4.2) holds. Fix a generating set $\{g_1,\ldots,g_k\}$ for G such that $g_1 \cdots g_k = 1$ and define g as in (4.1). Note that $k \geqslant 3$. Let d_i be the order of g_i and let $\mathrm{orb}(g_i)$ be the number of cycles of g_i on Ω. Without loss of generality, we may assume that $d_i \leqslant d_{i+1}$ for all i.

By the orbit-counting lemma we have

$$\mathrm{orb}(g_i) = \frac{n}{d_i}\sum_{x\in\langle g_i\rangle}\mathrm{fpr}(x,\Omega) = \frac{n}{d_i}\left(1+\sum_{1\neq x\in\langle g_i\rangle}\mathrm{fpr}(x,\Omega)\right)$$

and thus

$$\sum_{i=1}^{k}\mathrm{ind}(g_i) = \sum_{i=1}^{k}(n-\mathrm{orb}(g_i)) \geqslant \frac{85}{86}n\sum_{i=1}^{k}\frac{d_i-1}{d_i}.$$

Since G is insoluble and $G \not\cong \mathrm{Alt}(5)$, [**56**, Proposition 2.4] implies that

$$\sum_{i=1}^{k}\frac{d_i-1}{d_i} \geqslant \frac{85}{42}. \tag{4.3}$$

(Note that equality holds if and only if $k=3$ and $(d_1,d_2,d_3)=(2,3,7)$, so G is a *Hurwitz group*, such as $\mathrm{PSL}_2(7)$.) Therefore

$$2(n+g-1) = \sum_{i=1}^{k}\mathrm{ind}(g_i) \geqslant \frac{85}{86}\cdot\frac{85}{42}n$$

and thus $n \leqslant 7224(g-1)$. The result follows. □

Step 3. Bounded rank.

We combine Proposition 4.9 with Theorem 2.6, noting that $4/3q \leqslant 1/86$ when $q > 113$ (the almost simple groups with socle $\mathrm{PSL}_2(q)$ excluded in Theorem 2.6 can be handled separately).

Therefore, to complete the proof of the theorem we may assume that G is an almost simple classical group of large rank (in other words, we may assume that the dimension of the natural module of the socle of G is arbitrarily large).

Step 4. Classical groups in non-subspace actions.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group over $\mathbb{F}_q$ with socle G_0 in a non-subspace action (see Definition 2.9). Let m be the dimension of the natural module for G_0. By Theorem 2.15 there is a constant $\delta > 0$ such that

$$\max_{1\neq x\in G}\mathrm{fpr}(x) < q^{-\delta m},$$

so there are at most finitely many groups G with $\max_{1\neq x\in G}\mathrm{fpr}(x) > 1/86$. Now apply Proposition 4.9.

Step 5. Classical groups in subspace actions.

To complete the proof it remains to handle the subspace actions of classical groups. It is sufficient to prove the following result (see [**45**]).

PROPOSITION 4.10. *Fix a prime power q and non-negative integer g. Then there exists a constant $N = N(q)$ such that if $G \leqslant \mathrm{Sym}(\Omega)$ is any primitive almost simple classical group over $\mathbb{F}_q$ in a subspace action of genus g then either $m \leqslant N$ or $n \leqslant 2000g$, where m is the dimension of the natural module and n is the degree of G.*

In other words, if the dimension of the natural module V is large enough, then the degree of G is bounded above by a (linear) function of g and the result follows. The key tool is Theorem 2.13 – the details are rather technical, so we only provide a rough outline of the argument.

Let $G = \langle g_1, \ldots, g_k \rangle$ be a generating set such that $g_1 \cdots g_k = 1$ and (4.1) holds. Let d_i be the order of g_i and label the g_i so that $d_i \leqslant d_{i+1}$ for all i. Let φ be Euler's function and set

$$\begin{aligned}\nu(d) &= \min\{\nu(x) \,:\, x \in G,\, |x| = d\},\\ \alpha_0(d) &= 1 - \frac{1}{d}\sum_{a|d} \varphi(a) q^{-\nu(a)}\end{aligned}$$

for each natural number d. Note that $\alpha_0(d) \geqslant 1/4$ if $d \geqslant 2$. Set

$$\alpha(g_i) = \frac{\mathrm{ind}(g_i)}{n}, \quad \sigma = \sum_{i=1}^{k} \alpha(g_i)$$

and observe that it suffices to show that $\sigma > 2.001$ if m is sufficiently large (where m is the dimension of the natural module).

We may assume that m is large enough so that Theorem 2.13 gives

$$\mathrm{fpr}(x) < q^{-\nu(x)} + 10^{-3}$$

for all $1 \neq x \in G \cap \mathrm{PGL}(V)$. Then

$$\begin{aligned}\alpha(g_i) = 1 - \frac{1}{d_i}\sum_{j=1}^{d_i} \mathrm{fpr}(g_i^j) &> 1 - \frac{1}{d_i}\left(\sum_{j=1}^{d_i} q^{-\nu(|g_i^j|)}\right) - 10^{-3}\\ &= 1 - \frac{1}{d_i}\left(\sum_{a|d_i} \varphi(a) q^{-\nu(a)}\right) - 10^{-3}\\ &= \alpha_0(d_i) - 10^{-3}\end{aligned}$$

which is at least 0.249, whence $\sigma \geqslant 0.249k$. Therefore, we may assume that $k \leqslant 8$. With further work it is possible to reduce to the minimal case $k = 3$, where the final analysis splits into several subcases according to the values of d_1, d_2 and d_3. It is worth noting that an important tool in the latter reduction is the fact that

$$\sum_{i=1}^{k} \nu(g_i) \geqslant 2m,$$

which follows from a well known theorem of Scott [**93**]. □

4.3. Genus zero groups. It remains an open problem to explicitly determine the simple groups in $\mathcal{E}(g)$, although there has been some significant recent progress in the low genus cases, and in particular the special case $g = 0$. For example, the sporadic groups in $\mathcal{E}(0)$ have been determined by Magaard [**85**]; the examples are as follows:

$$\mathrm{M}_{11},\ \mathrm{M}_{12},\ \mathrm{M}_{22},\ \mathrm{M}_{23},\ \mathrm{M}_{24},\ \mathrm{J}_1,\ \mathrm{J}_2,\ \mathrm{Co}_3,\ \mathrm{HS}.$$

By work of Frohardt and Magaard [**42, 43**], the only exceptional groups in $\mathcal{E}(0)$ are ${}^2B_2(8)$, $G_2(2)' \cong \mathrm{PSU}_3(3)$ and ${}^2G_2(3)' \cong \mathrm{PSL}_2(8)$. The relevant groups of the form $\mathrm{PSL}_2(q)$ and $\mathrm{PSU}_3(q)$ are determined in [**40**]:

$$\begin{aligned} \mathrm{PSL}_2(q):\ & q \in \{7,8,11,13,16,17,19,25,27,29,31,32,37,41,43,64\} \\ \mathrm{PSU}_3(q):\ & q \in \{3,4,5\} \end{aligned}$$

There is work in progress by Frohardt, Guralnick, Hoffman and Magaard to extend the results in [**40**] to higher rank classical groups, leading to a complete classification of all primitive permutation groups of genus zero. In fact, the ultimate aim is to determine the primitive groups of genus at most two, building on earlier work in [**41**]. It is anticipated that these results will have interesting number-theoretic applications.

At a conference in July 2016 (*Algebraic Combinatorics and Group Actions*, Herstmonceux Castle, UK), Frohardt announced that the groups in $\mathcal{E}(0)$ have been determined. The complete list is as follows:

$\mathrm{PSL}_2(q)$, $7 \leqslant q \leqslant 43$, $q \neq 9, 23$
$\mathrm{PSL}_2(64)$
$\mathrm{PSL}_3(q)$, $q \in \{3,4,5,7\}$
$\mathrm{PSL}_4(3)$, $\mathrm{PSL}_4(4)$, $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_5(3)$, $\mathrm{PSL}_6(2)$
$\mathrm{PSU}_3(3)$, $\mathrm{PSU}_3(4)$, $\mathrm{PSU}_3(5)$
$\mathrm{PSp}_4(3)$, $\mathrm{PSp}_4(4)$, $\mathrm{PSp}_4(5)$
$\mathrm{PSp}_6(2)$, $\mathrm{PSp}_8(2)$
$\mathrm{P\Omega}_8^+(2)$, $\mathrm{P\Omega}_8^-(2)$
${}^2B_2(8)$
M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2, Co_3, HS

Example 4.11. Notice that $G = \mathrm{PSL}_2(23) \notin \mathcal{E}(0)$. To see that G does not have a primitive genus zero action, first observe that G has five conjugacy classes of maximal subgroups, represented by

$$Z_{23}{:}Z_{11},\ \ D_{24},\ \ D_{22},\ \ \mathrm{Sym}(4) \text{ (two classes).}$$

Fix a maximal subgroup M and set $n = |G : M|$. As recorded in the following table, it is straightforward to compute $\mathrm{ind}(x)$ for each non-identity $x \in G$ (with respect to the action of G on G/M):

M	n	$2n-2$	$\lvert x\rvert = 2$	3	4	6	11	12	23
$Z_{23}{:}Z_{11}$	24	46	12	16	18	20	20	22	22
D_{24}	253	504	120	168	186	208	230	230	242
D_{22}	276	550	132	184	208	238	250	252	264
$\mathrm{Sym}(4)$	253	504	122	166	186	208	230	230	242

Seeking a contradiction, suppose that $G = \langle g_1, \ldots, g_k\rangle$ with $g_1 \cdots g_k = 1$ and $\sum_i \mathrm{ind}(g_i) = 2n-2$. As before, let d_i denote the order of g_i and assume $d_i \leqslant d_{i+1}$ for all i.

Suppose M is the Borel subgroup $Z_{23}{:}Z_{11}$, so $2n-2 = 46$. From the above table, it follows that $k = 3$, $d_1 = 2$ and $d_2 \in \{2,3\}$. If $d_2 = 2$ then $\sum_i (d_i - 1)/d_i < 2$, which contradicts the bound in (4.3). Therefore, $d_2 = 3$

and a second application of (4.3) forces $d_3 \geqslant 11$. But this implies that

$$\sum_{i=1}^{k} \mathrm{ind}(g_i) \geqslant 12 + 16 + 20 > 46,$$

which is a contradiction. The other cases are similar.

4.4. Generalisations. As noted in Remark 4.4, there are natural generalisations to other fields. Let k be an algebraically closed field of characteristic $p \geqslant 0$ and let $f : X \to Y$ be a finite separable cover of smooth projective curves over k. Let G be the corresponding monodromy group, which is the Galois group of the normal closure of the extension $k(X)/k(Y)$ of function fields. As for $p = 0$, in positive characteristic we can seek restrictions on the structure of G according to the genus of X. There is still a translation of the problem to group theory, but the set-up is much more complicated. For example, there is no known analogue of Riemann's Existence Theorem and further complications arise if the given cover f is wildly ramified (the proof of the Guralnick-Thompson conjecture goes through essentially unchanged in the tamely ramified case).

The following conjecture of Guralnick is the positive characteristic analogue of the Guralnick-Thompson conjecture (see [**50**, Conjecture 1.6]). In order to state the conjecture, let p be a prime and let S be a nonabelian simple group. We say that S has genus g (in characteristic p) if S is a composition factor of the monodromy group of a finite separable cover $f : X \to Y$ of smooth projective curves over an algebraically closed field of characteristic p with X of genus at most g.

Conjecture 4.12. *Let $g \geqslant 0$ be an integer and let $\mathrm{E}_p(g)$ be the set of nonabelian non-alternating simple groups of genus g in characteristic $p > 0$. Then*

$$\mathrm{E}_p(g) \cap \left(\bigcup_{r \neq p} \mathrm{Lie}(r) \right)$$

is finite, where $\mathrm{Lie}(r)$ is the set of finite simple groups of Lie type in characteristic r.

The condition $r \neq p$ in the conjecture is necessary. For example, work of Abhyankar (see [**1**] and the references therein) shows that $\mathrm{E}_p(0)$ contains every simple classical group in characteristic p. Guralnick's conjecture is still open in its full generality, and we refer the reader to the survey article [**50**] for further details. Here it is worth highlighting [**50**, Theorem 1.5], which shows that the conjecture holds if we replace $\mathrm{Lie}(r)$ by the set of finite simple groups of Lie type in characteristic r of bounded dimension.

5. Bases

In this final section we introduce the classical notion of a base for a permutation group and we discuss how probabilistic methods, based on fixed point ratio estimates, have been used to establish strong results on the minimal size of bases for simple groups. In particular, we will sketch a solution to Problem C in the introduction.

5.1. Preliminaries. We begin by defining the base size of a permutation group.

DEFINITION 5.1. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group. A subset B of Ω is a *base* for G if $\bigcap_{\alpha \in B} G_\alpha = 1$. The *base size* of G, denoted by $b(G)$, is the minimal cardinality of a base.

EXAMPLES 5.2.

1. $b(G) = 1$ if and only if G has a regular orbit on Ω.
2. $b(G) = n - 1$ for the natural action of $G = \mathrm{Sym}(n)$ on $\Omega = \{1, \ldots, n\}$.
3. $b(G) = \dim V$ for the natural action of $G = \mathrm{GL}(V)$ on $\Omega = V$.
4. $b(G) = \dim V + 1$ for the action of $G = \mathrm{PGL}(V)$ on the set of 1-dimensional subspaces of V.

REMARK 5.3. Bases arise naturally in several different contexts:

a. *Abstract group theory.* Let G be a finite group and let H be a core-free subgroup, so we may view G as a permutation group on $\Omega = G/H$. In this context, $b(G)$ is the size of the smallest subset $S \subseteq G$ such that $\bigcap_{x \in S} H^x = 1$.

b. *Permutation group theory.* Let G be a permutation group of degree n and let B be a base for G. If $x, y \in G$ then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in B \iff xy^{-1} \in \bigcap_{\alpha \in B} G_\alpha \iff x = y$$

and thus $|G| \leqslant n^{|B|}$. In this way, (upper) bounds on $b(G)$ can be used to bound the order of G.

c. *Computational group theory.* The concept of a *base and strong generating set* was introduced by Sims [**96**] in the early 1970s, and it plays a fundamental role in the computational study of finite permutation groups (e.g. for computing the order of the group, and testing membership). See [**95**, Section 4] for more details.

d. *Graph theory.* Let Γ be a graph with vertices V and automorphism group $G = \mathrm{Aut}(\Gamma) \leqslant \mathrm{Sym}(V)$. Then

$$\begin{aligned} b(G) &= \text{the } \textit{fixing number} \text{ of } \Gamma \\ &= \text{the } \textit{determining number} \text{ of } \Gamma \\ &= \text{the } \textit{rigidity index} \text{ of } \Gamma \end{aligned}$$

is a well-studied graph invariant. See the survey article by Bailey and Cameron [**9**] for further details.

Let G be a permutation group of degree n. In general, it is very difficult to compute $b(G)$ precisely (indeed, algorithmically, this is known to be an *NP-hard* problem; see [**10**]), so we focus on bounds, and in particular upper bounds in view of applications. It is easy to see that

$$\frac{\log |G|}{\log n} \leqslant b(G) \leqslant \log_2 |G| \tag{5.1}$$

and it is straightforward to construct transitive groups G such that $b(G)$ is at either end of this range. A well known conjecture of Pyber [**92**] from the early 1990s asserts that the situation for primitive groups is rather more restrictive, in the sense that there is an absolute constant c such that

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

for any primitive group G of degree n. This conjecture has very recently been proved by Duyan, Halasi and Maróti [**39**], building on the earlier work of many authors.

The following lemma reveals a connection between the base size and the minimal degree of a transitive group (cf. Section 2.2).

Lemma 5.4. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive group of degree n. Then $b(G)\mu(G) \geqslant n$.*

Proof. Let B be a base of minimal size and let S be the support of an element $1 \neq g \in G$ of minimal degree. If $B^x \cap S = \emptyset$ for some $x \in G$, then $B^x \subseteq \Omega \setminus S$, so g fixes every element of B^x, but this is not possible since B^x is a base. Therefore $|B^x \cap S| \geqslant 1$ for all $x \in G$.

Next we claim that $|\{x \in G \,:\, \alpha \in B^x\}| = |B||G|/n$ for all $\alpha \in \Omega$. Consider $\alpha_1 \in B$. Fix $y \in G$ such that $\alpha^y = \alpha_1$. Then

$$\{x \in G \,:\, \alpha = \alpha_1^x\} = \{x \in G \,:\, \alpha = \alpha^{yx}\} = \{x \in G \,:\, yx \in G_\alpha\} = y^{-1}G_\alpha,$$

so $|\{x \in G \,:\, \alpha \in B^x\}| = |B||G_\alpha| = |B||G|/n$ as claimed. We conclude that

$$|G| \leqslant \sum_{x \in G} |B^x \cap S| = \sum_{\alpha \in S} |\{x \in G \,:\, \alpha \in B^x\}| = |S||B||G|/n$$

and thus $\mu(G)b(G) = |S||B| \geqslant n$. □

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive group of degree n. Since

$$b(\mathrm{Sym}(n)) = n-1, \;\; b(\mathrm{Alt}(n)) = n-2$$

we will assume that $G \neq \mathrm{Alt}(n), \mathrm{Sym}(n)$. Determining upper bounds on $b(G)$ in terms of n is an old problem. We record some results:

- Bochert [**11**], 1889: $b(G) \leqslant n/2$
- Babai [**7**], 1981: $b(G) \leqslant c\sqrt{n}\log n$ for some constant c (independent of CFSG)
- Liebeck [**72**], 1984: $b(G) \leqslant c\sqrt{n}$ (using CFSG)

Remark 5.5. It is easy to see that Liebeck's bound is best possible. For example, if $G = \mathrm{Sym}(m)$ and Ω is the set of 2-element subsets of $\{1, \ldots, m\}$, then $n = \binom{m}{2}$ and $b(G) \sim \frac{2}{3}m = O(\sqrt{n})$. For instance, if $m \equiv 1 \pmod{12}$ then

$$\{\{1,2\},\{2,3\}, \;\; \{4,5\},\{5,6\}, \;\; \ldots, \;\; \{m-3,m-2\},\{m-2,m-1\}\}$$

is a base of size $2(m-1)/3$ (this is optimal).

Stronger bounds are attainable if we focus on specific families of primitive groups. For instance, a striking theorem of Seress [**94**] states that $b(G) \leqslant 4$ if G is soluble. For the remainder we will focus on almost simple primitive groups.

5.2. Simple groups and probabilistic methods. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple group of degree n, with socle G_0 and point stabiliser H. In studying the base size of such groups, it is natural to make a distinction between *standard* and *non-standard* groups, according to the following definition (see Definition 2.9 for the notion of a subspace action of a classical group).

Definition 5.6. We say that G is *standard* if one of the following holds:

(i) $G_0 = \mathrm{Alt}(m)$ and Ω is an orbit of subsets or partitions of $\{1, \ldots, m\}$;

(ii) G is a classical group in a subspace action.

Otherwise, G is *non-standard.* (Note that we will only use the terms *standard* and *non-standard* in the context of a primitive group.)

In general, if G is standard then H is "large" in the sense that $|G|$ is not bounded above by a polynomial in $n = |G : H|$ of fixed degree. For example, if we take the standard action of $G = \mathrm{PGL}_m(q)$ on 1-spaces then $|G| \sim q^{m^2-1}$ and $n \sim q^{m-1}$. In view of (5.1), this implies that the base size of such a standard group can be arbitrarily large (indeed, we already noted that $b(G) = m+1$ for the given action of $\mathrm{PGL}_m(q)$).

Now assume G is non-standard. By a theorem of Cameron, there is an absolute constant c such that $|G| \leqslant n^c$ for any such group G. In later work, Liebeck [**72**] showed that $c = 9$ is sufficient, and this was extended by Liebeck and Saxl [**76**] to give the following.

Theorem 5.7. *Let G be a non-standard group of degree n. Then either $|G| \leqslant n^5$, or $(G, n) = (\mathrm{M}_{23}, 23)$ or $(\mathrm{M}_{24}, 24)$.*

This result suggests that non-standard groups may admit small bases. Indeed, the following striking theorem of Liebeck and Shalev [**81**] shows that this is true in a very strong sense. The proof uses probabilistic methods based on fixed point ratio estimates.

Theorem 5.8. *There is an absolute constant c such that if $G \leqslant \mathrm{Sym}(\Omega)$ is a non-standard permutation group then the probability that a randomly chosen c-tuple in Ω is a base for G tends to 1 as $|G|$ tends to infinity.*

Remark 5.9. This asymptotic result was conjectured by Cameron and Kantor [**33**], and they showed that it holds for alternating and symmetric groups with the best possible constant $c = 2$.

Let us explain the connection between fixed point ratios and base sizes. Let c be a positive integer and let $Q(G, c)$ be the probability that a randomly chosen c-tuple of points in Ω is *not* a base for G, so

$$b(G) \leqslant c \iff Q(G, c) < 1.$$

Observe that a c-tuple in Ω fails to be a base if and only if it is fixed by an element $x \in G$ of prime order, and note that the probability that a randomly chosen c-tuple is fixed by x is equal to $\mathrm{fpr}(x)^c$. Let $\mathcal{P}$ be the set of elements of prime order in G, and let $x_1, \ldots, x_k$ represent the G-classes in $\mathcal{P}$. Then

$$Q(G, c) \leqslant \sum_{x \in \mathcal{P}} \mathrm{fpr}(x)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c =: \widehat{Q}(G, c). \tag{5.2}$$

We have thus established the following key lemma, which allows us to exploit upper bounds on fixed point ratios to bound the base size.

LEMMA 5.10. *If $\widehat{Q}(G,c) < 1$ then $b(G) \leqslant c$.*

SKETCH PROOF OF THEOREM 5.8. Let G_0 denote the socle of G. In view of the work of Cameron and Kantor in [**33**], we may assume that G_0 is a group of Lie type over $\mathbb{F}_q$.

First we claim that $b(G) \leqslant 500$ if G_0 is an exceptional group. To see this, we apply Theorem 2.6, which states that

$$\mathrm{fpr}(x) \leqslant \frac{4}{3q}$$

for all non-identity elements $x \in G$. Now $|G| \leqslant |\mathrm{Aut}(E_8(q))| < q^{249}$, so

$$Q(G,500) \leqslant \widehat{Q}(G,500) \leqslant \left(\frac{4}{3q}\right)^{500} \sum_{i=1}^{k} |x_i^G| < \left(\frac{4}{3q}\right)^{500} |G|$$

which is at most q^{-1} since $|G| < q^{249}$. The claim follows. Similarly, if G_0 is a non-standard classical group of rank r, then the same argument yields $b(G) \leqslant c(r)$ (with $Q(G,c(r)) \to 0$ as q tends to infinity).

The key tool to handle the remaining non-standard classical groups of arbitrarily large rank is Theorem 2.15, which states that there is a constant $\epsilon > 0$ such that

$$\mathrm{fpr}(x) < |x^G|^{-\epsilon} \tag{5.3}$$

for all $x \in G$ of prime order (recall that the non-standard hypothesis is essential). Let m be the dimension of the natural module for G_0. We need two facts:

1. G has at most q^{4m} conjugacy classes of elements of prime order (for example, this follows from [**74**, Theorem 1]); and
2. $|x^G| \geqslant q^{m/2}$ for all $x \in G$ of prime order.

Set $c = \lceil 11/\epsilon \rceil$. Then

$$\widehat{Q}(G,c) = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c < \sum_{i=1}^{k} |x_i^G|^{-10} \leqslant k \cdot (q^{m/2})^{-10} \leqslant q^{-m}$$

and thus $Q(G,c)$ tends to 0 as $|G|$ tends to infinity, as required. □

5.3. Further results. As the above sketch proof indicates, the constant c in Theorem 5.8 depends on the constant ϵ in (5.3), and is therefore undetermined. However, by applying the stronger fixed point ratio estimates in [**19, 20, 21, 22**] and [**71**], it is possible to show that $c = 6$ is optimal. Indeed, the following result, which is proved in the sequence of papers [**23, 27, 30, 31**], reveals a striking dichotomy for almost simple primitive groups: either the base size can be arbitrarily large (standard groups), or there exists an extremely small base (non-standard groups). This solves Problem B as stated in the introduction.

THEOREM 5.11. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a non-standard permutation group. Then $b(G) \leqslant 7$, with equality if and only if $G = \mathrm{M}_{24}$ in its natural action* *on* 24 *points. Moreover, the probability that a random* 6*-tuple in* Ω *forms a base for* G *tends to* 1 *as* $|G|$ *tends to infinity.*

Example 5.12. To illustrate the proof of Theorem 5.11 for exceptional groups, let us briefly sketch an argument to show that $b(G) \leqslant 5$ for $G = E_8(q)$.

First assume H is small, say $|H| \leqslant q^{88}$, and write $\widehat{Q}(G,5) = \alpha + \beta$ where α is the contribution to the summation from elements $x \in G$ with $|x^G| \leqslant \frac{1}{2}q^{112}$. Observe that

$$\beta < \frac{1}{2}q^{112}\left(\frac{2|H|}{q^{112}}\right)^5 \leqslant \frac{1}{2}q^{112}\left(\frac{2q^{88}}{q^{112}}\right)^5 = 16q^{-8}.$$

Suppose $x \in G$ has prime order and $|x^G| \leqslant \frac{1}{2}q^{112}$. The sizes of the conjugacy classes of elements of prime order in G are available in the literature and by inspection we see that x is unipotent of type A_1 or $2A_1$ (in terms of the standard Bala-Carter labelling of unipotent classes). There are fewer than $2q^{92}$ such elements in G, and [**71**, Theorem 2] implies that $\mathrm{fpr}(x) \leqslant 2q^{-24}$, hence

$$\alpha < 2q^{92}(2q^{-24})^5 = 64q^{-28}$$

and the result follows.

To complete the analysis, we may assume $|H| > q^{88}$. As discussed in Section 2.8, if H is a maximal parabolic subgroup then it is possible to compute very accurate fixed point ratio estimates using character-theoretic methods (recall that for unipotent elements, this relies on Lübeck's work on Green functions for exceptional groups). This allows us to obtain strong upper bounds on $b(G)$ for parabolic actions. Moreover, when combined with the trivial lower bound $b(G) \geqslant \log|G|/\log|\Omega|$, we get the exact base size in all but one case (here P_i denotes the maximal parabolic subgroup of G corresponding to the i-th node in the Dynkin diagram of G with respect to the standard Bourbaki [**13**] labelling):

H	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
$b(G)$	4	3	3	3	3	3	3 or 4	5

Note that $\log|G|/\log|\Omega| = 3 - o(1)$ when $H = P_7$, so we expect $b(G) = 4$ is the correct answer in this case.

Finally, let us assume $|H| > q^{88}$ and H is non-parabolic. By applying a fundamental subgroup structure theorem of Liebeck and Seitz (see [**77**, Theorem 8]), we deduce that H is of type $D_8(q)$, $E_7(q)A_1(q)$ or $E_8(q_0)$ with $q = q_0^2$. Let us assume H is of type $D_8(q)$; the other cases are similar. Let K be the algebraic closure of $\mathbb{F}_q$ and set $\bar{G} = E_8(K)$ and $\bar{H} = D_8(K)$, so we may view G as $\bar{G}_\sigma$, and similarly H as $\bar{H}_\sigma$, for a suitable Frobenius morphism σ of $\bar{G}$. Write $\widehat{Q}(G,5) = \alpha + \beta$, where α is the contribution from semisimple elements.

Let $x \in G$ be a semisimple element of prime order. By applying [**71**, Lemma 4.5], we have

$$\mathrm{fpr}(x) \leqslant \frac{|W(\bar{G}){:}W(\bar{H})| \cdot 2(q+1)^8}{q^{\delta(x)}(q-1)^8} = 270\left(\frac{q+1}{q-1}\right)^8 q^{-\delta(x)},$$

where $W(\bar{X})$ is the Weyl group of $\bar{X}$ and $\delta(x) = \dim x^{\bar{G}} - \dim(x^{\bar{G}} \cap \bar{H})$. If $C_{\bar{G}}(x)^0$ is not of type D_8, E_7T_1 nor E_7A_1, then [**70**, Theorem 2] implies that $\delta(x) \geqslant 80$ and we deduce that $\mathrm{fpr}(x) < q^{-59}$. Therefore, if α_1 denotes the contribution to α from these elements then

$$\alpha_1 < |G| \cdot (q^{-59})^5 < q^{248} \cdot q^{-295} = q^{-47}.$$

There are fewer than q^{130} remaining semisimple elements in G and by applying [**71**, Theorem 2] we deduce that their contribution is less than $q^{130} \cdot (q^{-37})^5 = q^{-55}$. In particular,

$$\alpha < q^{-47} + q^{-55}$$

is tiny.

For unipotent elements there is a distinction between the cases q even and q odd (recall that we are only interested in elements of prime order). In any case, the fusion in $\bar{G}$ of unipotent classes in $\bar{H}$ has been determined by Lawther [**69**] and using these results it is straightforward to show that β is also small (and tends to zero as q tends to infinity). See the proof of [**30**, Lemma 4.5] for the details.

For classical groups, Theorem 2.16 is the key ingredient in the proof of Theorem 5.11, which roughly states that $\epsilon \sim 1/2$ is optimal in (5.3). In order to use it, let m be the dimension of the natural module for G_0 and set

$$\eta_G(t) = \sum_{i=1}^{k} |x_i^G|^{-t}$$

for $t \in \mathbb{R}$, where $x_1, \ldots, x_k$ represent the G-classes of elements of prime order in G. If $m \geqslant 6$, then careful calculation reveals that $\eta_G(1/3) < 1$. Therefore, by combining this with the generic upper bound $\mathrm{fpr}(x) < |x^G|^{-1/2+1/m}$ from Theorem 2.16, we deduce that

$$\widehat{Q}(G,4) < \sum_{i=1}^{k} |x_i^G|^{1+4(-\frac{1}{2}+\frac{1}{m})} \leqslant \eta_G(1/3) < 1$$

if $m \geqslant 6$, and thus $b(G) \leqslant 4$. In this way, we can establish the following sharpened version of Theorem 5.11 for classical groups (see [**23**, Theorem 1]).

Theorem 5.13. *Let G be a non-standard classical group with point stabiliser H. Then $b(G) \leqslant 5$, with equality if and only if $G = \mathrm{PSU}_6(2).2$ and $H = \mathrm{PSU}_4(3).2^2$. Moreover, the probability that a random 4-tuple in Ω forms a base for G tends to 1 as $|G|$ tends to infinity.*

The problem of determining the precise base size of every non-standard group is an ongoing project of the author with Guralnick and Saxl. We finish by reporting on some recent work towards this goal.

5.3.1. *Alternating and sporadic groups.* If G_0 is a (non-standard) alternating or sporadic group, then $b(G)$ has been calculated in all cases. For example, if $G_0 = \mathrm{Alt}(n)$ then [**27**, Theorem 1.1] implies that $b(G) = 2$ if $n > 12$ (if $G = \mathrm{Alt}(12)$ and $H = \mathrm{M}_{12}$, then $b(G) = 3$). Similarly, if $G = \mathbb{M}$

is the Monster sporadic group, then $b(G) = 2$ unless $H = 2.\mathbb{B}$, in which case $b(G) = 3$ (see [**31**]).

To handle the symmetric and alternating groups, we first observe that H is a primitive subgroup (this follows from the non-standard hypothesis), so we can use a well known result of Maróti [**86**] to bound $|H|$ from above. This is combined with Theorem 2.3 on the minimal degree of H, which tells us that either $\mu(H) \geqslant n/2$, or H is a product-type group arising from the action of a symmetric group on k-sets. The latter situation can be handled directly, whereas in the general case we translate the bound on $\mu(H)$ into a lower bound on $|x^G|$ for all $x \in H$ of prime order. This is useful because

$$\widehat{Q}(G,2) < |H|^2 \max_{1 \neq x \in H} |x^G|^{-1}.$$

The proof for sporadic groups relies heavily on computational methods, together with detailed information on their conjugacy classes, irreducible characters and subgroup structure that is available in GAP [**47**]. Further work is needed to handle the Baby Monster and the Monster (see [**31, 90**] for more details).

As an aside, it is worth noting that determining the exact base size for the *standard* groups with an alternating socle is a difficult combinatorial problem. Indeed, this is an open problem, even for the action of $\mathrm{Sym}(n)$ on k-sets. See [**57**] for the best known results in this particular case.

5.3.2. *Classical groups.* Suppose G_0 is a classical group, so H is either geometric or non-geometric. In [**28**], probabilistic methods are used to determine the precise base size of all non-geometric actions of classical groups. Here the key ingredient is Theorem 2.18, combined with a detailed analysis of the low-dimensional irreducible representations of quasisimple groups. As discussed in Section 2.7, the lower bound on $\nu(x)$ in part (ii) of Theorem 2.18 yields a lower bound on $|x^G|$, so our approach is somewhat similar to the one we used for symmetric and alternating groups (although the details are more complicated in this situation).

The following result is a simplified version of [**28**, Theorem 1].

THEOREM 5.14. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a non-standard classical group with socle G_0 and point stabiliser $H \in \mathcal{S}$. Assume $n > 8$, where n is the dimension of the natural module for G_0. Then one of the following holds:*

(i) $b(G) = 2$*;*
(ii) $b(G) = 3$ *and* $(G,H) = (\mathrm{O}_{14}^{+}(2), \mathrm{Sym}(16))$, $(\mathrm{O}_{12}^{-}(2), \mathrm{Sym}(13))$, $(\Omega_{12}^{-}(2), \mathrm{Alt}(13))$ *or* $(\Omega_{10}^{-}(2), \mathrm{Alt}(12))$*;*
(iii) $b(G) = 4$ *and* $(G,H) = (\mathrm{O}_{10}^{-}(2), \mathrm{Sym}(12))$.

The analysis of the geometric actions of classical groups is more difficult, and so far we only have partial results. For example, we can show that $b(G) = 2$ if H is a subfield subgroup corresponding to a subfield of $\mathbb{F}_q$ of odd prime index. The analysis in some cases is rather delicate; for example, it can be difficult to decide if $b(G) = 2$ or 3. This sort of situation tends to arise when $|H| \sim |G|^{1/2}$, which often corresponds to a case where H is the centraliser in G of an involution (at least when q is odd). We anticipate that our recent work in [**29**] on base sizes for primitive actions of simple algebraic groups will play a role in this analysis.

5.3.3. *Non-standard groups with large base size.* The proof of Theorem 5.11 reveals that there are infinitely many exceptional groups with $b(G) \geqslant 5$. In fact, it has recently been shown that there are infinitely many with $b(G) = 6$ (see [**29**, Theorem 11]) and with some additional work it is possible to determine them all (see [**24**]).

THEOREM 5.15. *Let* $G \leqslant \mathrm{Sym}(\Omega)$ *be a non-standard permutation group with socle* G_0 *and point stabiliser* H. *Then* $b(G) = 6$ *if and only if one of the following holds:*

(i) $(G, H) = (\mathrm{M}_{23}, \mathrm{M}_{22})$, $(\mathrm{Co}_3, \mathrm{McL}.2)$, $(\mathrm{Co}_2, \mathrm{PSU}_6(2).2)$, *or* $(\mathrm{Fi}_{22}.2, 2.\mathrm{PSU}_6(2).2)$*;*

(ii) $G_0 = E_7(q)$ *and* $H = P_7$*;*

(iii) $G_0 = E_6(q)$ *and* $H = P_1$ *or* P_6.

In cases (ii) and (iii), the usual estimates via fixed point ratios yield $b(G) \in \{5, 6\}$, so more work is needed to pin down the precise answer. To do this we apply some recent results from [**29**] on bases for simple algebraic groups.

For example, consider case (ii). Let $\bar{G} = E_7$ and $\bar{H}$ be the corresponding algebraic groups over $\bar{\mathbb{F}}_q$ (so $\bar{H}$ is a maximal parabolic subgroup of $\bar{G}$ with Levi factor of type E_6) and let σ be a Frobenius morphism of $\bar{G}$ such that $(\bar{G}_\sigma)' = G_0$. We may assume that $\bar{H}$ is σ-stable. In [**29**, Section 5] we show that the generic 5-point stabiliser in $\bar{G}$ with respect to the action on the coset variety $\bar{G}/\bar{H}$ is 8-dimensional (here *generic* means that there is a non-empty open subvariety U of $(\bar{G}/\bar{H})^5$ such that the stabiliser in $\bar{G}$ of any tuple in U is 8-dimensional). By considering the fixed points under σ, we deduce that every 5-point stabiliser in the finite group G is nontrivial, for any q, and the result follows. Note that the connected component of the generic 5-point stabiliser is not a torus (because it is 8-dimensional), so there are no complications with split tori when $q = 2$.

Bibliography

[1] S.S. Abhyankar and N. Inglis, *Galois groups of some vectorial polymomials*, Trans. Amer. Math. Soc. **353** (2001), 2941–2969.

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

[3] M. Aschbacher, *On conjectures of Guralnick and Thompson*, J. Algebra **135** (1990), 277–343.

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

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

[6] M. Aschbacher and G.M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.

[7] L. Babai, *On the order of uniprimitive permutation groups*, Annals of Math. **113** (1981), 553–568.

[8] L. Babai, *On the order of doubly transitive permutation groups*, Invent. Math. **65** (1982), 473–484.

[9] R.F. Bailey and P.J. Cameron, *Base size, metric dimension and other invariants of groups and graphs*, Bull. London Math. Soc. **43** (2011), 209–242.

[10] K.D. Blaha, *Minimum bases for permutation groups: the greedy approximation*, J. Algorithms **13** (1992), 297–306.

[11] A. Bochert, *Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann*, Math. Ann. **33** (1889), 584–590.

[12] A. Bochert, *Ueber die Classe der transitiven Substitutionengruppen*, Math. Ann. **40** (1892), 176–193.

[13] N. Bourbaki, *Lie Groups and Lie Algebras* (*Chapters 4-6*), Springer, 2002.

[14] 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.

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

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

[17] 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.

[18] T.C. Burness, *Fixed point spaces in actions of classical algebraic groups*, J. Group Theory **7** (2004), 311–346.

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

[20] T.C. Burness, *Fixed point ratios in actions of finite classical groups, II*, J. Algebra **309** (2007), 80–138.

[21] T.C. Burness, *Fixed point ratios in actions of finite classical groups, III*, J. Algebra **314** (2007), 693–748.

[22] T.C. Burness, *Fixed point ratios in actions of finite classical groups, IV*, J. Algebra **314** (2007), 749–788.

[23] T.C. Burness, *On base sizes for actions of finite classical groups*, J. London Math. Soc. **75** (2007), 545–562.

[24] T.C. Burness, *On base sizes for almost simple primitive groups*, in preparation.

[25] T.C. Burness and M. Giudici, *Classical groups, derangements and primes*, vol. 25, Lecture Notes Series of the Aust. Math. Soc., Cambridge University Press, 2016.

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

[27] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for symmetric groups*, Bull. London Math. Soc. **43** (2011), 386–391.

[28] T.C. Burness, R.M. Guralnick and J. Saxl, *Base sizes for $\mathcal{S}$-actions of finite classical groups*, Israel J. Math. **199** (2014), 711–756.

[29] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for algebraic groups*, J. European Math. Soc. (JEMS), to appear.

[30] T.C. Burness, M.W. Liebeck and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. London Math. Soc. **98** (2009), 116–162.

[31] T.C. Burness and E.A. O'Brien and R.A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–334.

[32] T.C. Burness and A.R. Thomas, *On the involution fixity of exceptional groups of Lie type*, preprint.

[33] P.J. Cameron and W.M. Kantor, *Random permutations: some group-theoretic aspects*, Combin. Probab. Comput. **2** (1993), 257–262.

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

[35] E. Covato, *The involution fixity of simple groups*, PhD thesis, University of Bristol, 2017.

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

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

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

[39] H. Duyan, Z. Halasi and A. Maróti, *A proof of Pyber's base size conjecture*, submitted (arxiv:1611.09487).

[40] D. Frohardt, R. Guralnick and K. Magaard, *Genus* 0 *actions of groups of Lie rank* 1, in Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 449–483, Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002.

[41] D. Frohardt, R. Guralnick and K. Magaard, *Primitive monodromy groups of genus at most two*, J. Algebra **417** (2014), 234–274.

[42] D. Frohardt and K. Magaard, *Monodromy composition factors among exceptional groups of Lie type*, in Group theory (Granville, OH, 1992), 134–143, World Sci. Publ., River Edge, NJ, 1993.

[43] D. Frohardt and K. Magaard, *About a conjecture of Guralnick and Thompson*, in Groups, difference sets, and the Monster (Columbus, OH, 1993), 43–54, Ohio State Univ. Math. Res. Inst. Publ., vol. 4, de Gruyter, Berlin, 1996.

[44] D. Frohardt and K. Magaard, *Grassmannian fixed point ratios*, Geom. Dedicata **82** (2000), 21–104.

[45] D. Frohardt and K. Magaard, *Composition factors of monodromy groups*, Annals of Math. **154** (2001), 327–345.

[46] D. Frohardt and K. Magaard, *Fixed point ratios in exceptional groups of rank at most two*, Comm. Algebra **30** (2002), 571–602.

[47] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004.

[48] J. Fulman and R.M. Guralnick, *The probability of generating an irreducible subgroup*, in preparation.

[49] R.M. Guralnick, *The genus of a permutation group*, in Groups, combinatorics & geometry (Durham 1990), 351–363, London Math. Soc. Lecture Note Ser. vol. 165, Cambridge University Press, 1992.

[50] R.M. Guralnick, *Monodromy groups of coverings of curves*, in Galois groups and fundamental groups, Math. Sci. Res. Inst. Publ. **41**, 1–46, Cambridge University Press, 2003.

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

[52] R.M. Guralnick and K. Magaard, *On the minimal degree of a primitive permutation group*, J. Algebra **207** (1998), 127–145.

[53] 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.

[54] R.M. Guralnick and J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), 519–571.

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

[56] R.M. Guralnick and J.G. Thompson, *Finite groups of genus zero*, J. Algebra **131** (1990), 303–341.

[57] Z. Halasi, *On the base size for the symmetric group acting on subsets*, Studia Sci. Math. Hungar. **49** (2012), 492–500.

[58] S. Harper, *On the uniform spread of almost simple symplectic and orthogonal groups*, in preparation.

[59] G. Hiss and G. Malle, *Low dimensional representations of quasi-simple groups*, LMS J. Comput. Math. **4** (2001), 22–63.

[60] G. Hiss and G. Malle, *Corrigenda: Low dimensional representations of quasi-simple groups*, LMS J. Comput. Math. **5** (2002), 95–126.

[61] G.D. James, *The Representation Theory of the Symmetric Groups*, Springer Lecture Notes in Math. **682**, Springer, Berlin, 1978.

[62] C. Jordan, *Théorèmes sur les groupes primitifs*, J. Math. Pures Appl. (Liouville) **16** (1871), 383–408.

[63] C. Jordan, *Recherches sur les substitutions*, J. Math. Pures Appl. (Liouville) **17** (1872), 351–367.

[64] W.M. Kantor, *Subgroups of classical groups generated by long root elements*, Trans. Amer. Math. Soc. **248** (1979), 347–379.

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

[66] J. Kempe, L. Pyber and A. Shalev, *Permutation groups, minimal degrees and quantum computing*, Groups Geom. Dyn. **1** (2007), 553–584.

[67] 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.

[68] 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.

[69] R. Lawther, *Unipotent classes in maximal subgroups of exceptional algebraic groups*, J. Algebra **322** (2009), 270–293.

[70] R. Lawther, M.W. Liebeck and G.M. Seitz, *Fixed point spaces in actions of exceptional algebraic groups*, Pacific J. Math. **205** (2002), 339–391.

[71] 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.

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

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

[74] M.W. Liebeck and L. Pyber, *Upper bounds for the number of conjugacy classes of a finite group*, J. Algebra **198** (1997), 538–562.

[75] 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.

[76] M.W. Liebeck and J. Saxl, *Maximal subgroups of finite simple groups and their automorphism groups*, Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989), 243–259, Contemp. Math. **131**, Amer. Math. Soc., 1992.

[77] 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.

[78] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.

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

[80] M.W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky*, J. Algebra **184** (1996), 31–57.

[81] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.

[82] M.W. Liebeck and A. Shalev, *On fixed points of elements in primitive permutation groups*, J. Algebra **421** (2015), 438–459.

[83] L. Lovász, *Combinatorial problems and exercises*, North-Holland, Amsterdam, 1979.

[84] F. Lübeck, *Small degree representations of finite Chevalley groups in defining characteristic*, LMS J. Comput. Math. **4** (2001), 135–169.

[85] K. Magaard, *Monodromy and sporadic groups*, Comm. Algebra **21** (1993), 4271–4297.

[86] A. Maróti, *On the order of primitive groups*, J. Algebra **258** (2002), 631–640.

[87] 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.

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

[89] M.G. Neubauer, *On monodromy groups of fixed genus*, J. Algebra **153** (1992), 215–261.

[90] M. Neunhöffer, F. Noeske, E.A. O'Brien and R.A. Wilson, *Orbit invariants and an application to the Baby Monster*, J. Algebra **341** (2011), 297–305.

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

[92] L. Pyber, *Asymptotic results for permutation groups*, in Groups and Computation (eds. L. Finkelstein and W. Kantor), DIMACS Series, vol. 11, pp.197–219, 1993.

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

[94] Á. Seress, *The minimal base size of primitive solvable permutation groups*, J. London Math. Soc. **53** (1996), 243–255.

[95] Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics **152**, Cambridge University Press, 2003.

[96] C.C. Sims, *Computation with permutation groups*, Proc. Second Sympos. on Symbolic and Algebraic Manipulation, (ACM, New York), pp.23–28, 1971.

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

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

[99] R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. **80** (1968).

[100] H. Völklein, *Groups as Galois Groups: An Introduction*, Cambridge Studies in Advanced Math. **53**, Cambridge University Press, 1996.

[101] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.