# ON THE UNIFORM DOMINATION NUMBER OF A FINITE SIMPLE GROUP

TIMOTHY C. BURNESS AND SCOTT HARPER

ABSTRACT. Let $G$ be a finite simple group. By a theorem of Guralnick and Kantor, $G$ contains a conjugacy class $C$ such that for each non-identity element $x \in G$, there exists $y \in C$ with $G = \langle x, y \rangle$. Building on this deep result, we introduce a new invariant $\gamma_u(G)$, which we call the uniform domination number of $G$. This is the minimal size of a subset $S$ of conjugate elements such that for each $1 \neq x \in G$, there exists $s \in S$ with $G = \langle x, s \rangle$. (This invariant is closely related to the total domination number of the generating graph of $G$, which explains our choice of terminology.) By the result of Guralnick and Kantor, we have $\gamma_u(G) \leqslant |C|$ for some conjugacy class $C$ of $G$, and the aim of this paper is to determine close to best possible bounds on $\gamma_u(G)$ for each family of simple groups. For example, we will prove that there are infinitely many non-abelian simple groups $G$ with $\gamma_u(G) = 2$. To do this, we develop a probabilistic approach, based on fixed point ratio estimates. We also establish a connection to the theory of bases for permutation groups, which allows us to apply recent results on base sizes for primitive actions of simple groups.

## CONTENTS



## 1. INTRODUCTION

The study of generators for simple groups has a long and rich history, with numerous applications. As a consequence of the Classification of Finite Simple Groups, it is known that every finite simple group can be generated by two elements; this is a theorem of Steinberg [45] for groups of Lie type, and the argument was completed by Aschbacher and Guralnick in [2]. This result leads to many interesting problems that have been the focus of intensive research in recent years. For instance, it is natural to consider the abundance of generating pairs in a simple group, and also the existence of generators with prescribed properties, such as restrictions on the orders of the generating elements.

Through the work of many authors, we now understand that finite simple groups have some remarkable generation properties. For example, a theorem of Liebeck and Shalev [40], extending earlier work of Dixon [22] and Kantor and Lubotzky [34], shows that a randomly

*Date*: March 21, 2018.

2010 *Mathematics Subject Classification.* Primary 20E32, 20F05; Secondary 20E28, 20P05.

The second author thanks the Engineering and Physical Sciences Research Council and the Heilbronn Institute for Mathematical Research for their financial support. Both authors thank an anonymous referee for helpful comments on a previous version of the paper.

chosen pair of elements in a finite simple group $G$ forms a generating set with probability tending to 1 as $|G|$ tends to infinity. In [24] (also see [44]), Guralnick and Kantor use probabilistic methods to prove that every non-identity element of a finite simple group $G$ belongs to a generating pair (a group with this strong 2-generation property is said to be $\frac{3}{2}$-*generated*). See [10, 16, 28, 31] for further results in this direction for simple and almost simple groups. We refer the reader to [15] for a recent survey of related topics concerning the generation of simple groups.

Let $G$ be a finite group and let $G^{\#}$ be the set of non-identity elements of $G$. The *generating graph* of $G$, denoted by $\Gamma(G)$, has vertex set $G^{\#}$ and two vertices are adjacent if and only if they generate $G$. This graph encodes many interesting generation properties of a 2-generated group. For example, $G$ is $\frac{3}{2}$-generated if and only if $\Gamma(G)$ has no isolated vertices. In turn, many natural invariants of this graph have interesting group-theoretic interpretations, and this provides an appealing interplay between group theory and graph theory. For instance, it is natural to consider the connectedness, diameter and Hamiltonicity of $\Gamma(G)$, as well as its clique, co-clique and chromatic numbers. In recent years, numerous authors have focussed on these problems in the context of a non-abelian finite simple group $G$. Here one of the most striking results is [10, Theorem 1.2], which implies that $\Gamma(G)$ is connected with diameter 2. In [11], it is conjectured that $\Gamma(G)$ always contains a Hamiltonian cycle, but so far this has only been established for all sufficiently large simple groups (see [11, Theorem 1.2]). The proof of this result uses a combination of probabilistic and combinatorial techniques.

In this paper we initiate the study of another natural invariant of the generating graph of a finite group. Let $\Gamma$ be a finite graph with no isolated vertices. A subset $S$ of $\Gamma$ is a *total dominating set* if every vertex of $\Gamma$ is adjacent to a vertex in $S$, and the *total domination number* of $\Gamma$ is the minimal size of a total dominating set. This is a well-studied invariant, which, in general, is rather difficult to compute precisely. Indeed, the problem of determining whether the total domination number of a given graph is at most a given number $k$ is NP-complete (see the survey [32] for more details).

As noted above, if a finite group $G$ is $\frac{3}{2}$-generated then its generating graph $\Gamma(G)$ has no isolated vertices. In this situation, we define the *total domination number* $\gamma_t(G)$ of $G$ to be the total domination number of $\Gamma(G)$.

In this paper, we will work with a slightly stronger notion. Let $k$ be a positive integer. Following [10], we say that $G$ has *uniform spread* $k$ if there exists a fixed conjugacy class $C$ of $G$ with the property that for any $k$ elements $x_1, \ldots, x_k \in G^{\#}$ there exists $g \in C$ such that $G = \langle x_i, g \rangle$ for all $i$. Therefore, $G$ has uniform spread 1 if and only if some conjugacy class of $G$ is a total dominating set for $\Gamma(G)$. By the main theorem of [24], every finite simple group $G$ has uniform spread 1 (in fact, [10, Theorem 1.2] shows that all finite simple groups have uniform spread 2). Therefore, for finite groups with uniform spread 1, such as simple groups, it is natural to seek small total dominating sets of conjugate elements. This leads us naturally to the following definition.

**Definition.** Let $G$ be a finite group with uniform spread 1 and generating graph $\Gamma(G)$. We define the *uniform domination number* $\gamma_u(G)$ of $G$ to be the minimal number of conjugate elements that form a total dominating set for $\Gamma(G)$.

Observe that $\gamma_t(G) \leqslant \gamma_u(G)$. Also note that $\gamma_u(G) = 1$ if and only if $G$ is cyclic.

We are now in a position to state our main results on the uniform domination number of simple groups. By the above observations, if $G$ is a non-abelian finite simple group then

$$2 \leqslant \gamma_u(G) \leqslant |C| \tag{1.1}$$

for some conjugacy class $C$ of $G$. (Typically, $C$ is large, such as a class of regular semisimple elements if $G$ is a group of Lie type.) Our first result shows that there are infinitely many groups for which the trivial lower bound in (1.1) is sharp (see Theorems 3.8 and 5.2(i)).

**Theorem 1.** *There are infinitely many non-abelian finite simple groups $G$ with $\gamma_u(G) = 2$. For example, $\gamma_u(A_n) = 2$ for every prime number $n \geqslant 13$.*

Next we present results for alternating, sporadic and groups of Lie type, in turn. Our main result for alternating groups is the following (see Theorem 3.7 for a more detailed statement).

**Theorem 2.** *There exists an absolute constant $c$ such that*

$$\gamma_u(A_n) \leqslant c(\log_2 n)$$

*for all $n \geqslant 5$. In particular, if $n \geqslant 6$ is even, then*

$$\lceil \log_2 n \rceil - 1 \leqslant \gamma_u(A_n) \leqslant 2\lceil \log_2 n \rceil.$$

**Remark 1.** Notice that if $n$ is even then Theorem 2 gives the exact value of $\gamma_u(A_n)$, up to a small constant. It is also worth noting that the uniform domination number of an alternating group can be arbitrarily large. The analysis of odd degree alternating groups is more difficult and our best estimate is $\gamma_u(A_n) \leqslant 77 \log_2 n$ (see Proposition 3.15).

We can compute precise results for sporadic simple groups; a simplified version of our main result (Theorem 4.2) is as follows.

**Theorem 3.** *Let $G$ be a sporadic simple group. Then $\gamma_u(G) \leqslant 4$, with equality if $G = \mathrm{M}_{11}$ or $\mathrm{M}_{12}$.*

Finally, we present a version of our main result for simple groups of Lie type (see Theorems 5.2 and 6.3 for more detailed results). In the statement, $r$ is the untwisted Lie rank of $G$ (that is, $r$ is the rank of the ambient simple algebraic group).

**Theorem 4.** *Let $G$ be a finite simple group of Lie type of rank $r$.*

(i) *If $G = \mathrm{L}_2(q)$, then $\gamma_u(G) \leqslant 4$, with equality if and only if $q = 9$.*
(ii) *If $G$ is an exceptional group of Lie type, then $\gamma_u(G) \leqslant 6$.*
(iii) *If $G$ is a classical group, then $\gamma_u(G) \leqslant 7r + 56$.*

**Remark 2.** Let us make some comments on the statement of Theorem 4.

(a) The upper bound in part (ii) can be improved for some families of exceptional groups. For instance, by Theorem 5.2, $\gamma_u(G) = 2$ if $G \in \{{}^2B_2(q), {}^2G_2(q), E_8(q)\}$.
(b) We refer the reader to Theorem 6.3 for a more detailed version of part (iii), which provides stronger bounds in some special cases. For example, if $G$ is a symplectic group in even characteristic, or an odd dimensional orthogonal group, then

$$r \leqslant \gamma_u(G) \leqslant 7r$$

and thus the linear bound in (iii) is essentially best possible (up to constants). In other cases, we can establish a constant bound. For instance, if $G = \mathrm{U}_{r+1}(q)$ and $r \geqslant 7$ is odd, then $\gamma_u(G) \leqslant 15$.

Let us briefly describe some of the main ideas in the proofs of Theorems 1–4. Following Guralnick and Kantor [24] in their work on the uniform spread of simple groups, we develop a probabilistic approach to study the uniform domination number. Let $G$ be a finite group and fix an element $s \in G^{\#}$. Write $\mathcal{M}(G, s)$ for the set of maximal subgroups of $G$ containing $s$. For an element $x \in G$ and subgroup $H < G$, let $\mathrm{fpr}(x, G/H)$ be the *fixed point ratio* of $x$ for the action of $G$ on the set of cosets $G/H$. For a positive integer $c$, let $Q(G, s, c)$ be the probability that a randomly chosen $c$-tuple of conjugates of $s$ is *not* a total dominating set for $\Gamma(G)$. Clearly, if $Q(G, s, c) < 1$ for some $s \in G^{\#}$ then $\gamma_u(G) \leqslant c$, so we are interested in bounding $Q(G, s, c)$ from above.

Here the key tool is Lemma 2.5, which states that

$$Q(G,s,c) \leqslant \sum_{i=1}^{k} |x_i^G| \left( \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x_i, G/H) \right)^c =: \widehat{Q}(G,s,c),$$

where $\{x_1, \ldots, x_k\}$ is a set of representatives of the conjugacy classes in $G$ of prime order elements. To apply this result, the first step is to identify an element $s \in G^{\#}$ that is contained in very few maximal subgroups of $G$. We then need to determine the specific subgroups in $\mathcal{M}(G,s)$ and compute upper bounds for the relevant fixed point ratios. Here we can appeal to the extensive literature on fixed point ratios for simple groups. For example, if $G$ is a simple group of Lie type over $\mathbb{F}_q$ and $H$ is a maximal subgroup of $G$, then a well known theorem of Liebeck and Saxl [38, Theorem 1] implies that $\mathrm{fpr}(x, G/H) \leqslant 4/3q$ for all $x \in G^{\#}$, with a short list of known exceptions. Stronger bounds are established in [12] (for non-subspace actions of classical groups), [24, Section 3] (subspace actions) and [36] (exceptional groups).

In the special case where there is an element $s \in G^{\#}$ with $\mathcal{M}(G,s) = \{H\}$ and $H$ is core-free, it is easy to see that $\gamma_u(G) \leqslant b$, where $b = b(G, G/H)$ is the *base size* of $G$ with respect to the action on $G/H$ (that is, $b$ is the minimal size of a subset of $G/H$ with trivial pointwise stabiliser). This observation provides an important connection between the uniform domination number of $G$ and the base sizes of primitive permutation representations of $G$. Bases for primitive groups have been a topic of interest in group theory since the nineteenth century, with a wide range of applications. In particular, strong upper bounds on the base sizes of primitive almost simple groups have recently been established (see [14, 17, 19, 20, 29] for example), and in many cases we can apply these results to bound the uniform domination number. For example, Halasi's results [29] on the base size for the action of a symmetric group on $k$-sets are a key ingredient in the proof of the bounds in Theorem 2 for even degree alternating groups.

**Remark 3.** In many cases, our probabilistic approach also yields strong asymptotic results. Indeed, if $\widehat{Q}(G,s,c) \to 0$ as $|G| \to \infty$, then almost every $c$-tuple of conjugates of $s$ is a total dominating set for $\Gamma(G)$. For instance, suppose $G$ is an exceptional group of Lie type, in which case Theorem 4(ii) gives $\gamma_u(G) \leqslant 6$. By combining the proof of Theorem 5.2 with [19, Theorem 2], we deduce that there is an element $s \in G$ such that the probability that 6 randomly chosen conjugates of $s$ form a total dominating set for $\Gamma(G)$ tends to 1 as $|G| \to \infty$.

As noted above, in order to effectively apply the probabilistic approach, we need to find an element $s \in G^{\#}$ that is contained in a small number of maximal subgroups of $G$. In this way, it is natural to consider the parameter

$$\mu(G) = \min_{s \in G} |\mathcal{M}(G,s)|.$$

We establish the following result for simple groups.

**Theorem 5.** *If $G$ is a finite simple group, then either $\mu(G) \leqslant 3$ or $(G, \mu(G))$ is one of the following:*

| $G$ | $\mathrm{U}_6(2)$ | $\mathrm{U}_4(3)$ | $\Omega_8^+(2)$ | $\mathrm{P}\Omega_8^+(3)$ |
|---|---|---|---|---|
| $\mu(G)$ | 4 | 5 | 7 | 7 |

*In particular, $\mu(G) \leqslant 7$ for every finite simple group $G$.*

In fact, we can compute the exact value of $\mu(G)$ for any alternating or sporadic group $G$ (see Theorems 3.1 and 4.1), and it is worth noting that there are infinitely many alternating groups $G$ with $\mu(G) = 3$. The result for alternating and classical groups is essentially a corollary of the proof of the main theorem of Guralnick and Kantor [24], which identifies an explicit element that is contained in very few maximal subgroups (typically, this is a

regular semisimple element when $G$ is a classical group). Finally, we appeal to earlier work of Weigel [46], which shows that almost every finite simple exceptional group of Lie type has an element that is contained in a unique maximal subgroup.

Our notation is standard. We adopt the notation from [35] for simple groups, so we write $\mathrm{L}_n(q) = \mathrm{PSL}_n(q)$ and $\mathrm{U}_n(q) = \mathrm{PSU}_n(q)$ for linear and unitary groups, and $\mathrm{P}\Omega^{\varepsilon}_n(q)$ is a simple orthogonal group, etc. In addition, we will write $(a_1, \ldots, a_k)$ for the greatest common divisor of a collection of positive integers $a_1, \ldots, a_k$.

## 2. Methods

In this section we introduce some of the main tools that will be needed in the proofs of Theorems 1–5. First, in Section 2.1, we establish an important connection between the uniform domination number and base sizes. Our probabilistic approach to bounding the uniform domination number, based on fixed point ratio estimates, is presented in Section 2.2; here the main result is Lemma 2.5. Finally, in Section 2.3, we outline some of the computational methods that we will employ.

### 2.1. Bases.

Let $G$ be a finite group with generating graph $\Gamma(G)$. Recall that a subset $S \subseteq G^{\#}$ is a *total dominating set* (TDS for short) for $\Gamma(G)$ if for all $g \in G^{\#}$ there exists $s \in S$ such that $G = \langle g, s\rangle$. For any $g \in G$, write $\mathcal{M}(G, g)$ for the set of maximal subgroups of $G$ containing $g$.

**Lemma 2.1.** *A subset $\{s_1, \ldots, s_c\} \subseteq G^{\#}$ is a total dominating set for $\Gamma(G)$ if and only if*

$$\bigcap_{i=1}^{c} H_i = 1$$

*for all $(H_1, \ldots, H_c) \in \prod_{i=1}^{c} \mathcal{M}(G, s_i)$.*

*Proof.* Let $S = \{s_1, \ldots, s_c\}$. By definition, $S$ is not a total dominating set if and only if there exists $g \in G^{\#}$ such that $G \neq \langle g, s_i\rangle$ for all $i$; that is, for each $i$, $g$ is contained a maximal subgroup of $G$ containing $s_i$. So $S$ is not a total dominating set if and only if there exists $(H_1, \ldots, H_c) \in \prod_i \mathcal{M}(G, s_i)$ such that $\bigcap_i H_i \neq 1$. The result follows. □

Let $G$ be a group acting faithfully on a finite set $\Omega$. Recall that a subset $B \subseteq \Omega$ is a *base* if the pointwise stabiliser of $B$ in $G$ is trivial. Write $b(G, \Omega)$ for the minimal size of a base for the action of $G$ on $\Omega$. Note that if $G$ is transitive on $\Omega$ and $H$ is a point stabiliser, then $b(G, \Omega) \leqslant c$ if and only if there exist $g_1, \ldots, g_c \in G$ such that

$$\bigcap_{i=1}^{c} H^{g_i} = 1.$$

Let us also observe that

$$b(G, \Omega) \geqslant \frac{\log |G|}{\log |\Omega|}. \tag{2.1}$$

**Corollary 2.2.** *Suppose there is an element $s \in G$ such that $\mathcal{M}(G, s) = \{H\}$ and $H$ is core-free. Then $b(G, G/H)$ is the minimal size of a total dominating set for $\Gamma(G)$ containing only conjugates of $s$.*

*Proof.* Let $c$ be a positive integer. As noted above, $b(G, G/H) \leqslant c$ if and only if there exist $g_1, \ldots, g_c \in G$ such that $\bigcap_i H^{g_i} = 1$. Since $\mathcal{M}(G, s^{g_i}) = \{H^{g_i}\}$ for each $i$, the result follows from Lemma 2.1. □

This corollary connects the study of base sizes for primitive permutation groups to the existence of total dominating sets comprising conjugate elements. In particular, it leads us naturally to the notion of the *uniform domination number* $\gamma_u(G)$ of $G$ introduced in

Section 1, which is our main focus in this paper. Recall that this is defined to be the minimal number of conjugate elements that form a total dominating set for $\Gamma(G)$.

The main goal of this paper is to study $\gamma_u(G)$ for finite simple groups $G$. (By the main theorem of [24], simple groups have uniform spread 1 and thus $\gamma_u(G)$ is well-defined.) Of course, in this situation every proper subgroup of $G$ is core-free and so we are in a position to apply Corollary 2.2. Indeed, if we can identify an element $s \in G$ with $\mathcal{M}(G,s) = \{H\}$ then $\gamma_u(G) \leqslant b(G, G/H)$ and we can appeal to the extensive literature on bases for simple groups, which is a topic that has seen a great deal of activity in recent years (see [14, 17, 19, 20, 29], for example). In the next section, we will develop a probabilistic approach which can be used to obtain upper bounds on $\gamma_u(G)$ in the general case where we have an element $s \in G$ that is contained in several maximal subgroups.

We conclude this section by recording a result which allows us to exploit information on base sizes to determine lower bounds on $\gamma_u(G)$.

**Corollary 2.3.** *Let $s \in G^{\#}$ and let $H \in \mathcal{M}(G,s)$ with $b(G,G/H) = b$. Then any total dominating set for $\Gamma(G)$ containing only conjugates of $s$ has size at least $b$.*

*Proof.* Let $\{s^{g_1}, \ldots, s^{g_c}\}$ be a total dominating set for $\Gamma(G)$. Then $H^{g_i} \in \mathcal{M}(G, s^{g_i})$ for all $i$. Therefore, Lemma 2.1 implies that $\bigcap_i H^{g_i} = 1$ and thus $b \leqslant c$. □

**Remark 2.4.** We can use Corollary 2.3 to derive lower bounds on $\gamma_u(G)$. Indeed, if there is a positive integer $c$ such that for each $s \in G^{\#}$ there exists $H \in \mathcal{M}(G,s)$ with $b(G,G/H) \geqslant c$, then $\gamma_u(G) \geqslant c$. Of course, one only needs to check this condition on $s$ for a set of conjugacy class representatives. In fact, it suffices only to check for a set $\{g_1, \ldots, g_m\}$ of class representatives with the property that for all $x \in G^{\#}$ there exists $y \in g_1^G \cup \cdots \cup g_m^G$ such that $x = y^{\ell}$ for some integer $\ell$.

2.2. **Probabilistic methods.** In [41], Liebeck and Shalev introduced a probabilistic approach for studying the base size of a finite transitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$. The basic idea is to consider the probability that a randomly chosen $c$-tuple of points in $\Omega$ is *not* a base for $G$ and then show that this probability is strictly less than 1 for some appropriate positive integer $c$; this immediately implies that $b(G,\Omega) \leqslant c$. This has proven to be an effective way of establishing accurate (upper) bounds on the base size of almost simple primitive permutation groups; indeed, this is the main tool in the proof of an influential conjecture of Cameron on the base size of so-called *non-standard* primitive groups (see [19] and the references therein). Here our goal is to develop a similar approach to study the uniform domination number of simple groups.

Let $G$ be a finite group, let $c$ be a positive integer and fix an element $s \in G^{\#}$. Write $Q(G,s,c)$ for the probability that a random $c$-tuple $(z_1, \ldots, z_c)$ of conjugates of $s$ is such that $\{z_1, \ldots, z_c\}$ is *not* a total dominating set for $\Gamma(G)$. Consequently, $\gamma_u(G) \leqslant c$ if $Q(G,s,c) < 1$ for some $s$. In order to present an upper bound for $Q(G,s,c)$, we need some additional notation. For an element $x \in G$ and a subgroup $H < G$, let

$$\mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|} \tag{2.2}$$

be the *fixed point ratio* of $x$ in the action of $G$ on the set of cosets $G/H$; that is, $\mathrm{fpr}(x,G/H)$ is the proportion of points in $G/H$ fixed by $x$ (equivalently, it is the probability that a randomly chosen coset of $H$ is fixed by $x$). Let $\{x_1, \ldots, x_k\}$ be a set of representatives of the conjugacy classes in $G$ of prime order elements.

We can now present our key lemma for studying uniform domination numbers.

**Lemma 2.5.** *Let $G$ be a finite group, $s \in G^{\#}$ and $c \in \mathbb{N}$. Then*

$$Q(G,s,c) \leqslant \sum_{i=1}^{k} |x_i^G| \left( \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x_i, G/H) \right)^c =: \widehat{Q}(G,s,c). \tag{2.3}$$

*Proof.* Let $\mathcal{P}$ be the set of elements in $G$ of prime order. For each $x \in G$, let

$$P(x,s) = \frac{|\{z \in s^G \,:\, G \neq \langle x, z\rangle\}|}{|s^G|} = \frac{|\{g \in G \,:\, G \neq \langle x, s^g\rangle\}|}{|G|}$$

be the probability that a randomly chosen conjugate of $s$ does not generate $G$ with $x$. Since $G \neq \langle x, s^g\rangle$ if and only if $x^{g^{-1}} \in H$ for some $H \in \mathcal{M}(G,s)$, it follows that

$$P(x,s) \leqslant \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|\,|C_G(x)|}{|G|} = \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H).$$

Now $\{s^{g_1}, \ldots, s^{g_c}\}$ is not a total dominating set for $\Gamma(G)$ if and only if there exists $x \in \mathcal{P}$ such that $G \neq \langle x, s^{g_i}\rangle$ for all $i$. Therefore,

$$Q(G,s,c) \leqslant \sum_{x \in \mathcal{P}} P(x,s)^c = \sum_{i=1}^{k} |x_i^G|\, P(x_i,s)^c \tag{2.4}$$

and the result follows. □

**Remark 2.6.** Note that if $\mathcal{M}(G,s) = \{H\}$, then the probabilistic approach via Lemma 2.5 coincides with the method introduced by Liebeck and Shalev in [41] to study the base size $b(G, G/H)$. Accordingly, Lemma 2.5 gives no more information than Corollary 2.2 in this case. However, the utility of Lemma 2.5 is that it allows us to handle groups for which every element belongs to at least two maximal subgroups.

The following elementary observation is a natural extension of [19, Proposition 2.3].

**Lemma 2.7.** *Let $G$ be a finite group and let $\{H_1, \ldots, H_\ell\}$ be proper subgroups of $G$. Suppose that $x_1, \ldots, x_m$ represent distinct $G$-classes such that $\sum_i |x_i^G \cap H_j| \leqslant A_j$ and $|x_i^G| \geqslant B$ for all $i, j$. Then*

$$\sum_{i=1}^{m} |x_i^G| \left( \sum_{j=1}^{\ell} \mathrm{fpr}(x_i, G/H_j) \right)^c \leqslant B^{1-c} \left( \sum_j A_j \right)^c$$

*for all $c \in \mathbb{N}$.*

*Proof.* Write $a_{ij} = |x_i^G \cap H_j|$ and $b_i = |x_i^G|$, so $\sum_i a_{ij} \leqslant A_j$ and $b_i \geqslant B$. Then the left hand side of the required inequality is

$$\sum_i b_i \left( \sum_j a_{ij}/b_i \right)^c = \sum_i b_i^{1-c} \left( \sum_j a_{ij} \right)^c \leqslant B^{1-c} \sum_i \left( \sum_j a_{ij} \right)^c \leqslant B^{1-c} \left( \sum_{i,j} a_{ij} \right)^c$$

and the result follows. □

It is natural to expect that the upper bound in (2.3) will be easier to compute if we can find an element $s \in G$ such that $|\mathcal{M}(G,s)|$ is small. With this in mind, it is interesting to study the following parameter

$$\mu(G) = \min_{s \in G} |\mathcal{M}(G,s)|, \tag{2.5}$$

which we introduced in Section 1. Our main result is Theorem 5, which reveals that every finite simple group has an element that is contained in very few maximal subgroups (at most 3 in fact, apart from 4 specific exceptions).

2.3. **Computational methods.** For some small simple groups $G$, we can use computational methods, implemented in GAP [23] and Magma [6], to study $\mu(G)$ and $\gamma_u(G)$. For example, all of our results for sporadic groups (see Section 4) are obtained by computation. Here we outline the main techniques.

A detailed description of these computations can be found at [18], including the relevant GAP and Magma code we used to obtain the results.

2.3.1. *Probabilistic methods.* Let us first describe an implementation of the probabilistic method introduced in Section 2.2. Let $G$ be a finite group and fix an element $s \in G^{\#}$. Our aim is to determine the minimal value of $c$ such that $\widehat{Q}(G,s,c) < 1$ (see Lemma 2.5). In order to calculate $\widehat{Q}(G,s,c)$ we first need to determine $\mathcal{M}(G,s)$, and then calculate the fixed point ratios $\mathrm{fpr}(x,G/H)$ for each prime order element $x \in G$ and subgroup $H \in \mathcal{M}(G,s)$. If such a subgroup $H$ is self-normalising, then $s$ is contained in exactly

$$\mathrm{fpr}(s,G/H) \cdot |G:H|$$

distinct conjugates of $H$. Therefore, if $G$ is simple then in order to determine $\mathcal{M}(G,s)$ it suffices to compute $\mathrm{fpr}(s,G/H)$ for a representative $H$ of each conjugacy class of maximal subgroups of $G$. Hence, we focus on determining the fixed point ratios $\mathrm{fpr}(x,G/H)$ for elements $x \in G$ and maximal subgroups $H < G$. Of course, this approach via GAP and Magma is only feasible if $G$ is amenable to computational methods, which typically means that the order of $G$, or the minimal degree of a faithful permutation representation, is not too large.

If the Character Table Library [8] in GAP contains the ordinary character tables of $G$ and each of its maximal subgroups, then we can adopt the techniques of Breuer, which are detailed in [9, Section 3.2]. Indeed, in this situation we can compute $\mathrm{fpr}(x,G/H)$ by observing that the number of fixed points of $x$ on $G/H$ is equal to $\chi(x)$, where $\chi = 1_H^G$ is the corresponding permutation character. If this character-theoretic approach is not available, then we turn to Magma. If the functions `MaximalSubgroups` and `Classes` return the maximal subgroups and conjugacy classes of $G$, then we can calculate $\mathrm{fpr}(x,G/H)$ via (2.2), using `IsConjugate` to compute $|x^G \cap H|$.

2.3.2. *Maximal subgroups.* We can often use the above methods to determine the maximal overgroups of a specific element of $G$, which allows us to determine $\mu(G)$ in this way. In addition, by determining $\mathcal{M}(G,s)$ for a complete set of conjugacy class representatives $s$, we can apply the observations in Remark 2.4 to derive a lower bound on $\gamma_u(G)$.

2.3.3. *Random and exhaustive searches.* Let $c \geqslant 2$ be an integer and fix $s \in G^{\#}$. If we have a faithful permutation representation of $G$, which permits calculation in Magma, then we can randomly choose $c$-tuples of conjugates of $s$ and check whether they form a TDS for $\Gamma(G)$. Of course, if we find such a $c$-tuple, then $\gamma_u(G) \leqslant c$. In contrast, to establish the bound $\gamma_u(G) > c$ we must show that for each conjugacy class $s^G$, there are no $c$-tuples of conjugates of $s$ which form a TDS. Here it is helpful to observe that if there is such a $c$-tuple, then there is one containing $s$. Therefore, when trying to verify upper (or lower) bounds on $\gamma_u(G)$ we may randomly (or exhaustively) choose $(c-1)$-tuples of elements in $s^G$ and check whether they, together with $s$, form a TDS for $\Gamma(G)$.

**Remark 2.8.** Let us say a few words on the computational resources needed for the main calculations. For the computations in this paper, we use a combination of GAP Version 4.5.6 and Magma 2.19-2, on a 2.7GHz machine with 128 GB RAM. The character-theoretic computations run quickly in GAP and we adopt this approach whenever possible. The computations in Magma for determining maximal overgroups of specific elements and implementing the probabilistic approach (via fixed point ratios) are more resource-intensive, but still feasible for the groups we are interested in. For example, an implementation of the probabilistic method applied to $\mathrm{L}_9(2)$ with an element of order 465 (see Proposition 6.14) can be done in 616 seconds, using 771 MB of memory. Similar resources are needed for most of the exhaustive searches in Magma, which we use to rule out the existence of total domination sets with prescribed properties. However, the verification of the bound $\gamma_u(\mathrm{M}_{12}) \geqslant 4$ is a notable exception. Here, in view of Corollary 2.3 and the base size results in [20], we quickly reduce the problem to showing that no triple of elements in the class

6A form a TDS for $\Gamma(\mathrm{M}_{12})$. We timed this computation at 17613 seconds, using 13 MB of memory.

For the remainder of the paper we will focus on the proofs of Theorems 1–5, by considering each family of (non-abelian) simple groups $G$ in turn. In each case, we first study the parameter $\mu(G)$ defined in (2.5), with the aim of establishing a strong form of Theorem 5. We then establish our main results on the uniform domination number of $G$.

## 3. Alternating groups

3.1. **Maximal overgroups.** In this section we verify Theorem 5 for alternating groups. More precisely, we compute the exact value of $\mu(G)$ for each simple alternating group $G$. In order to state our main result, let

$$\mathcal{H} = \left\{ n \in \mathbb{N} \,:\, n = \tfrac{q^d-1}{q-1} \text{ for some prime power } q \text{ and integer } d \geqslant 2 \right\}. \tag{3.1}$$

We refer the reader to [4, Table II] for a convenient list of the first 240 primes in $\mathcal{H}$.

**Theorem 3.1.** *Let $G = A_n$ with $n \geqslant 5$. Then $\mu(G) \leqslant 3$. Moreover,*

(i) *$\mu(G) = 1$ if and only if one of the following hold:*
   (a) *$n = 5$;*
   (b) *$n \geqslant 8$ is even;*
   (c) *$n \in \{r, r^2\}$, where $r$ is a prime, $n \notin \{11, 23\}$ and $n \notin \mathcal{H}$.*

(ii) *$\mu(G) = 2$ if and only if one of the following hold:*
   (a) *$n \in \{6, 7, 11, 17, 23\}$;*
   (b) *$n \in \{rs, r^3\}$, where $r, s$ are distinct odd primes and $n \notin \mathcal{H}$.*

*In particular, Theorem 5 holds for alternating groups.*

The proof of Theorem 3.1 closely follows the proof of [24, Proposition 7.1], which identifies an element $g \in G$ that is contained in very few maximal subgroups. Indeed, the bound $\mu(G) \leqslant 3$ is an immediate corollary of the proof of [24, Proposition 7.1] (with a small correction when $n$ is an odd integer of the form $3m$) but more work is needed to compute the exact value in every case.

**Remark 3.2.** There are infinitely many primes $r$ with $\mu(A_r) = 1$. To see this, we need to show that there are infinitely many prime numbers that are not contained in $\mathcal{H}$. For a real number $x$, let $\pi(x)$ be the number of primes less than or equal to $x$, and let $H(x)$ be the number of primes at most $x$ in $\mathcal{H}$. By the prime number theorem, we have $\pi(x) = (1 + o(1))x(\log x)^{-1}$, whereas [4, Theorem 4] gives $H(x) \leqslant 50x^{1/2}(\log x)^{-2}$ for $x \gg 0$. In other words, if $x$ is large enough then almost all primes at most $x$ are not in $\mathcal{H}$.

In order to prove Theorem 3.1, we need to record some preliminary lemmas. The first follows from the main theorem in [37].

**Lemma 3.3.** *Let $G = A_n$ with $n \geqslant 5$ and let $H$ be an intransitive subgroup of the form $(S_k \times S_{n-k}) \cap G$ with $k < n/2$, or an imprimitive subgroup $(S_k \wr S_{n/k}) \cap G$ with $1 < k \leqslant n/2$. Then $H$ is a maximal subgroup of $G$ unless $G = A_8$ and $H = (S_2 \wr S_4) \cap G$.*

We denote the shape of a permutation $g \in S_n$ by writing $[l_1, \ldots, l_t]$ with $\sum_i l_i = n$, where the $l_i$ are the lengths of the disjoint cycles comprising $g$ (in addition, if $g$ has $b_i$ cycles of length $a_i$, where $a_1 > a_2 > \cdots > a_k$, then it will be convenient to write $[a_1^{b_1}, \ldots, a_k^{b_k}]$ for the shape of $g$). The next result concerns the containment of certain elements in imprimitive subgroups; the proof is a straightforward application of [1, Theorem 2.5].

**Lemma 3.4.** *Let $G = S_n$, with $n \geqslant 5$, and let $g \in G$.*

(i) *If $g$ is an $n$-cycle, then $g$ is not contained in an imprimitive subgroup of $G$ if and only if $n$ is a prime. Moreover, if $n = mk$ with $m, k > 1$, then $g$ is contained in a unique subgroup $S_m \wr S_k$.*

(ii) *If $g$ has shape $[l_1, l_2]$, then $g$ is not contained in an imprimitive subgroup of $G$ if and only if $(l_1, l_2) = 1$.*

(iii) *If $g$ has shape $[l_1, l_2, l_3]$, then $g$ is not contained in an imprimitive subgroup of $G$ if and only if $(l_1, l_2, l_3) = 1$, and if $d$ divides $(l_i, l_j)$ then $\frac{l_i+l_j}{d}$ does not divide $l_k$, where $\{i, j, k\} = \{1, 2, 3\}$.*

The following lemma is a classical result of Marggraf (see [47, Theorem 13.5]).

**Lemma 3.5.** *If a primitive subgroup $H \leqslant S_n$ contains a cycle of length $\ell < n/2$, then $H = A_n$ or $S_n$.*

We will also need the following technical result.

**Lemma 3.6.** *Let $G = A_n$, where $n \geqslant 7$ is odd. Suppose $n = (q^d - 1)/(q - 1)$, where $d \geqslant 2$ and $q = p^f$ for a prime $p$. Let $g \in G$ be an $n$-cycle and let $N$ be the number of subgroups of $G$ of the form $\mathrm{P\Gamma L}_d(q) \cap G$ containing $g$. Then*

$$\frac{\varphi(n)}{2df} \leqslant N \leqslant \frac{\varphi(n)}{d},$$

*where $\varphi$ is Euler's totient function.*

*Proof.* For $n \in \{7, 9\}$, it is easy to check that $N = \varphi(n)/d$, so we may assume $n > 9$. Fix a subgroup $H = \mathrm{P\Gamma L}_d(q) \cap G$ containing $g$ and let $k$ be the number of $G$-conjugates of $H$ containing $g$, so

$$k = \mathrm{fpr}(g, G/H) \cdot |G : H| = \frac{|g^G \cap H|}{|g^G|} \cdot |G : H|.$$

Since $C_G(g) = C_H(g) = \langle g \rangle$, it follows that $k$ is the number of $H$-classes in $g^G \cap H$.

By [33, Theorem 1], every $n$-cycle in $H$ generates a Singer subgroup of $\mathrm{PGL}_d(q)$ and thus $H$ contains $\varphi(n)/d$ distinct $\mathrm{PGL}_d(q)$-classes of $n$-cycles. Since only half of these classes are contained in $g^G$, we get $k \leqslant \varphi(n)/2d$. By considering the fusing action of field automorphisms in $\mathrm{P\Gamma L}_d(q)$ on $\mathrm{PGL}_d(q)$-classes, we also deduce that $k \geqslant \varphi(n)/2df$. Finally, we note that $S_n$ has a unique class of subgroups of the form $\mathrm{P\Gamma L}_d(q)$ (the corresponding actions of $\mathrm{P\Gamma L}_d(q)$ on lines and hyperplanes in $\mathbb{F}_q^d$ are permutation isomorphic), so $G$ contains at most two conjugacy classes of subgroups of the form $\mathrm{P\Gamma L}_d(q) \cap G$. We conclude that $N \leqslant 2k \leqslant \varphi(n)/d$. □

We are now ready to prove Theorem 3.1.

*Proof of Theorem 3.1.* First assume $n$ is even. If $n = 6$, then it is easy to check that $\mu(G) = 2$; in particular, if $g \in G$ is a 5-cycle then $\mathcal{M}(G, g) = \{H, K\}$ with $H \cong K \cong A_5$. Now assume $n \geqslant 8$. We claim that $\mu(G) = 1$. To see this, write $n = 2m$, $k = m - (m - 1, 2)$ and choose an element $g \in G$ with shape $[k, n - k]$. The unique intransitive subgroup in $\mathcal{M}(G, g)$ has the form $(S_k \times S_{n-k}) \cap G$, and imprimitive groups are ruled out by Lemma 3.4(ii) since $(k, n - k) = 1$. Furthermore, Lemma 3.5 eliminates primitive subgroups since $g^{n-k}$ is a $k$-cycle and $k < n/2$. Therefore, $\mathcal{M}(G, g) = \{H\}$ with $H = (S_k \times S_{n-k}) \cap G$.

For the remainder, we may assume $n$ is odd. If $n \leqslant 23$ then we verify the result computationally in Magma (see Section 2.3.1). In particular, the value of $\mu(G)$ and the shape of an element $g$ for which $|\mathcal{M}(G, g)| = \mu(G)$ are as follows:

| $n$ | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\mu(G)$ | 1 | 2 | 3 | 2 | 3 | 3 | 2 | 1 | 3 | 2 |
| $g$ | [5] | [7] | $[5, 2^2]$ | [11] | $[9, 2^2]$ | $[11, 2^2]$ | [17] | [19] | $[17, 2^2]$ | [23] |

Now assume $n \geqslant 25$ is odd. Our goal is to establish the following five statements:

(1) $\mu(G) \leqslant 3$.
(2) If $n \in \{r, r^2\}$, where $r$ is a prime and $n \notin \mathcal{H}$, then $\mu(G) = 1$.
(3) If $n \in \{rs, r^3\}$, where $r, s$ are distinct primes and $n \notin \mathcal{H}$, then $\mu(G) \leqslant 2$.
(4) If $\mu(G) \leqslant 2$ then $n \notin \mathcal{H}$ and $n \in \{r, r^2, r^3, rs\}$ for distinct primes $r, s$.
(5) If $n \in \{rs, r^3\}$, where $r, s$ are distinct primes, then $\mu(G) \geqslant 2$.

Indeed, observe that (1)–(5) complete the proof of Theorem 3.1. More precisely, (1) gives the main statement of the theorem, (2) completes the reverse implication in part (i), (3) gives the reverse implication of (ii), and by combining (2), (4) and (5) we obtain the forward implications in parts (i) and (ii).

First consider (1). Let $g \in G$ be an element with the following shape:

$$\begin{cases} [m+2, m, m-2] & \text{if } n = 3m \\ [m+1, m+1, m-1] & \text{if } n = 3m+1 \\ [m+2, m, m] & \text{if } n = 3m+2. \end{cases} \tag{3.2}$$

By applying Lemma 3.4(iii), we deduce that $g$ does not have any imprimitive maximal overgroups. For example, if $n = 3m+1$ then $m$ is even so $(m+1, m-1) = 1$. Moreover, $(m+1+m-1)/1 = 2m$ does not divide $m+1$, and $(m+1+m+1)/(m+1) = 2$ does not divide $m-1$. The other two cases are similar. As before, primitive maximal overgroups can be ruled out via Lemma 3.5 and we conclude that $\mu(G) \leqslant 3$ as claimed.

Now consider (2), so $n \in \{r, r^2\}$ and $n \notin \mathcal{H}$ for a prime $r$. Let $g \in G$ be an $n$-cycle and note that $g$ is not contained in an intransitive subgroup. Suppose $n = r$. By Lemma 3.4(i), $g$ is not contained in an imprimitive subgroup. Moreover, [33, Theorem 3] implies that $\mathrm{AGL}_1(r) \cap G$ is the only primitive maximal overgroup of $g$, so $\mu(G) = 1$ as required. Similarly, if $n = r^2$ then by applying [33, Theorem 3] to rule out primitive groups we deduce that $g$ is contained in a unique imprimitive subgroup $(S_r \wr S_r) \cap G$, so $\mu(G) = 1$ once again.

Next consider (3) and let $g$ be an $n$-cycle. As before, by applying [33, Theorem 3], we deduce that the maximal overgroups of $g$ are imprimitive. More precisely,

$$\mathcal{M}(G, g) = \begin{cases} \{(S_r \wr S_s) \cap G, (S_s \wr S_r) \cap G\} & \text{if } n = rs \\ \{(S_r \wr S_{r^2}) \cap G, (S_{r^2} \wr S_r) \cap G\} & \text{if } n = r^3 \end{cases}$$

and thus $\mu(G) \leqslant 2$.

Let us now turn to (4). Suppose that $\mu(G) \leqslant 2$ and fix $g \in G$ with $|\mathcal{M}(G, g)| = \mu(G)$. Since $g$ is even and $n$ is odd, $g$ is not the product of exactly two cycles. If $g$ has at least three cycles, then $\mathcal{M}(G, g)$ contains at least three intransitive subgroups, so $g$ must be an $n$-cycle. If $n$ has at least three distinct prime divisors, or if $n = r^2 s$ for distinct primes $r, s$, then Lemma 3.4(i) implies that $\mathcal{M}(G, g)$ contains at least three imprimitive subgroups. Therefore, $n \in \{r, r^2, r^3, rs\}$, where $r, s$ are distinct primes, and it remains to prove that $n \notin \mathcal{H}$. If $n \in \{r^3, rs\}$, then $g$ is already contained in two imprimitive subgroups, so the condition $\mu(G) \leqslant 2$ implies that $g$ is not contained in a proper primitive subgroup, whence $n \notin \mathcal{H}$ by [33, Theorem 3]. The cases $n \in \{r, r^2\}$ require special attention.

First assume $n = r$. Seeking a contradiction, suppose that $n \in \mathcal{H}$. By [33, Theorem 3], $\mathcal{M}(G, g)$ contains a unique subgroup of the form $\mathrm{AGL}_1(r) \cap G$ (namely, $N_G(\langle g \rangle)$), together with a collection of subgroups $\mathrm{P\Gamma L}_d(q)$ for each prime power $q$ and integer $d \geqslant 2$ such that $n = (q^d - 1)/(q-1)$. More precisely, for each $(q, d)$ with $q = p^f$ and $p$ a prime, Lemma 3.6 implies that $g$ is contained in at least $(n-1)/2df$ such subgroups. Since $n \geqslant 25$, one can check that this gives $|\mathcal{M}(G, g)| > 2$ and we have reached a contradiction. A similar argument applies if $n = r^2 \in \mathcal{H}$. Indeed, $\mathcal{M}(G, g)$ contains a unique subgroup of the form $(S_r \wr S_r) \cap G$ and at least two primitive subgroups $\mathrm{P\Gamma L}_d(q) \cap G$. Once again, this is a contradiction and the proof of (4) is complete.

Finally, let us consider (5), so $n \in \{rs, r^3\}$ for distinct primes $r$ and $s$. Fix an element $1 \neq g \in G$. If $g$ is not an $n$-cycle then the argument in (4) shows that $g$ is contained in at least three intransitive maximal subgroups. On the other hand, if $g$ is an $n$-cycle then the proof of (3) implies that $g$ is contained in at least two imprimitive subgroups. Therefore, $|\mathcal{M}(G,g)| \geqslant 2$ and thus $\mu(G) \geqslant 2$. □

3.2. **Uniform domination number.** We now apply Theorem 3.1 to study the uniform domination number of alternating groups. Our main result is the following.

**Theorem 3.7.** *We have $\gamma_u(A_n) \leqslant 77 \log_2 n$ for all $n \geqslant 5$. More precisely, the following hold:*

(i) *If $n \geqslant 13$ is a prime, then $\gamma_u(A_n) = 2$.*
(ii) *If $n \geqslant 6$ is even, then $\lceil \log_2 n \rceil - 1 \leqslant \gamma_u(A_n) \leqslant 2\lceil \log_2 n \rceil$.*

We partition the proof of Theorem 3.7 into three propositions which are proved in the following three sections.

3.2.1. *Prime degree.* We start by considering alternating groups of prime degree.

**Proposition 3.8.** *Let $r \geqslant 13$ be a prime number. Then $\gamma_u(A_r) = 2$.*

We need some preliminary lemmas. Recall the definition of the set of integers $\mathcal{H}$ in (3.1). Fix a prime number $r \geqslant 5$ and set

$$\mathcal{H}_r = \left\{ (q,d) \,:\, r = \tfrac{q^d-1}{q-1},\ q \text{ a prime power},\ d \geqslant 2 \right\}.$$

**Lemma 3.9.** $|\mathcal{H}_r| < \log_2 r$.

*Proof.* Suppose $(q,d) \in \mathcal{H}_r$. Then $d$ is a prime number and it is easy to see that $(s,d) \in \mathcal{H}_r$ if and only if $s = q$. Indeed, if $q < s$ then

$$\frac{q^d-1}{q-1} = \frac{s^d-1}{s-1} \geqslant \frac{(q+1)^d-1}{q},$$

which is absurd. Therefore, we just need to count the possibilities for $d$. Since $r > q^{d-1}$ we have

$$d \leqslant \left\lfloor \frac{\log r}{\log q} \right\rfloor + 1 =: D$$

and the result follows since there are fewer than $\log_2 r$ primes at most $D$. □

As an immediate corollary, it follows that if $r \geqslant 5$ is a prime in $\mathcal{H}$ then

$$\ell := 1 + \sum_{(q,d) \in \mathcal{H}_r} \frac{r-1}{d} < r \log_2 r. \tag{3.3}$$

Set $G = A_r$, where $r \geqslant 73$ is a prime in $\mathcal{H}$. Fix an $r$-cycle $s \in G$. As observed in the proof of Theorem 3.1, $\mathcal{M}(G,s)$ comprises a single copy of $\mathrm{AGL}_1(r) \cap G$, together with at most $(r-1)/d$ copies of $\mathrm{P\Gamma L}_d(q) \cap G$ for each $(q,d) \in \mathcal{H}_r$. In particular, $|\mathcal{M}(G,s)| \leqslant \ell$, where $\ell$ is given in (3.3).

**Lemma 3.10.** *If $r \geqslant 73$ is a prime in $\mathcal{H}$, then $|H| \geqslant r(r-1)/2$ for all $H \in \mathcal{M}(G,s)$.*

*Proof.* First observe that $|\mathrm{AGL}_1(r) \cap G| \geqslant r(r-1)/2$. Fix $(q,d) \in \mathcal{H}_r$ and note that $r < 2q^{d-1}$. Then

$$|\mathrm{P\Gamma L}_d(q) \cap G| > \frac{1}{4} q^{d^2-1} > \frac{1}{4} \left(\frac{r}{2}\right)^{d+1} \geqslant \frac{1}{32} r^3$$

and the result follows. □

Define

$$C = \max\{|H| \,:\, H \in \mathcal{M}(G,s)\}. \tag{3.4}$$

**Lemma 3.11.** *Suppose $r \geqslant 73$ is a prime in $\mathcal{H}$, $H \in \mathcal{M}(G,s)$ and $x \in H$ has prime order. Then $|x^G| > C^4$.*

*Proof.* We use some of the ideas in the proof of [17, Theorem 1.1]. Fix $H \in \mathcal{M}(G,s)$ containing $x$ and observe that $H$ is primitive, so a theorem of Maróti [42] gives

$$|H| < r^{1+\log_2 r}.$$

By the main theorem of [25], the minimal degree of $H$ is at least $r/2$, which means that

$$|x^G| \geqslant \frac{r!}{2^{r/4}\lceil r/4\rceil!\lceil r/2\rceil!} =: f(r).$$

Using the bounds

$$\sqrt{2\pi}\cdot n^{1/2}\left(\frac{n}{e}\right)^n < n! < e\cdot n^{1/2}\left(\frac{n}{e}\right)^n,$$

which are valid for all positive integers $n$, we get

$$\begin{aligned} f(r) &> \frac{\sqrt{2\pi}\cdot r^{r+1/2}e^{-r}}{2^{r/4}\cdot e\left(\frac{r+3}{4}\right)^{(r+3)/4+1/2}e^{-(r+3)/4}\cdot e\left(\frac{r+1}{2}\right)^{(r+1)/2+1/2}e^{-(r+1)/2}} \\ &> 2^{r/4}\left(\frac{r^{r+1/2}}{(r+3)^{r/4+5/4}(r+1)^{r/2+1}}\right) \\ &> r^{r/4} \end{aligned}$$

and thus it suffices to show that $r \geqslant 16(1+\log_2 r)$. One checks that this inequality holds if $r > 127$, so it just remains to handle the primes $r \in \{73, 127\}$ (recall that $r \in \mathcal{H}$). If $r = 73$ then $C = |\mathrm{P\Gamma L}_3(8)|$ and similarly $C = |\mathrm{P\Gamma L}_7(2)|$ if $r = 127$; in both cases, the desired bound is easily checked using Magma. □

We are now in a position to prove Proposition 3.8.

*Proof of Proposition 3.8.* Set $G = A_r$, where $r \geqslant 13$ is a prime number, and let $s \in G$ be an $r$-cycle. First assume $r \notin \mathcal{H}$. If $r = 23$ then a straightforward computation (see Section 2.3.1) shows that $\gamma_u(G) = 2$. Now assume $r \neq 23$, in which case the proof of Theorem 3.1 implies that $\mathcal{M}(G,s) = \{H\}$ with $H = \mathrm{AGL}_1(r) \cap G$. Now $b(G, G/H) = 2$ by [17, Corollary 1.5], so Corollary 2.2 implies that $\gamma_u(G) = 2$.

To complete the proof, we may assume $r \in \mathcal{H}$. To handle the case $r = 13$, we use random search in Magma to show that $\gamma_u(G) = 2$ (we refer the reader to [18, Section 1.2.4] for further details of the computation). For example, one can check that

$$\{(1,2,3,4,5,6,7,8,9,10,11,12,13), (1,2,3,4,5,6,8,9,12,7,11,10,13)\}$$

is a TDS for $\Gamma(G)$. For $r \in \{17, 31\}$ we can use Lemma 2.5 to show that $\gamma_u(G) = 2$.

Now assume $r > 31$, which means that $r \geqslant 73$ (see [4, Table II]). Set $\mathcal{M}(G,s) = \{H_1, \ldots, H_k\}$ and let $x_1, \ldots, x_m$ be representatives of the $G$-classes of elements of prime order which meet at least one of the subgroups in $\mathcal{M}(G,s)$. Note that $k \leqslant \ell$, where $\ell$ is defined in (3.3). By Lemma 2.5, we need to show that

$$\sum_{i=1}^{m} |x_i^G| \left(\sum_{j=1}^{k} \mathrm{fpr}(x_i, G/H_j)\right)^2 < 1.$$

To do this, we apply Lemma 2.7 with $A_j = C$ and $B = C^4$ for all $j$, where $C$ is defined in (3.4), noting that the value of $B$ is justified by Lemma 3.11. This yields

$$\sum_{i=1}^{m} |x_i^G| \left(\sum_{j=1}^{k} \mathrm{fpr}(x_i, G/H_j)\right)^2 < \left(\frac{\ell}{C}\right)^2.$$

Finally, we recall that $\ell < r\log_2 r$ and $|C| \geqslant r(r-1)/2$ (see (3.3) and Lemma 3.10), whence $\ell < C$ and the proof is complete. □

**Remark 3.12.** We can use computational methods (see Section 2.3) to compute $\gamma_u(G)$ when $G = A_r$ and $r \in \{5, 7, 11\}$ is one of the primes excluded in Proposition 3.8. We get the following results:

$$\gamma_u(A_r) = \begin{cases} 3 & \text{if } r = 5, 11, \\ 4 & \text{if } r = 7. \end{cases}$$

For example, suppose $r = 11$. By applying Lemma 2.5, with $s \in G$ an 11-cycle, it is easy to see that $\gamma_u(G) \leqslant 3$. To show that $\gamma_u(G) \geqslant 3$ we employ the method described in Remark 2.4. Fix an element $g \in G$. If $g$ is not an 11-cycle then $g$ is contained in an intransitive subgroup $H$ with $b(G, G/H) \geqslant 3$ (see Lemma 3.13 below). On the other hand, if $g$ is an 11-cycle then $g$ is contained in a subgroup $H = \mathrm{M}_{11}$ (see the proof of Theorem 3.1) and by [17, Theorem 1] we have $b(G, G/H) = 3$. Therefore, Corollary 2.3 implies that $\gamma_u(G) \geqslant 3$ and thus $\gamma_u(G) = 3$. The other cases are handled in a similar fashion.

3.2.2. *Even degree.* Next we consider the alternating groups of even degree; the analysis of the groups of odd composite degree is more complicated and we postpone the study of these groups to the end of the section.

Our main result is Proposition 3.14 below, which gives the exact value of $\gamma_u(A_n)$, up to a small constant. The key tool is the following result of Halasi (see [29, Theorems 3.1 and 4.2]) on the base size of $S_n$ on $k$-sets.

**Lemma 3.13.** *Let $n \geqslant 5$ be an integer and let $\Omega$ be the set of $k$-element subsets of $\{1, \ldots, n\}$ for some $1 \leqslant k \leqslant n/2$. Then*

$$\lceil \log_2 n \rceil \leqslant b(S_n, \Omega) \leqslant \left\lceil \log_{\lceil n/k \rceil} n \right\rceil \cdot (\lceil n/k \rceil - 1).$$

Note that if $S_n$ acts faithfully on a finite set $\Omega$, then

$$b(A_n, \Omega) \leqslant b(S_n, \Omega) \leqslant b(A_n, \Omega) + 1.$$

**Proposition 3.14.** *Let $n \geqslant 6$ be an even integer. Then $\lceil \log_2 n \rceil - 1 \leqslant \gamma_u(A_n) \leqslant 2\lceil \log_2 n \rceil$.*

*Proof.* Write $G = A_n$ and $n = 2m$. If $n = 6$ then by a direct computation in Magma (see Section 2.3.3) we can prove that $\gamma_u(G) = 4$; indeed, $\Gamma(G)$ has a total dominating set comprising four conjugate 5-cycles.

Now assume that $n \geqslant 8$. First we establish the upper bound. Set $l = (m-1, 2)$ and fix $s \in G$ with shape $[k, n-k]$, where $k = m - l$. By the proof of Theorem 3.1, $\mathcal{M}(G, s) = \{H\}$ with $H = (S_k \times S_{n-k}) \cap G$. By combining Corollary 2.2 and Lemma 3.13, we get

$$\gamma_u(G) \leqslant b(G, G/H) \leqslant \left\lceil \log_{\lceil \frac{2n}{n-2l} \rceil} n \right\rceil \cdot \left\lceil \frac{n+2l}{n-2l} \right\rceil \leqslant 2\lceil \log_2 n \rceil$$

as required.

To prove the lower bound, fix an element $1 \neq s \in G$. Since $n$ is even, $s$ is not an $n$-cycle. Therefore, $s$ is contained in the stabiliser $H$ of a proper subset of $\{1, \ldots, n\}$, and we have $b(G, G/H) \geqslant \lceil \log_2 n \rceil - 1$ by Lemma 3.13. By applying Corollary 2.3, we conclude that $\gamma_u(G) \geqslant \lceil \log_2 n \rceil - 1$. □

3.2.3. *Odd degree.* To complete the proof of Theorem 3.7, we may assume $G = A_n$, where $n \geqslant 9$ is a composite odd integer.

**Proposition 3.15.** *Let $n \geqslant 5$ be an odd integer. Then $\gamma_u(A_n) \leqslant 77 \log_2 n$.*

In order to prove Proposition 3.15, we need some preliminary results. We start with the following technical lemma. Note that for the remainder of this section, we adopt the standard convention that $\binom{a}{b} = 0$ if $b > a$.

**Lemma 3.16.** *Let $l$ and $m$ be integers such that $l \geqslant 2$ and $0 \leqslant m \leqslant 4l$. Then*

$$f(l,m) \coloneqq \sum_{j=0}^{\min\{l,\lfloor m/2 \rfloor\}} \binom{l}{j}\binom{4l}{2m-4j} \geqslant \binom{4l}{m}.$$

*Proof.* First assume $0 \leqslant m \leqslant 2l-2$, so $\lfloor m/4 \rfloor \leqslant \min\{l, \lfloor m/2 \rfloor\}$ and we can consider the term

$$\binom{l}{\lfloor m/4 \rfloor}\binom{4l}{2m-4\lfloor m/4 \rfloor}$$

in $f(l,m)$. If $m \leqslant 2l-3$, then $m-3 \leqslant 4\lfloor m/4 \rfloor \leqslant m$, so $m \leqslant 2m-4\lfloor m/4 \rfloor \leqslant m+3 \leqslant 2l$. Similarly, if $m = 2l-2$ then $2l-4 \leqslant 4\lfloor (2l-2)/4 \rfloor \leqslant 2l-2$ and $m \leqslant 2m-4\lfloor m/4 \rfloor \leqslant 2l$ in this case also. Therefore,

$$f(l,m) \geqslant \binom{l}{\lfloor m/4 \rfloor}\binom{4l}{2m-4\lfloor m/4 \rfloor} \geqslant \binom{4l}{2m-4\lfloor m/4 \rfloor} \geqslant \binom{4l}{m}.$$

A very similar argument applies if $2l+2 \leqslant m \leqslant 4l$, working with the term corresponding to $j = \lceil m/4 \rceil$. We omit the details.

Finally, let us assume $m \in \{2l-1, 2l, 2l+1\}$. We will provide the details for $m = 2l-1$; the other cases are very similar. The result is easily verified if $l = 2$, so assume that $l \geqslant 3$. Observe that $2l-2 \leqslant 2m-4\lfloor m/4 \rfloor \leqslant 2l$, so

$$\binom{4l}{2m-4\lfloor m/4 \rfloor} \geqslant \binom{4l}{2l-2} = \frac{2l-1}{2l+2}\binom{4l}{2l-1} \geqslant \frac{1}{2}\binom{4l}{m}.$$

Additionally, since $m = 2l-1 \geqslant 5$, we have

$$\binom{l}{\lfloor m/4 \rfloor} \geqslant l \geqslant 3$$

and thus

$$f(l,m) \geqslant \binom{l}{\lfloor m/4 \rfloor}\binom{4l}{2m-4\lfloor m/4 \rfloor} \geqslant 3 \cdot \frac{1}{2}\binom{4l}{m} \geqslant \binom{4l}{m}.$$

This completes the proof. □

The next result on fixed point ratios is a key ingredient in the proof of Proposition 3.15. For $g \in G$, we write $\mathrm{supp}(g)$ to denote the support of $g$.

**Lemma 3.17.** *Suppose $G = S_n$, where $n$ is odd and let $s \in G$ be an element with shape as in (3.2). Fix an element $x \in G$ with shape $[d^r, 1^{n-dr}]$ for some $d \geqslant 2$ and $r \geqslant 1$. Set $t = |\mathrm{supp}(g)| = dr$. If $t \geqslant 100$, then*

$$\mathrm{fpr}(x, G/H) < 0.98^t$$

*for all $H \in \mathcal{M}(G,s)$.*

*Proof.* As noted in the proof of Theorem 3.1, $\mathcal{M}(G,s)$ comprises three intransitive subgroups. Write $H = S_k \times S_{n-k} \in \mathcal{M}(G,s)$, where $k < \frac{n}{2}$, and identify $G/H$ with the set $\Omega$ of $k$-element subsets of $\{1, \ldots, n\}$. Since a set $A \in \Omega$ is fixed (setwise) by $x$ if and only if each cycle of $x$ is contained in or disjoint from $A$, it follows that

$$\mathrm{fpr}(x, G/H) = \sum_{i=0}^{r} \binom{r}{i} f(i)$$

where

$$f(i) = \frac{\binom{n-t}{k-di}}{\binom{n}{k}} = \frac{k \cdots (k-di+1)(n-k)\cdots(n-t-k+di+1)}{n \cdots (n-t+1)}.$$

Note that

$$f(i) \leqslant \min\left\{ \left(\frac{k}{n}\right)^{di}, \left(1-\frac{k}{n}\right)^{t-di} \right\}.$$

Since $n \geqslant t \geqslant 100$, from the shape of $s$ in (3.2) it follows that $31/99 \leqslant k/n \leqslant 35/99$. Therefore, if $di \geqslant 0.265t$ then

$$f(i) \leqslant \left(\frac{k}{n}\right)^{0.265t} \leqslant \left(\left(\frac{35}{99}\right)^{0.265}\right)^t < 0.76^t,$$

otherwise

$$f(i) \leqslant \left(\frac{n-k}{n}\right)^{0.735t} \leqslant \left(\left(\frac{68}{99}\right)^{0.735}\right)^t < 0.76^t.$$

It follows that

$$\mathrm{fpr}(x, G/H) < \sum_{i=0}^{r} \binom{r}{i} 0.76^t = 2^r \cdot 0.76^t = (2^{1/d} \cdot 0.76)^t$$

and thus

$$\mathrm{fpr}(x, G/H) < (2^{1/3} \cdot 0.76)^t < 0.9576^t \tag{3.5}$$

if $d \geqslant 3$.

The case $d = 2$ requires special attention. Here $x$ has cycle shape $[2^r, 1^{n-2r}]$ with $r \geqslant 50$. Set $l = \lfloor r/4 \rfloor$ and fix elements $y$ and $z$ in $G$ of shape $[2^{4l}, 1^{n-8l}]$ and $[4^l, 1^{n-4l}]$, respectively. Without loss of generality, we may assume that

$$\begin{aligned} x &= (1,2)(3,4)\cdots(2r-1,2r) \\ y &= (1,2)(3,4)\cdots(8l-1,8l) \\ z &= (1,2,3,4)\cdots(4l-3,4l-2,4l-1,4l). \end{aligned}$$

We claim that

$$\mathrm{fpr}(x, \Omega) \leqslant \mathrm{fpr}(y, \Omega) \leqslant \mathrm{fpr}(z, \Omega).$$

Let $\mathrm{Fix}(g, \Omega)$ be the set of fixed points of $g$ on $\Omega$. Since a set $A \in \Omega$ is fixed by $g$ if and only if each cycle of $g$ is contained in or disjoint from $A$, it follows that $\mathrm{Fix}(x, \Omega) \subseteq \mathrm{Fix}(y, \Omega)$ and thus $\mathrm{fpr}(x, \Omega) \leqslant \mathrm{fpr}(y, \Omega)$.

For $0 \leqslant m \leqslant k/2$ define

$$\begin{aligned} Y_m &= \{A \cap \mathrm{supp}(y) \,:\, A \in \mathrm{Fix}(y, \Omega), |A \cap \mathrm{supp}(y)| = 2m\} \\ Z_m &= \{A \cap \mathrm{supp}(y) \,:\, A \in \mathrm{Fix}(z, \Omega), |A \cap \mathrm{supp}(y)| = 2m\}. \end{aligned}$$

By counting the sets $A \in \mathrm{Fix}(y, \Omega)$ according to the size of $A \cap \mathrm{supp}(y)$, we see that

$$|\mathrm{Fix}(y, \Omega)| = \sum_{m=0}^{\min\{4l, \lfloor k/2 \rfloor\}} \binom{n-8l}{k-2m} |Y_m|,$$

and similarly

$$|\mathrm{Fix}(z, \Omega)| = \sum_{m=0}^{\min\{4l, \lfloor k/2 \rfloor\}} \binom{n-8l}{k-2m} |Z_m|.$$

In particular, $\mathrm{fpr}(y, \Omega) \leqslant \mathrm{fpr}(z, \Omega)$ if $|Y_m| \leqslant |Z_m|$ for all $0 \leqslant m \leqslant k/2$.

Since a subset of $\mathrm{supp}(y)$ is fixed by $y$ if and only if it is a union of cycles of $y$, we have

$$|Y_m| = \binom{4l}{m}.$$

Similarly, a subset $A$ of $\mathrm{supp}(y)$ is fixed by $z$ if and only if it is a union of cycles of $z$, that is, $A = A_1 \cup A_2$ where $A_1$ is the support of a collection of 4-cycles of $z$, and $A_2$ is a subset

of $\mathrm{supp}(y) \setminus \mathrm{supp}(z) = \{4l+1, \ldots, 8l\}$ of the appropriate size. By considering the possible 4-cycles corresponding to $A_1$, we deduce that

$$|Z_m| = \sum_{j=0}^{\min\{l, \lfloor m/2 \rfloor\}} \binom{l}{j} \binom{4l}{2m-4j}.$$

By Lemma 3.16, we have $|Y_m| \leqslant |Z_m|$ for all $0 \leqslant m \leqslant k/2$, hence $\mathrm{fpr}(y, \Omega) \leqslant \mathrm{fpr}(z, \Omega)$ as claimed.

In view of the above bound for $d = 4$ (see (3.5)), it follows that

$$\mathrm{fpr}(x, G/H) \leqslant \mathrm{fpr}(z, G/H) < 0.9576^{4l}$$

where $4l = 4\lfloor r/4 \rfloor \geqslant r - 3 \geqslant 47t/100$, and thus

$$\mathrm{fpr}(x, G/H) < 0.9576^{47t/100} \leqslant 0.98^t$$

as required. □

Finally, we are now in a position to prove Proposition 3.15, which completes the proof of Theorem 3.7.

*Proof of Proposition 3.15.* First assume $n \leqslant 19$. If $n$ is a prime then $\gamma_u(G) \leqslant 4$ by Proposition 3.8 and Remark 3.12. For $n \in \{9, 15\}$, a straightforward computation in Magma shows that $G$ has a total dominating set consisting of 6 conjugate $n$-cycles (see Section 2.3.1). For the remainder, we may assume $n \geqslant 21$.

We apply the probabilistic method in Lemma 2.5. Let $s \in G$ be an element with shape as in (3.2) and suppose $x \in G$ has prime order. As in the proof of Lemma 2.5, write

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

and recall that

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

For $t \in \{3, \ldots, n\}$, let $N_t$ be the number of elements in $G$ with support of size $t$. By (2.4),

$$Q(G, s, c) \leqslant \sum_{t=3}^{n} N_t \cdot \xi(t, s)^c,$$

where

$$\xi(t, s) = \max\{P(x, s) \,:\, x \in G \text{ has prime order and } |\mathrm{supp}(x)| = t\}.$$

Note that $N_t \leqslant n^t$.

Set $\alpha = 0.991$ and write $|\mathrm{supp}(x)| = t$. By the proof of [24, Proposition 7.1], using the fact that $n \geqslant 21$, we see that $P(x, s) \leqslant 0.9$ if $t \in \{3, 4\}$, and $P(x, s) \leqslant 0.36$ if $t \geqslant 5$. Therefore, $\xi(t, s) \leqslant \alpha^{t+1}$ if $t < 100$. Similarly, if $t \geqslant 100$ then Lemma 3.17 implies that

$$\xi(t, s) \leqslant 3 \cdot 0.98^t = 3 \cdot 0.98^{t/2 - 1/2} (0.98^{1/2})^{t+1} \leqslant \alpha^{t+1}.$$

Therefore, $\xi(t, s) \leqslant \alpha^{t+1}$ for all $t$. As a result, if $c = \log_{1/\alpha} n \leqslant 77 \log_2 n$, then

$$Q(G, s, c) \leqslant \sum_{t=3}^{n} n^t (\alpha^{t+1})^c = \sum_{t=3}^{n} n^t \left(\frac{1}{n}\right)^{t+1} = \sum_{t=3}^{n} \frac{1}{n} = \frac{n-2}{n} < 1$$

and we conclude that $\gamma_u(G) \leqslant c \leqslant 77 \log_2 n$. □

| $G$ | $\mu(G)$ | $\gamma_u(G)$ | $s$ | $\mathcal{M}(G,g)$ | $b$ | $c$ |
|---|---|---|---|---|---|---|
| $\mathrm{M}_{11}$ | 1 | 4 | 11A | $\mathrm{L}_2(11)$ | 4 | |
| $\mathrm{M}_{12}$ | 3 | 4 | 10A | $A_6.2^2$, $A_6.2^2$, $2 \times S_5$ | | 6 |
| $\mathrm{M}_{22}$ | 1 | 3 | 11A | $\mathrm{L}_2(11)$ | 3 | |
| $\mathrm{M}_{23}$ | 1 | 2 | 23A | 23:11 | 2 | |
| $\mathrm{M}_{24}$ | 2 | 3 or 4 | 21A | $\mathrm{L}_3(4){:}S_3$, $2^6{:}(\mathrm{L}_3(2) \times S_3)$ | | 4 |
| $\mathrm{J}_1$ | 1 | 2 | 15A | $D_6 \times D_{10}$ | 2 | |
| $\mathrm{J}_2$ | 3 | 3 or 4 | 10C | $2^{1+4}{:}A_5$, $A_5 \times D_{10}$, $5^2{:}D_{12}$ | | 4 |
| $\mathrm{J}_3$ | 2 | 2 or 3 | 19A | $\mathrm{L}_2(19)$, $\mathrm{L}_2(19)$ | | 3 |
| $\mathrm{J}_4$ | 1 | 2 | 43A | 43:14 | 2 | |
| HS | 2 | 3 or 4 | 15A | $S_8$, $5{:}4 \times A_5$ | | 4 |
| Suz | 3 | 3 | 14A | $\mathrm{J}_2{:}2$, $\mathrm{J}_2{:}2$, $(A_4 \times \mathrm{L}_3(4)){:}2$ | | 3 |
| McL | 3 | 3 | 15A | $3^{1+4}{:}2.S_5$, $2.A_8$, $5^{1+2}{:}3{:}8$ | | 3 |
| Ru | 1 | 2 | 29A | $\mathrm{L}_2(29)$ | 2 | |
| He | 1 | 2 or 3 | 17A | $\mathrm{Sp}_4(4){:}2$ | 4 | |
| | | | 21A | $3.S_7$, $7^{1+2}{:}(3 \times S_3)$, $7{:}3 \times \mathrm{L}_3(2)$, $7{:}3 \times \mathrm{L}_3(2)$ | | 3 |
| Ly | 1 | 2 | 28A | $2.A_{11}$ | 2 | |
| O′N | 2 | 2 | 31A | $\mathrm{L}_2(31)$, $\mathrm{L}_2(31)$ | | 2 |
| $\mathrm{Co}_1$ | 1 | 2 or 3 | 26A | $(A_4 \times G_2(4)){:}2$ | 3 | |
| $\mathrm{Co}_2$ | 1 | 3 | 23A | $\mathrm{M}_{23}$ | 3 | |
| $\mathrm{Co}_3$ | 1 | 3 | 23A | $\mathrm{M}_{23}$ | 3 | |
| $\mathrm{Fi}_{22}$ | 1 | 3 or 4 | 22A | $2.\mathrm{U}_6(2)$ | 5 | |
| | | | 16A | $2^{5+8}{:}(S_3 \times A_6)$, $2.2^{1+8}{:}(\mathrm{U}_4(2){:}2)$, $2^{10}{:}\mathrm{M}_{22}$, ${}^2F_4(2)'$ (4 times) | | 4 |
| $\mathrm{Fi}_{23}$ | 1 | 2 | 35A | $S_{12}$ | 2 | |
| $\mathrm{Fi}'_{24}$ | 1 | 2 | 29A | 29:14 | 2 | |
| HN | 1 | 2 or 3 | 22A | 2.HS.2 | 3 | |
| Th | 2 | 2 | 19A | $\mathrm{U}_3(8){:}6$, $\mathrm{L}_2(19){:}2$ | | 2 |
| $\mathbb{B}$ | 1 | 2 | 47A | 47:23 | 2 | |
| $\mathbb{M}$ | 1 | 2 | 59A | $\mathrm{L}_2(59)$ | 2 | |

TABLE 1. Sporadic simple groups

## 4. Sporadic simple groups

4.1. **Maximal overgroups.** In this section we determine the exact value of $\mu(G)$ for all sporadic simple groups $G$.

**Theorem 4.1.** *For each sporadic simple group $G$, the value of $\mu(G)$ is recorded in Table 1. In particular, $\mu(G) \leqslant 3$, with equality if and only if $G \in \{\mathrm{M}_{12}, \mathrm{J}_2, \mathrm{McL}, \mathrm{Suz}\}$.*

*Proof.* If $G = \mathbb{B}$ or $\mathbb{M}$, then $\mu(G) = 1$ (see [24, Table IV]); in the final two rows of Table 1 we present an element $s \in G$ (using ATLAS [21] notation to identify the conjugacy class of $s$) such that $|\mathcal{M}(G,s)| = 1$. In each of the remaining cases, we can use GAP to determine $|\mathcal{M}(G,s)|$ for each conjugacy class representative $s \in G$ (see Section 2.3.2). In this way, we compute $\mu(G)$ and we identify an element $s \in G$ with $|\mathcal{M}(G,s)| = \mu(G)$. This information is presented in Table 1. (For $G \notin \{\mathrm{Co}_1, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}\}$, the value of $\mu(G)$ given in Table 1 was known to be an upper bound; see [24, Table IV] and [10, Table 7].) □

4.2. **Uniform domination number.** Our main result on the uniform domination number of sporadic groups is the following. Note that this immediately implies Theorem 3.

**Theorem 4.2.** *Let $G$ be a sporadic simple group. Then*

$$d - \varepsilon \leqslant \gamma_u(G) \leqslant d,$$

*where $d$ is defined as follows:*

| $G$ | $\mathrm{M}_{11}$ | $\mathrm{M}_{12}$ | $\mathrm{M}_{22}$ | $\mathrm{M}_{23}$ | $\mathrm{M}_{24}$ | $\mathrm{J}_1$ | $\mathrm{J}_2$ | $\mathrm{J}_3$ | $\mathrm{J}_4$ | HS | Suz | McL | Ru |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $d$ | 4 | 4 | 3 | 2 | $4^*$ | 2 | $4^*$ | $3^*$ | 2 | $4^*$ | 3 | 3 | 2 |

| | He | Ly | O′N | $\mathrm{Co}_1$ | $\mathrm{Co}_2$ | $\mathrm{Co}_3$ | $\mathrm{Fi}_{22}$ | $\mathrm{Fi}_{23}$ | $\mathrm{Fi}'_{24}$ | HN | Th | $\mathbb{B}$ | $\mathbb{M}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $3^*$ | 2 | 2 | $3^*$ | 3 | 3 | $4^*$ | 2 | 2 | $3^*$ | 2 | 2 | 2 |

*Here an asterisk indicates that $\varepsilon = 1$; otherwise $\varepsilon = 0$ and $\gamma_u(G) = d$. In particular, $\gamma_u(G) \leqslant 4$, with equality if $G = \mathrm{M}_{11}$ or $\mathrm{M}_{12}$.*

*Proof.* If $\mu(G) = 1$ then we choose an element $s \in G$ such that $\mathcal{M}(G,s) = \{H\}$ and $b(G, G/H)$ is minimal (note that the base size of every almost simple primitive group with sporadic socle has been computed; see [20, 43]). The element $s$, subgroup $H$ and base size $b = b(G, G/H)$ are recorded in Table 1, and we note that $\gamma_u(G) \leqslant b$ by Corollary 2.2. In particular, we conclude that $\gamma_u(G) = 2$ if $G = \mathbb{B}$ or $\mathbb{M}$.

For each sporadic group $G \notin \{\mathbb{B}, \mathbb{M}\}$ and each class representative $s \in G$ we use GAP to determine the minimal $c$ such that $\widehat{Q}(G,s,c) < 1$ (see (2.3)), following the method described in Section 2.3.1. By Lemma 2.5, we have $\gamma_u(G) \leqslant c$. For the groups with $\mu(G) = 1$, we almost always find that $b \leqslant c$; the exceptions are the cases $G \in \{\mathrm{He}, \mathrm{Fi}_{22}\}$, where it is better to apply Lemma 2.5 with an element $s \in G$ for which $|\mathcal{M}(G,s)| > 1$. For these two groups, and also for those with $\mu(G) > 1$, we record the minimal value of $c$ in Table 1, together with an element $s \in G$ such that $\widehat{Q}(G,s,c) < 1$. For example, if $G = \mathrm{He}$ and $s \in$ `17A` then Table 1 indicates that $\mathcal{M}(G,s) = \{H\}$ with $H = \mathrm{Sp}_4(4).2$ and $b(G, G/H) = 4$. However, if we choose $s \in$ `21A` then $|\mathcal{M}(G,s)| = 4$ and $\widehat{Q}(G,s,3) < 1$, so $\gamma_u(G) \in \{2,3\}$.

To derive a lower bound on $\gamma_u(G)$, we proceed as in Remark 2.4 (see Section 2.3.2). For example, if $G = \mathrm{M}_{11}$ then every element of $G$ is contained in a subgroup $H$ isomorphic to $\mathrm{L}_2(11)$ or $\mathrm{M}_{10}$; in both cases $b(G, G/H) = 4$, so Corollary 2.3 implies that $\gamma_u(G) \geqslant 4$. With the exception of $G = \mathrm{M}_{12}$, this explains how we obtain the results on $\gamma_u(G)$ presented in Table 1.

The case $G = \mathrm{M}_{12}$ requires special attention. Here the above approach only gives $3 \leqslant \gamma_u(G) \leqslant 6$, but by carrying out a random search in Magma (see Section 2.3.3) one can show that the class `10A` contains a total dominating set for $\Gamma(G)$ of size 4 and thus $\gamma_u(G) \in \{3,4\}$. To rule out the existence of a uniform dominating set of size 3, we first combine the base size results in [20] with Corollary 2.3 to reduce the problem to the classes labelled `3B` and `6A`. In fact, since the square of an element in `6A` is in the class `3B`, we only need to consider `6A`. The required exhaustive search can now be carried out in Magma and we refer the reader to [18, Section 1.2.4] for further details of this computation. We conclude that $\gamma_u(G) = 4$. □

## 5. Exceptional groups of Lie type

Let us now assume $G$ is a simple group of Lie type over $\mathbb{F}_q$, where $q = p^a$ and $p$ is prime. In this section we prove Theorems 4 and 5 for exceptional groups of Lie type; the classical groups will be handled in Section 6.

### 5.1. **Maximal overgroups.**

**Theorem 5.1.** *Let $G$ be a finite simple exceptional group of Lie type over $\mathbb{F}_q$, where $q = p^a$ and $p$ is prime. Then either $\mu(G) = 1$ or one of the following holds:*

(i) *either $G = F_4(q)$ with $p = 2$, or $G = G_2(q)$ with $q > p = 3$, and $\mu(G) \leqslant 2$;*

(ii) $(G, \mu(G)) \in \{({}^2F_4(2)', 2), (G_2(3), 3)\}$.

*In particular,* $\mu(G) \leqslant 3$ *with equality if and only if* $G = G_2(3)$.

*Proof.* This is essentially an immediate corollary of the work of Weigel in [46]. Set

$$\mathcal{E} = \{E_7(2), E_7(3), {}^2E_6(2), {}^2E_6(3), F_4(3), F_4(2), {}^2F_4(2)', G_2(3), G_2(4)\}.$$

For $G \notin \mathcal{E}$, Weigel identifies an element $s \in G$ with $|\mathcal{M}(G,s)| = 1$, with the possible exception of the groups $F_4(2^a)$ and $G_2(3^a)$ (with $a \geqslant 2$), where he finds an element $s$ with $|\mathcal{M}(G,s)| = 2$. (In every case, $s$ is a generator of a maximal torus of $G$.)

To complete the proof, we just need to handle the groups in $\mathcal{E}$. If $G$ is one of the first five groups in $\mathcal{E}$, then [24, Proposition 6.2] implies that $\mu(G) = 1$. If $G$ is one of the remaining four groups, then we can use GAP to compute $\mu(G)$ and find an element $s \in G$ with $|\mathcal{M}(G,s)| = \mu(G)$ (see Section 2.3.2):

| $G$ | $F_4(2)$ | ${}^2F_4(2)'$ | $G_2(3)$ | $G_2(4)$ |
|---|---|---|---|---|
| $\mu(G)$ | 2 | 2 | 3 | 1 |
| $s$ | 17A | 16A | 13A | 21A |

This completes the proof. □

5.2. **Uniform domination number.** Our main result on the uniform domination number of exceptional groups is the following theorem, which proves Theorem 4(ii). Note that this also gives infinitely many more examples with $\gamma_u(G) = 2$ (see Theorem 1).

**Theorem 5.2.** *If* $G$ *is a finite simple exceptional group of Lie type, then* $\gamma_u(G) \leqslant 6$. *Moreover, if* $G \in \{{}^2B_2(q), {}^2G_2(q), E_8(q)\}$ *then* $\gamma_u(G) = 2$.

*Proof.* First assume that $\mu(G) = 1$, and let $s \in G$ such that $\mathcal{M}(G,s) = \{H\}$. By combining Corollary 2.2 and the main theorem of [19], we deduce that $\gamma_u(G) \leqslant b(G, G/H) \leqslant 6$.

Next suppose that $G \in \{{}^2B_2(q), {}^2G_2(q)\}$. By [46], there is an element $s \in G$ such that $\mathcal{M}(G,s) = \{H\}$ where $H = N_G(\langle s \rangle)$. (More precisely, $|s| = q + \sqrt{2q} + 1$ if $G = {}^2B_2(q)$, and $|s| = q + \sqrt{3q} + 1$ if ${}^2G_2(q)$.) In both cases, by applying [19, Lemmas 4.37 and 4.39], we get $b(G, G/H) = 2$ and thus $\gamma_u(G) = 2$ as claimed.

Now assume $G = E_8(q)$. Here we apply the probabilistic method from Lemma 2.5 and we adopt the notation therein. Fix an element $s \in G$ of order $q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$. By [46, Section 4(j)], $\mathcal{M}(G,s) = \{H\}$ where $H = N_G(\langle s \rangle)$. Moreover,

$$|x^G \cap H| < |H| = 30(q^8 + q^7 - q^5 - q^4 - q^3 + q + 1) < q^{14}$$

(see [39, Theorem 5.2], for example) and $|x^G| > q^{58}$ for every element $x \in G$ of prime order (indeed, $|x^G|$ is minimal when $q$ is even and $x$ is a long root element). Therefore, by [19, Proposition 2.3],

$$Q(G,s,2) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H)^2 < q^{58}(q^{-44})^2 = q^{-30} < 1$$

and we conclude that $\gamma_u(G) = 2$.

To complete the proof, it remains to handle the cases with $\mu(G) > 1$. In two cases we employ computational methods. Indeed, for

$$(G,s) \in \{({}^2F_4(2)', \texttt{16A}),\ (G_2(3), \texttt{13A})\}$$

we can use GAP to verify the bound $\widehat{Q}(G,s,5) < 1$ (see Section 2.3.1). By Lemma 2.5, this gives $\gamma_u(G) \leqslant 5$.

Next assume $G = F_4(q)$ with $q = 2^a$. There is an element $s \in G$ with $\mathcal{M}(G,s) = \{H, K\}$, where $H \cong K \cong {}^3D_4(q).3$ if $a > 1$ (see [46, Section 4(f)]) and $H \cong K \cong \mathrm{Sp}_8(2)$ if

$a = 1$ (see [24, Proposition 6.2]). Since $H$ and $K$ are $\mathrm{Aut}(G)$-conjugate, it follows that

$$\widehat{Q}(G,s,c) \leqslant 2^c \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H)^c \tag{5.1}$$

in terms of the notation of Lemma 2.5.

Suppose $a = 1$. The GAP Character Table Library contains the character tables of $G$ and $H$, so as described in Section 2.3.1, we can compute $\mathrm{fpr}(x, G/H)$ for all prime order elements $x \in G$. In this way, we deduce that $\widehat{Q}(G,s,5) < 1$ and thus $\gamma_u(G) \leqslant 5$.

Now assume $a > 1$. By inspecting the proof of [19, Lemma 4.26], we deduce that

$$\widehat{Q}(G,s,6) < 64 \sum_{i=1}^{5} a_i b_i^6,$$

where $a_i, b_i$ are defined as follows:

| $i$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $a_i$ | $q^{52}$ | $2q^{31}$ | $2q^{16}$ | $3q^{22}$ | $q^{48}$ |
| $b_i$ | $q^{-9}$ | $q^{-6}$ | $2q^{-5}$ | $2q^{-6}$ | $8q^{-12}$ |

It is easy to check that this yields $\widehat{Q}(G,s,6) < 1$ for all $q \geqslant 16$. For $q \in \{4, 8\}$, one checks that the value of $q^{-9}$ for $b_1$ can be replaced by $q^{-11}$ and this minor modification yields $\widehat{Q}(G,s,6) < 1$. Therefore, $\gamma_u(G) \leqslant 6$ as required.

A similar argument applies when $G = G_2(q)$ with $q = 3^a$ and $a \geqslant 2$. As explained in [46, Section 4(d)], there is an element $s \in G$ such that $\mathcal{M}(G,s) = \{H, K\}$ and $H \cong K \cong \mathrm{SU}_3(q).2$. In particular, (5.1) holds and one can check that

$$\widehat{Q}(G,s,6) < 64 \sum_{i=1}^{4} a_i b_i^6 < 1,$$

where the $a_i, b_i$ are given in the proof of [19, Lemma 4.31], hence $\gamma_u(G) \leqslant 6$. □

## 6. Classical groups

In this final section, we study the parameters $\mu(G)$ and $\gamma_u(G)$ when $G$ is a finite simple classical group. In particular, we complete the proofs of Theorems 4 and 5.

Throughout this section, we will write $r$ for the untwisted Lie rank of $G$ (that is, $r$ is the rank of the ambient simple algebraic group). Due to the existence of isomorphisms between certain low rank classical groups (see [35, Proposition 2.9.1], for example), we may (and will) assume that $G$ is one of the following:

$$\mathrm{L}_{r+1}(q),\ r \geqslant 1;\ \ \mathrm{U}_{r+1}(q),\ r \geqslant 2;\ \ \mathrm{PSp}_{2r}(q)',\ r \geqslant 2;\ \ \mathrm{P}\Omega^{\pm}_{2r}(q),\ r \geqslant 4;\ \ \Omega_{2r+1}(q),\ r \geqslant 3.$$

In addition, we assume $q$ is odd if $G = \Omega_{2r+1}(q)$.

### 6.1. Maximal overgroups.

The main result of this section is the following theorem, which completes the proof of Theorem 5.

**Theorem 6.1.** *If $G$ is a finite simple classical group, then either $\mu(G) \leqslant 3$ or $(G, \mu(G))$ is one of the following:*

| $G$ | $\mathrm{U}_6(2)$ | $\mathrm{U}_4(3)$ | $\Omega^+_8(2)$ | $\mathrm{P}\Omega^+_8(3)$ |
|---|---|---|---|---|
| $\mu(G)$ | 4 | 5 | 7 | 7 |

In order to prove Theorem 6.1, we need to introduce some additional notation and terminology, which will also be useful later in Section 6.2.

Let $G$ be a finite simple classical group over $\mathbb{F}_q$ with natural module $V$ of dimension $n$. We will write $k \oplus (n-k)$ to denote a decomposition $V = U \oplus W$, where $U$ and $W$

are totally singular subspaces of dimensions $k$ and $n-k$ (if $G = \mathrm{L}_n(q)$ then all subspaces are totally singular). In turn, $g = k \oplus (n-k)$ will denote a semisimple element $g \in G$ which preserves such a decomposition and acts irreducibly on both $U$ and $W$. Similarly, if $G \neq \mathrm{L}_n(q)$, then $k \perp (n-k)$ denotes an orthogonal decomposition $V = U \perp W$ where $U$ is a non-degenerate $k$-space, and we will write $g = k \perp (n-k)$ for an element in $G$ acting irreducibly on $U$ and $W$. For an orthogonal group, we extend this notation in the obvious way by writing $k^{\pm}$ to denote a non-degenerate $k$-space of type $\pm$ (with $k$ even). This is consistent with the notation used in [10, 24]. Following [35], we will sometimes refer to the *type* of a maximal subgroup $H$ of $G$, which provides an approximate description of the group-theoretic structure of $H$.

Write $q = p^a$ for a prime $p$ and suppose $t$ is a prime divisor of $q^e - 1$ for some $e \geqslant 2$. Recall that $t$ is a *primitive prime divisor* (ppd for short) of $q^e - 1$ if $t$ is not a divisor of $q^i - 1$ for all $1 \leqslant i < e$. A classical theorem of Zsigmondy [48] states that if $e \geqslant 3$ then $q^e - 1$ has a ppd unless $(q, e) = (2, 6)$. Primitive prime divisors also exist when $e = 2$, provided $q$ is not a Mersenne prime. Note that if $t$ is a ppd of $q^e - 1$ then $t \equiv 1 \pmod{e}$.

The following lemma establishes a special case of Theorem 6.1.

**Lemma 6.2.** *Suppose $G = \mathrm{Sp}_{2r}(q)$, where $r \geqslant 6$ is even and $q$ is even. Let*

$$s = (r-2k) \perp (r+2k) \in G,$$

*where $k = (r/2 - 1, 2)$. Then*

$$\mathcal{M}(G, s) = \{\mathrm{Sp}_{r-2k}(q) \times \mathrm{Sp}_{r+2k}(q), O^+_{2r}(q)\}$$

*and thus $\mu(G) \leqslant 2$.*

*Proof.* Write $V = U \perp W$, where $U$ and $W$ are the proper non-degenerate subspaces preserved by $s$. First observe that the order of $s$ is divisible by a ppd $t$ of $q^{r+2k} - 1$, so we are in a position to apply the main result of [27] to determine the subgroups in $\mathcal{M}(G, s)$. Following the notation of [27], set $d = 2r$ and $e = r + 2k$. By the main theorem of [27], every maximal overgroup of $s$ in $G$ is one of those listed in [27, Examples 2.1–2.9]. We will consider each of these cases in turn.

Write $q = p^a$ and consider the classical groups arising in [27, Example 2.1]. The element $s$ is not contained in any subfield subgroups since $t$ does not divide

$$|\mathrm{Sp}_{2r}(q_0)| = q_0^{r^2} \prod_{i=1}^{r} (q_0^{2i} - 1)$$

for $q_0 = p^b$ and $b < a$. The orthogonal groups $O^{\pm}_{2r}(q)$ are the only other maximal subgroups that can arise in [27, Example 2.1] (moreover, it is well known that every element in $G$ is contained in such a subgroup). First observe that if $s$ is contained in an orthogonal subgroup $H$ then the irreducibility of $s$ on $U$ and $W$ implies that both $U$ and $W$ are minus-type orthogonal spaces (with respect to the quadratic form corresponding to $H$), so $H = O^+_{2r}(q)$ is the only possibility. Moreover, we claim that $s$ is contained in exactly one such subgroup. As noted in [35, Table 3.5C], $G$ contains a unique conjugacy class of subgroups $O^+_{2r}(q)$, so we just need to compute $\mathrm{fpr}(s, G/H) \cdot |G : H|$, which is the number of $G$-conjugates of $H$ containing $s$. Since conjugacy of semisimple elements of odd order in both $G$ and $H$ is determined by eigenvalues (in a suitable field extension of $\mathbb{F}_q$), it follows that $s^G \cap H = s^H$. Moreover,

$$|C_G(s)| = (q^{r/2+k} + 1)(q^{r/2-k} + 1) = |C_H(s)|$$

and thus $\mathrm{fpr}(s, G/H) \cdot |G : H| = 1$, as claimed.

The subgroups in [27, Example 2.2] are reducible. Since $s$ acts irreducibly on both $U$ and $W$, it follows that the subspace stabiliser $G_U = \mathrm{Sp}_{r-2k}(q) \times \mathrm{Sp}_{r+2k}(q)$ is the only reducible maximal subgroup of $G$ containing $s$. No imprimitive subgroups arise from [27,

Example 2.3]. Since $q$ is even, the field extension subgroups in [27, Example 2.4] have type $\mathrm{Sp}_{2r/l}(q^l)$ for a prime divisor $l$ of $r$. If $s$ is contained in such a subgroup, then $l$ must divide $r/2-k$ and $r/2+k$, but this is not possible because these numbers are coprime.

To complete the proof of the lemma, we need to show that there are no additional subgroups in $\mathcal{M}(G,s)$. To do this, we need to argue that none of the subgroups in [27, Examples 2.5–2.9] can arise.

Let us first observe that the conditions $r \geqslant 6$ and $e = r+2k$ imply that if $t = e+1$ then $q = 2$ and $r \in \{6, 8, 14, 16\}$ (see [26, Lemma 2.1(ii)]). Now [27, Example 2.5] requires $t = e+1$ and $p$ odd, so no examples occur, and we can also rule out the cases in [27, Examples 2.6(b,c) and 2.8] since $r \geqslant 6$. In [27, Example 2.6(a)] we have $t = e+1$, so $r \in \{6, 8, 14, 16\}$ and $q = 2$. Here $(G, H) = (\mathrm{Sp}_{2r}(2), S_{2r+2})$ and the embedding of $H$ in $G$ is afforded by the fully deleted permutation module for $H$ over $\mathbb{F}_2$. Since

$$|s| = \mathrm{lcm}\{2^{r/2-k}+1, 2^{r/2+k}+1\},$$

we can easily rule out $r \in \{8, 14, 16\}$ by simply considering the orders of elements in $H$. Now assume $r = 6$, so $|s| = 33$ and $H$ has a unique class of elements of order 33. We also note that $G$ has a unique conjugacy class of maximal subgroups isomorphic to $H$ (see [7, Table 8.81]). Finally, since $G$ has three classes of elements of order 33 and type $2 \perp 10$, without any loss of generality we may assume that $\mathcal{M}(G, g)$ does not contain any subgroups isomorphic to $S_{14}$.

Finally, the handful of cases with $r \geqslant 6$ in [27, Examples 2.7 and 2.9] are not compatible with our condition $e = r+2k$, unless $(r, q) = (6, 2)$. In this case, the candidate maximal subgroup is almost simple with socle $\mathrm{L}_2(11)$, and this can be excluded since it does not contain an element of order $|s| = 33$. □

We are now ready to prove Theorem 6.1.

*Proof of Theorem 6.1.* Let $G$ be a finite simple classical group over $\mathbb{F}_q$ with natural module $V$. First we appeal to the proof of the main theorem of [24], which identifies an element $s \in G$ such that $\mathcal{M}(G, s)$ is small.

If the rank $r$ of $G$ is large (for example, $r \geqslant 11$ suffices), then this element is given in [24, Table II] and the remaining groups are covered in [24, Section 5], except for a short list of small groups which are handled in [24, Proposition 6.3]. Moreover, additional information regarding the action of $s$ on $V$ is provided in [24], which allows us to determine the precise subgroups in $\mathcal{M}(G, s)$. For example, if $G = \mathrm{P}\Omega^-_{2r}(q)$ where $r \geqslant 7$ and $r \equiv 3 \pmod 4$, then following [24, Table II] we choose

$$s = (r+1)^- \perp \left(\frac{r-1}{2} \oplus \frac{r-1}{2}\right).$$

By the proof of [24, Proposition 4.1], it follows that $\mathcal{M}(G, s) = \{H, K_1, K_2\}$ where $H$ has type $O^-_{r+1}(q) \times O^+_{r-1}(q)$ and both $K_1$ and $K_2$ are $P_{(r-1)/2}$ parabolic subgroups (that is, $K_1$ and $K_2$ are the stabilisers of totally singular subspaces of dimension $(r-1)/2$). Similarly, [10, Proposition 5.14] implies that $\mu(G) \leqslant 3$ if $G = \mathrm{P}\Omega^+_{2r}(q)$ and $r \geqslant 4$ is even.

In this way, we deduce that $\mu(G) \leqslant 3$, unless $G$ is one of the following:

(a) $\mathrm{Sp}_{2r}(q)$ with $r \geqslant 6$ even and $q$ even;

(b) $\mathrm{P}\Omega^+_8(3)$, $\Omega^+_8(2)$, $\Omega_7(3)$, $\mathrm{U}_6(2)$, $\mathrm{Sp}_6(2)$, $\mathrm{U}_4(3)$.

Case (a) was handled in Lemma 6.2. For the groups $G$ in (b), we can use GAP to determine $\mu(G)$ and to identify an element $s \in G$ with $|\mathcal{M}(G, s)| = \mu(G)$ (see Section 2.3.2). We obtain the following results, in terms of the Atlas [21] notation for conjugacy classes:

| $G$ | $\mathrm{P}\Omega^+_8(3)$ | $\Omega^+_8(2)$ | $\Omega_7(3)$ | $\mathrm{U}_6(2)$ | $\mathrm{Sp}_6(2)$ | $\mathrm{U}_4(3)$ |
|---|---|---|---|---|---|---|
| $\mu(G)$ | 7 | 7 | 3 | 4 | 2 | 5 |
| $s$ | 14A | 15A | 14A | 11A | 15A | 9A |

This proves the result. □

This completes the proof of Theorem 5.

6.2. **Uniform domination number.** Our main result is Theorem 6.3, which completes the proof of Theorem 4. In order to state this result, set

$$\mathcal{A} = \{\mathrm{U}_{r+1}(q) : r \geqslant 7 \text{ odd}\} \cup \{\mathrm{PSp}_{2r}(q) : r \geqslant 3 \text{ odd}, q \text{ odd}\} \cup \{\mathrm{P}\Omega^+_{2r}(q) : r \geqslant 5 \text{ odd}\}$$
$$\mathcal{B} = \{\mathrm{Sp}_{2r}(q) : r \geqslant 2, q \text{ even}, (r,q) \neq (2,2)\} \cup \{\Omega_{2r+1}(q) : r \geqslant 3, q \text{ odd}\}$$

**Theorem 6.3.** *Let $G$ be a finite simple classical group of rank $r$. Then*

$$\gamma_u(G) \leqslant 7r + 56.$$

*More precisely, the following hold:*

(i) *If $G = \mathrm{L}_2(q)$, then $\gamma_u(G) \leqslant 4$, with equality if and only if $q = 9$.*
(ii) *If $G \in \mathcal{A}$, then $\gamma_u(G) \leqslant 15$.*
(iii) *If $G \in \mathcal{B}$, then $r \leqslant \gamma_u(G) \leqslant 7r$.*

Note that the conclusion in part (iii) of Theorem 6.3 still holds for $G = \mathrm{Sp}_4(2)'$, but it will be convenient to exclude this group from $\mathcal{B}$. Indeed, $\mathrm{Sp}_4(2)' \cong A_6$ and the proof of Proposition 3.14 gives $\gamma_u(A_6) = 4$.

We will prove Theorem 6.3 in a sequence of propositions.

6.2.1. *Special cases.* We start by handling the special cases referred to in parts (i), (ii) and (iii). Note that part (iii) shows that the uniform domination number of the groups in $\mathcal{B}$ can be arbitrarily large. It also shows that the linear bound in Theorem 6.3 is essentially best possible (up to constants).

**Proposition 6.4.** *If $q \geqslant 4$, then $\gamma_u(\mathrm{L}_2(q)) \leqslant 4$ with equality if and only if $q = 9$.*

*Proof.* For $q < 11$, the result can be verified computationally; see Section 2.3.1. Now assume $q \geqslant 11$. Set $d = (2, q-1)$ and fix an element $s \in G$ of order $(q+1)/d$. Then $\mathcal{M}(G,s) = \{H\}$, where $H = N_G(\langle g \rangle) \cong D_{2(q+1)/d}$ (see [24, Section 5]). By combining Corollary 2.2 and [14, Lemma 4.5], we conclude that $\gamma_u(G) \leqslant b(G, G/H) \leqslant 3$. □

In order to prove the bound in part (ii) of Theorem 6.3, we need the following recent result of Halasi, Liebeck and Maróti [30, Theorem 3.3] on the base sizes of subspace actions of classical groups.

**Proposition 6.5.** *Let $G$ be a finite simple classical group with natural module $V$ of dimension $n$. Let $H$ be the stabiliser of a $k$-dimensional subspace of $V$ with $k \leqslant n/2$ and assume $H$ is a maximal subgroup of $G$. Then*

$$b(G, G/H) \leqslant \left\lfloor \frac{n}{k} \right\rfloor + 11.$$

**Proposition 6.6.** *If $G \in \mathcal{A}$, then $\gamma_u(G) \leqslant 15$.*

*Proof.* First assume that $G = \mathrm{P}\Omega^+_{2r}(q)$ where $r \geqslant 5$ is odd. For $G = \Omega^+_{10}(2)$ we choose $s = 2^- \perp 8^-$ as in [24, Proposition 6.3] and a straightforward computation shows that $\gamma_u(G) \leqslant 5$ (see Section 2.3.1). Now assume $G \neq \Omega^+_{10}(2)$. Following [24, Table II], fix an element $s = (r-1)^- \perp (r+1)^-$ in $G$. From the proof of [24, Proposition 4.1], it follows that $\mathcal{M}(G,s) = \{H\}$, where $H$ is a reducible subgroup of type $O^-_{r-1}(q) \times O^-_{r+1}(q)$. By Proposition 6.5, we have

$$b(G, G/H) \leqslant \left\lfloor \frac{2r}{r-1} \right\rfloor + 11 \leqslant 13$$

and thus Corollary 2.2 implies that $\gamma_u(G) \leqslant b(G, G/H) \leqslant 13$.

The other groups $G \in \mathcal{A}$ are handled in a very similar fashion. In each case we choose $s \in G$ as in [24, Table II], noting that $\mathcal{M}(G,s) = \{H\}$ for some reducible subgroup $H$ (as before, this follows from the proof of [24, Proposition 4.1]). Once again, the desired bound follows from Proposition 6.5, and it is worth noting that there are no special cases that require direct computation. □

Next we turn to the bounds in part (iii) of Theorem 6.3. First we establish the lower bound.

**Proposition 6.7.** *If $G \in \mathcal{B}$, then $\gamma_u(G) \geqslant r$.*

*Proof.* Suppose $G = \Omega_{2r+1}(q)$ and $1 \neq g \in G$. Then $g$ fixes a non-zero vector $v \in V$, where $V$ is the natural module. Therefore, $g$ is contained in the subspace stabiliser $H = G_{\langle v \rangle}$, which is a maximal subgroup of $G$. There are two possibilities: either $v$ is a singular vector, in which case $H$ is a $P_1$ parabolic subgroup of $G$, or $v$ is non-singular and $H$ is a subgroup of type $O^{\pm}_{2r}(q)$. In view of (2.1), we get

$$b(G, G/H) \geqslant \left\lceil \frac{\log |G|}{\log |G/H|} \right\rceil \geqslant r$$

in both cases. It follows that every non-identity element of $G$ is contained in a maximal subgroup $H$ with $b(G, G/H) \geqslant r$, so Corollary 2.3 implies that $\gamma_u(G) \geqslant r$.

A very similar argument applies when $G = \mathrm{Sp}_{2r}(q)$ with $q$ even, using the fact that every element of $G$ is contained in an orthogonal subgroup $O^{\pm}_{2r}(q)$. We omit the details. □

**Proposition 6.8.** *If $G = \Omega_{2r+1}(q) \in \mathcal{B}$, then $\gamma_u(G) \leqslant 2r + 12 \leqslant 7r$.*

*Proof.* As in [24, Table II], fix a semisimple element $s = 1 \perp (2r)^-$ and note that $\mathcal{M}(G,s) = \{H\}$, where $H$ is the stabiliser of a non-singular 1-space. By combining Corollary 2.2 and Proposition 6.5, we deduce that

$$r \leqslant \gamma_u(G) \leqslant b(G, G/H) \leqslant 2r + 12$$

as required. □

To complete the proof of the bounds in parts (i), (ii) and (iii) in Theorem 6.3, it remains to handle the groups $G = \mathrm{Sp}_{2r}(q) \in \mathcal{B}$.

6.2.2. *Symplectic groups in even characteristic.* In this section we complete the proof of Theorem 6.3 by showing that $\gamma_u(G) \leqslant 7r$ for all $G = \mathrm{Sp}_{2r}(q) \in \mathcal{B}$. To do this, we require some preliminary lemmas and additional notation. Let $\bar{G} = \mathrm{Sp}_{2r}(K)$ be the ambient simple algebraic group over the algebraic closure $K$ of $\mathbb{F}_q$ and let $\bar{V}$ be the natural module for $\bar{G}$. For an element $x \in G$, we define $\nu(x)$ to be the codimension of the largest eigenspace of $x$ on $\bar{V}$.

To establish the desired bound $\gamma_u(G) \leqslant 7r$, we will work with an element $g \in G$ of order $q^r + 1$. This allows us to appeal to earlier work of Bereczky [5] to determine the maximal overgroups of $g$ (see Lemma 6.11(i) for $r \geqslant 5$) and we then establish upper bounds on the relevant fixed point ratios (see Lemmas 6.10 and 6.11(ii)). Finally, we use Lemma 2.5 to establish the required bound on $\gamma_u(G)$; the groups with $r \geqslant 5$ are handled in Proposition 6.12, with the remaining cases treated in Proposition 6.13.

**Lemma 6.9.** *Suppose $G = \mathrm{Sp}_{2r}(q) \in \mathcal{B}$. For $s \in \{1, \ldots, 2r-1\}$, let $N_s$ be the number of elements $x \in G$ of prime order with $\nu(x) = s$. Then*

$$N_s < q^{\frac{1}{2}(4rs - s^2 + 3s + 5)}.$$

*Proof.* Fix a prime $t$ and let $N_{s,t}$ be the number of elements $x \in G$ of order $t$ with $\nu(x) = s$. By combining [13, Corollary 3.38 and Proposition 3.40], we deduce that

$$N_{s,t} < q^{\frac{1}{2}(s+1)} \cdot 2\left(\frac{q}{q-1}\right)^{\frac{s}{2}} q^{\frac{1}{2}(4rs-s^2+1)} \leqslant q^{\frac{1}{2}(4rs-s^2+2s+4)}.$$

To complete the argument, we need to show that there are at most $q^{(s+1)/2}$ possibilities for $t$. Suppose $t$ is odd and fix an element $x \in G$ of order $t$ with $\nu(x) = s$. Let $i \geqslant 1$ be minimal such that $t$ divides $q^i - 1$. Set $c = i$ if $i$ is even, otherwise $c = 2i$. Note that $t \leqslant q^{c/2} + 1$, so it suffices to show that $c \leqslant s + 1$.

If $s < r$ then $s$ is even and the 1-eigenspace of $x$ has dimension $2r - s$. Therefore, $\mathrm{Sp}_s(q)$ contains an element of order $t$, so $c \leqslant s$ and the result follows. Now assume $s \geqslant r$. Once again, if $G$ contains an element of order $t$ whose 1-eigenspace is $(2r - s)$-dimensional, then $c \leqslant s$ and we are done. If not, then $x$ must have a non-trivial eigenvalue (in $\mathbb{F}_{q^i}$) with multiplicity $2r - s$. Therefore, $(2r - s)c \leqslant 2r$ and thus $c \leqslant s + 1$ as required. □

**Lemma 6.10.** *Suppose $G = \mathrm{Sp}_{2r}(q) \in \mathcal{B}$. Let $x \in G$ be an element of prime order with $\nu(x) = s$ and let $H < G$ be a maximal subgroup of type $O^{\varepsilon}_{2r}(q)$. Then*

$$\mathrm{fpr}(x, G/H) \leqslant \frac{1}{q^s} + \frac{1}{q^r - 1}.$$

*Proof.* Let $x \in H$ be an element of prime order $t$ with $\nu(x) = s$. For now, let us assume $t$ is odd, so $s \geqslant 2$. Since two semisimple elements in $H$ are $H$-conjugate if and only if they have the same eigenvalues on $\bar{V}$, it follows that $x^G \cap H = x^H$ and thus

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

The centraliser orders $|C_G(x)|$ and $|C_H(x)|$ can be read off from [13, Table 3.6] and we deduce that

$$\mathrm{fpr}(x, G/H) = \frac{|H|}{|G|}\frac{|\mathrm{Sp}_e(q)|}{|O^{\varepsilon'}_e(q)|},$$

where $e \geqslant 0$ is the dimension of the 1-eigenspace of $x$ on $\bar{V}$ (if $e = 0$ then we define $\mathrm{Sp}_e(q) = O^{\varepsilon'}_e(q) = 1$) and $\varepsilon'$ is a suitable choice of sign. Since $e \leqslant 2r - s$ we deduce that

$$\mathrm{fpr}(x, G/H) \leqslant \frac{|H|}{|G|} \cdot \frac{1}{2} q^{r-s/2}(q^{r-s/2} + 1) \leqslant \frac{q^{r-s/2}(q^{r-s/2} + 1)}{q^r(q^r - 1)}$$

and the desired bound quickly follows.

Now assume $t = 2$. Here we use the Aschbacher–Seitz [3] notation for involution class representatives, so $x = a_s$, $b_s$ or $c_s$. It is easy to see that the $G$-class and $H$-class of $x$ have the same label and thus $x^G \cap H = x^H$. The conjugacy class sizes $|x^H|$ and $|x^G|$ can be read off from the proof of [13, Proposition 3.22] and the desired bound is easily established. For example, suppose $x = b_s$, in which case $s$ is odd. Here

$$|x^H| = \frac{|O^{\varepsilon}_{2r}(q)|}{2|\mathrm{Sp}_{s-1}(q)||\mathrm{Sp}_{2r-2s}(q)|q^{2r(s-1)-3s^2/2+3s/2}}$$

$$|x^G| = \frac{|\mathrm{Sp}_{2r}(q)|}{|\mathrm{Sp}_{s-1}(q)||\mathrm{Sp}_{2r-2s}(q)|q^{2rs-3s^2/2+s/2}}$$

and thus

$$\mathrm{fpr}(x, G/H) = \frac{1}{q^s}\left(1 + \frac{\varepsilon}{q^r - \varepsilon}\right) \leqslant \frac{1}{q^s}\left(1 + \frac{1}{q^r - 1}\right).$$

The result follows. □

**Lemma 6.11.** *Suppose $G = \mathrm{Sp}_{2r}(q) \in \mathcal{B}$ with $r \geqslant 5$, and let $g \in G$ be an element of order $q^r + 1$.*

(i) $\mathcal{M}(G,g) = \{H, H_1, \ldots, H_\ell\}$, *where* $H = O_{2r}^-(q)$ *and* $H_i = \mathrm{Sp}_{2r/k}(q^k).k$ *for some prime divisor* $k$ *of* $r$ *(one subgroup for each prime).*

(ii) *If* $x \in G$ *has prime order and* $\nu(x) = s \geqslant 3$, *then*

$$\sum_{i=1}^{\ell} \mathrm{fpr}(x, G/H_i) < \frac{1}{q^s} + \frac{1}{q^r - 1}. \tag{6.1}$$

*Proof.* The description of the maximal overgroups in part (i) follows from the proof of [10, Proposition 5.8] (also see [5]). Now consider (ii). By [13, Corollary 3.38] we have $|x^G| > \alpha$, where

$$\alpha = \frac{1}{2}\left(\frac{q}{q+1}\right) q^\beta, \quad \beta = \begin{cases} s(2r-s) & s < r \\ rs & s \geqslant r \end{cases} \tag{6.2}$$

(since $q$ is even, we can replace the coefficient $\frac{1}{4}$ in [13, Corollary 3.38] by $\frac{1}{2}$). Moreover, by the main theorem of [12] we have

$$\mathrm{fpr}(x, G/H_i) < |x^G|^{-\frac{1}{2}+\frac{1}{2r}+\frac{1}{2r+2}}$$

for all $i$. Since $\ell \leqslant \log_2 r$, we deduce that

$$\sum_{i=1}^{\ell} \mathrm{fpr}(x, G/H_i) < \log_2 r \cdot \alpha^{-\frac{1}{2}+\frac{1}{2r}+\frac{1}{2r+2}}.$$

In view of the conditions $r \geqslant 5$ and $s \geqslant 3$, one checks that this upper bound is less than $q^{-s} + (q^r - 1)^{-1}$ and the result follows. □

**Proposition 6.12.** *If* $G = \mathrm{Sp}_{2r}(q) \in \mathcal{B}$ *and* $r \geqslant 5$, *then* $\gamma_u(G) \leqslant 7r$.

*Proof.* As in Lemma 6.11, let $g \in G$ be an element of order $q^r + 1$ and define $\widehat{Q}(G, g, 7r)$ as in (2.3). In view of Lemma 2.5, it suffices to show that $\widehat{Q}(G, g, 7r) < 1$. To do this, it will be convenient to write

$$\widehat{Q}(G, g, 7r) = \widehat{Q}_1 + \widehat{Q}_2 + \widehat{Q}_3,$$

where $\widehat{Q}_1$ and $\widehat{Q}_2$ are the contributions to $\widehat{Q}(G, g, 7r)$ from the elements $x \in G$ of prime order with $\nu(x) = 1$ and 2, respectively, and $\widehat{Q}_3$ is the contribution from the remaining elements of prime order in $G$. We will estimate each $\widehat{Q}_i$ in turn. By Lemma 6.11(i), $\mathcal{M}(G, g) = \{H, H_1, \ldots, H_\ell\}$, where $H = O_{2r}^-(q)$ and $H_i = \mathrm{Sp}_{2r/k}(q^k).k$ for some prime divisor $k$ of $r$ (one subgroup for each prime). As before, we use the notation of [3] for involution class representatives.

First consider $\widehat{Q}_1$. There is a unique class of elements $x \in G$ of prime order with $\nu(x) = 1$, namely the involutions of type $b_1$ (that is, the transvections in $G$). Here $|x^G| = q^{2r} - 1$ and it is very easy to check that

$$\mathrm{fpr}(x, G/H) = \frac{1}{q} + \frac{1}{q(q^r - 1)}$$

and $\mathrm{fpr}(x, G/H_i) = 0$ for all $i$, whence

$$\widehat{Q}_1 = (q^{2r} - 1) \cdot \left(\frac{1}{q} + \frac{1}{q(q^r - 1)}\right)^{7r}. \tag{6.3}$$

Now let us turn to $\widehat{Q}_2$. If $x$ is an $a_2$-involution, then

$$|x^G| = \frac{(q^{2r-2} - 1)(q^{2r} - 1)}{(q^2 - 1)} = u_1, \quad \mathrm{fpr}(x, G/H) = \frac{q^{r-2} - 1}{q^r - 1} = v_1$$

and $\mathrm{fpr}(x, G/H_i) = 0$ for all $i$. Similarly, if $x = c_2$ then

$$|x^G| = (q^{2r-2} - 1)(q^{2r} - 1) = u_2, \quad \mathrm{fpr}(x, G/H) = \frac{1}{q^2} + \frac{1}{q^2(q^r - 1)} = v_2$$

and $\mathrm{fpr}(x, G/H_i) = 0$, unless $r$ is even and $H_i = \mathrm{Sp}_r(q^2).2$, in which case

$$\mathrm{fpr}(x, G/H_i) = \frac{q^{2r}-1}{|x^G|} = \frac{1}{q^{2r-2}-1} = w_2.$$

Now assume $x \in G$ has odd prime order $t$ and $\nu(x) = 2$, so $t$ divides $q^2-1$ and $G$ has exactly $(t-1)/2$ distinct conjugacy classes of such elements. In particular, if $t$ divides $q-\varepsilon$, then $G$ contains at most

$$\frac{1}{2}(q-\varepsilon) \cdot \frac{|\mathrm{Sp}_{2r}(q)|}{|\mathrm{Sp}_{2r-2}(q)||\mathrm{GL}_1^{\varepsilon}(q)|} = \frac{1}{2}q^{2r-1}(q^{2r}-1)$$

elements of order $t$. Since $q-\varepsilon$ has fewer than $\log_2(q-\varepsilon)$ odd prime divisors, it follows that $G$ contains at most

$$\log_2(q^2-1) \cdot \frac{1}{2}q^{2r-1}(q^{2r}-1)$$

such elements. Now $\mathrm{fpr}(x, G/H_i) = 0$ for all $i$ and

$$\mathrm{fpr}(x, G/H) \leqslant \frac{|O_{2r}^-(q)|}{|O_{2r-2}^+(q)||\mathrm{GU}_1(q)|} \cdot \frac{|\mathrm{Sp}_{2r-2}(q)||\mathrm{GU}_1(q)|}{|\mathrm{Sp}_{2r}(q)|} = \frac{q^{r-1}+1}{q(q^r-1)}.$$

Putting all this together, we conclude that

$$\widehat{Q}_2 < u_1 v_1^{7r} + u_2(v_2+w_2)^{7r} + \log_2(q^2-1) \cdot \frac{1}{2}q^{2r-1}(q^{2r}-1) \cdot \left(\frac{q^{r-1}+1}{q(q^r-1)}\right)^{7r}. \tag{6.4}$$

Finally, let us consider $\widehat{Q}_3$. We will use the inequality

$$(a+b)^n \leqslant 2^{n-1}(a^n+b^n),$$

which is valid for all positive real numbers $a, b, n$ with $n \geqslant 1$. By combining Lemmas 6.9, 6.10 and 6.11, we get

$$\begin{aligned}
\widehat{Q}_3 &< \sum_{s=3}^{2r-1} q^{\frac{1}{2}(4rs-s^2+3s+5)} \cdot \left(\frac{2}{q^s} + \frac{2}{q^r-1}\right)^{7r} \\
&< \sum_{s=3}^{2r-1} q^{\frac{1}{2}(4rs-s^2+3s+5)} \cdot q^{14r-1}\left(q^{-7rs} + q^{-7r(r-1)}\right) \\
&= q^{14r+\frac{3}{2}}\left(\sum_{s=3}^{2r-1} q^{\frac{1}{2}(3s-s^2-10rs)}\right) + q^{21r-7r^2+\frac{3}{2}}\left(\sum_{s=3}^{2r-1} q^{\frac{1}{2}(4rs-s^2+3s)}\right) \\
&< q^{14r+\frac{3}{2}} \cdot q^{-15r+1} + q^{21r-7r^2+\frac{3}{2}} \cdot q^{2r^2+3r-1}
\end{aligned}$$

and thus

$$\widehat{Q}_3 < q^{-r+\frac{5}{2}} + q^{24r-5r^2+\frac{1}{2}}. \tag{6.5}$$

By combining the expression for $\widehat{Q}_1$ in (6.3) with the bounds on $\widehat{Q}_2$ and $\widehat{Q}_3$ in (6.4) and (6.5), it is easy to check that $\widehat{Q}(G, g, 7r) < 1$ for all $r \geqslant 5$. This completes the proof of the proposition. □

Finally, we show that the desired bound also holds when $r \in \{2, 3, 4\}$.

**Proposition 6.13.** *If $G = \mathrm{Sp}_{2r}(q) \in \mathcal{B}$ and $r \in \{2, 3, 4\}$, then $\gamma_u(G) \leqslant 7r$.*

*Proof.* As before, fix an element $g \in G$ of order $q^r+1$ and note that the description of $\mathcal{M}(G, g)$ in Lemma 6.11(i) still holds. In addition, if we define $\widehat{Q}_i$ as above then the expression for $\widehat{Q}_1$ in (6.3) is still valid. Similarly, if $r \in \{3, 4\}$ then we get the upper bound on $\widehat{Q}_2$ in (6.4) (and we can set $w_2 = 0$ when $r = 3$).

First assume $r = 4$ and $q \geqslant 4$, so $\mathcal{M}(G,g) = \{O_8^-(q), \mathrm{Sp}_4(q^2).2\}$ and $\ell = 1$ in the notation of Lemma 6.11. Moreover, one can check that the upper bound in (6.1) holds (the same proof goes through unchanged) and thus

$$\widehat{Q}_3 < |G| \cdot \left(\frac{2}{q^3} + \frac{2}{q^4-1}\right)^{28} < q^{36}\left(\frac{2}{q^3} + \frac{2}{q^4-1}\right)^{28}.$$

It is now easy to check that $\widehat{Q}(G,g,28) < 1$. The case $(r,q) = (4,2)$ can be handled using GAP (see Section 2.3.1) and we get $\gamma_u(G) \leqslant 10$.

The case $r = 3$ is very similar. Here $\mathcal{M}(G,g) = \{O_6^-(q), \mathrm{Sp}_2(q^3).3\}$ and the bound in (6.1) still holds. Indeed, the main theorem of [12] implies that

$$\sum_{i=1}^{\ell} \mathrm{fpr}(x, G/H_i) = \mathrm{fpr}(x, G/H_1) < \alpha^{-\frac{1}{2}+\frac{1}{6}} = \alpha^{-\frac{1}{3}},$$

where $H_1 = \mathrm{Sp}_2(q^3).3$ and $\alpha$ is defined as in (6.2), and one checks that this is less than $q^{-s} + (q^3-1)^{-1}$. Therefore,

$$\widehat{Q}_3 < |G| \cdot \left(\frac{2}{q^3} + \frac{2}{q^3-1}\right)^{21} < q^{21}\left(\frac{2}{q^3} + \frac{2}{q^3-1}\right)^{21}$$

and the result follows.

Finally, suppose $r = 2$ and $q \geqslant 4$. Write $\mathcal{M}(G,g) = \{H, H_1\}$, where $H = O_4^-(q)$ and $H_1 = \mathrm{Sp}_2(q^2).2$. As noted above, the expression for $\widehat{Q}_1$ in (6.3) is still valid. Now consider $\widehat{Q}_2$. If $x = a_2$ then $\mathrm{fpr}(x, G/H) = 0$ and $\mathrm{fpr}(x, G/H_1) = q/(q^2-1)$ (the involutory field automorphisms of $\mathrm{Sp}_2(q^2)$ are $a_2$-involutions). Similarly, if $x = c_2$ then $|x^G| = u_2$, $\mathrm{fpr}(x, G/H) = v_2$ and $\mathrm{fpr}(x, G/H_1) = w_2$ as before, so the upper bound in (6.4) holds, with $v_1 = q/(q^2-1)$.

To complete the proof of the proposition, we may assume $x \in G$ has prime order $t$ and $\nu(x) = 3$. Here $t$ is odd and $x$ is regular. Let $i \in \{1,2,4\}$ be minimal such that $t$ divides $q^i - 1$. We consider each possibility for $i$ in turn.

Suppose $i = 4$, so $t$ divides $q^2+1$ and we see that there are at most $\log_2(q^2+1)$ possibilities for $t$. In addition, for a fixed prime $t$, there are at most $\frac{1}{4}(t-1) \leqslant \frac{1}{4}q^2$ distinct $G$-classes of elements of order $t$, each of which has size

$$\frac{|\mathrm{Sp}_4(q)|}{|\mathrm{GU}_1(q^2)|} = q^4(q^2-1)^2.$$

It is straightforward to check that

$$\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G/H_1) = \frac{2}{q^2(q^2-1)}.$$

Finally, suppose $i \in \{1,2\}$. Here neither $H$ nor $H_1$ contains any regular semisimple elements of order $t$, so $\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, G/H_1) = 0$. Putting this together, we conclude that

$$\widehat{Q}_3 < \log_2(q^2+1) \cdot \frac{1}{4}q^2 \cdot q^4(q^2-1)^2 \cdot \left(\frac{2}{q^2(q^2-1)}\right)^{14}$$

and the result follows. □

6.2.3. *General case.* To complete the proof of Theorem 6.3, we need to verify the bound

$$\gamma_u(G) \leqslant 7r + 56.$$

In view of our earlier work, we may assume that $r > 1$ and $G \notin \mathcal{A} \cup \mathcal{B}$. It will be convenient to handle some small groups separately, and with this in mind we define

$$\mathcal{C} = \{\mathrm{L}_9(2), \mathrm{L}_8(2), \mathrm{P}\Omega_8^+(3), \Omega_8^+(2), \mathrm{L}_7(2), \mathrm{PSp}_6(3), \mathrm{U}_6(2), \mathrm{L}_4(2), \mathrm{U}_4(3), \mathrm{U}_4(2), \mathrm{U}_3(5)\}.$$

**Proposition 6.14.** *If $G \in \mathcal{C}$, then $\gamma_u(G) \leqslant c$, where $c$ is as follows:*

| $G$ | $\mathrm{L}_9(2)$ | $\mathrm{L}_8(2)$ | $\mathrm{P}\Omega_8^+(3)$ | $\Omega_8^+(2)$ | $\mathrm{L}_7(2)$ | $\mathrm{PSp}_6(3)$ | $\mathrm{U}_6(2)$ | $\mathrm{L}_4(2)$ | $\mathrm{U}_4(3)$ | $\mathrm{U}_4(2)$ | $\mathrm{U}_3(5)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $c$ | 7 | 9 | 19 | 26 | 6 | 3 | 6 | 4 | 16 | 8 | 13 |
| $s$ | $4 \oplus 5$ | $3 \oplus 5$ | 14A | 15A | 105A | 14A | 11A | 15A | 9A | 9A | 13A |

*In particular, $\gamma_u(G) \leqslant 7r + 56$.*

*Proof.* We implement the probabilistic method computationally (see Section 2.3.1), working with an element $s \in G$ in the conjugacy class specified in the table. We use Magma to handle the groups $\mathrm{L}_9(2)$ and $\mathrm{L}_8(2)$, and GAP for the remaining cases. In this way, for $G \neq \Omega_8^+(2)$, one can check that $\widehat{Q}(G, s, c) < 1$ for the stated value of $c$, whence $\gamma_u(G) \leqslant c$ as required.

The case $G = \Omega_8^+(2)$ requires more attention. If $s$ is in 15A, then

$$F(x, s) := \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H) > 1 \tag{6.6}$$

for some elements $x \in G$ of prime order and thus $\widehat{Q}(G, s, d) > 1$ for all $d \geqslant 1$. However, the proof of [24, Proposition 6.2] gives

$$P(x, s) = \frac{|\{z \in s^G \,:\, G \neq \langle x, z\rangle\}|}{|s^G|} < \frac{7}{10}$$

for all elements $x \in G$ of prime order. Therefore, $P(x, s) \leqslant \min\{F(x, s), 7/10\} =: Q(x, s)$ and thus

$$Q(G, s, 26) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot P(x_i, s)^{26} \leqslant \sum_{i=1}^{k} |x_i^G| \cdot Q(x_i, s)^{26} < 1$$

(see (2.4)). This gives $\gamma_u(G) \leqslant 26$ as claimed. □

For the remainder, we can assume $r > 1$ and $G \notin \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$. Define an integer $R(G)$ as follows:

| $G$ | $\mathrm{L}_{r+1}(q)$ | $\mathrm{U}_{r+1}(q)$ | $\mathrm{PSp}_{2r}(q)$ | $\mathrm{P}\Omega_{2r}^+(q)$ | $\mathrm{P}\Omega_{2r}^-(q)$ |
|---|---|---|---|---|---|
| $R(G)$ | 6 | 7 | 4 | 4 | 6 |

**Remark 6.15.** Suppose $G \notin \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$, $r < R(G)$ and $G \neq \mathrm{Sp}_4(2)' \cong A_6$. Then $|\mathcal{M}(G, s)| = 1$ for the element $s \in G$ identified in the proof of Theorem 6.1.

The following lemma on fixed point ratios is our key tool in the proof of Theorem 6.3. The proof uses several results on fixed point ratios for primitive actions of finite simple classical groups. For example, if $H$ acts reducibly on the natural module $V$ then we appeal to the bounds on $\mathrm{fpr}(x, G/H)$ obtained by Guralnick and Kantor in [24, Section 3]. For an irreducible subgroup $H$, we apply the main theorem of [12]. For instance, if $H$ is irreducible and the rank $r$ of $G$ is large enough, then [12, Corollary 2] states that

$$\mathrm{fpr}(x, G/H) < 2q^{-\frac{r(r-1)}{r+1}} \tag{6.7}$$

for all $x \in G$ of prime order (in particular, this holds if $\dim V \geqslant 7$). In the statement of the lemma, we define $F(x, s)$ as in (6.6).

**Lemma 6.16.** *Let $G \notin \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ be a finite simple classical group of rank $r \geqslant R(G)$. Then there exists $s \in G$ such that for all elements $x \in G$ of prime order*

$$F(x, s) < \min\left\{\frac{c}{q^2}, \frac{c}{q^{r/2-3/2}}\right\}$$

*where $c = 3$ unless $G = \mathrm{L}_{r+1}(q)$, in which case $c = 4$.*

*Proof.* Throughout, let $x \in G$ be an element of prime order. We partition the proof into four cases:

(a) $G \in \{\mathrm{L}_{r+1}(q) : r \geqslant 6\} \cup \{\mathrm{U}_{r+1}(q) : r \geqslant 8 \text{ even}\}$.
(b) $G \in \{\mathrm{P}\Omega^-_{2r}(q) : r \geqslant 6\} \cup \{\mathrm{PSp}_{2r}(q) : r \geqslant 6 \text{ even}, q \text{ odd}\}$.
(c) $G = \mathrm{P}\Omega^+_{2r}(q)$, where $r \geqslant 6$ is even.
(d) $G = \mathrm{PSp}_8(q)$ with $q$ odd, or $G = \mathrm{P}\Omega^+_8(q)$ and $q \geqslant 4$.

First consider (a). The case $G = \mathrm{L}_{11}(2)$ requires special attention. If $s \in G$ has order $2^{11}-1$ then the proof of [24, Proposition 6.3] gives $\mathcal{M}(G,s) = \{H\}$ with $H$ a field extension subgroup of type $\mathrm{GL}_1(2^{11})$. By applying the bound in (6.7), we deduce that $F(x,s) = \mathrm{fpr}(x, G/H) < 2^{-79/11}$ and the result follows.

For the other groups in (a), let $s \in G$ be the element defined in [24, Table II]. As explained in the proof of [24, Proposition 4.1], the maximal overgroups of $s$ are the obvious reducible subgroups, and [24, Propositions 3.15 and 3.16] supply upper bounds on the associated fixed point ratios. It is now straightforward to verify the desired bound. For example, suppose $G = \mathrm{L}_{r+1}(q)$ with $r \geqslant 6$. As in [24, Table II], we take

$$s = \begin{cases} \frac{r+2}{2} \oplus \frac{r}{2} & \text{if } r \text{ is even} \\ \frac{r+5}{2} \oplus \frac{r-3}{2} & \text{if } r \equiv 1 \pmod 4 \\ \frac{r+3}{2} \oplus \frac{r-1}{2} & \text{if } r \equiv 3 \pmod 4, \end{cases}$$

noting that $\mathcal{M}(G,s) = \{H, K\}$ where $H$ and $K$ are the stabilisers of appropriate $k$- and $(r+1-k)$-spaces with $k \leqslant r/2$. By [24, Proposition 3.1(i)], if $L \leqslant G$ is the stabiliser of an $\ell$-space with $\ell \leqslant (r+1)/2$, then $\mathrm{fpr}(y, G/H) < 2q^{-\ell}$ for all $1 \neq y \in G$. Therefore,

$$F(x,s) = \mathrm{fpr}(x, G/H) + \mathrm{fpr}(x^\tau, G/H) < \min\left\{\frac{4}{q^2}, \frac{4}{q^{r/2-3/2}}\right\},$$

where $\tau \in \mathrm{Aut}(G)$ is an involutory graph automorphism. A similar argument applies when $G = \mathrm{U}_{r+1}(q)$ with $r \geqslant 8$ even and we omit the details.

Next consider the groups in (b). Let $s \in G$ be a Singer cycle (that is, $s$ generates an irreducible cyclic subgroup of maximal possible order). By the main theorem of Bereczky [5], the maximal overgroups of $s$ are field extension subgroups and [12] provides upper bounds on the associated fixed point ratios. We will assume $G = \mathrm{P}\Omega^-_{2r}(q)$ with $r \geqslant 6$; the other case is very similar.

By [5], the members of $\mathcal{M}(G,s)$ are subgroups of type $\mathrm{GU}_r(q)$ and $O^-_{2r/k}(q^k)$, where $k$ is a prime divisor of $r$. In addition, if $qr$ is odd, then there are also field extension subgroups of type $O_r(q^2)$. A straightforward calculation shows that $\mathcal{M}(G,s)$ contains exactly one of each such subgroup. From [13, Corollary 3.38] we get

$$|x^G| > \frac{1}{4}\left(\frac{q}{q+1}\right) q^{4r-6}$$

and thus [12, Theorem 1] implies that

$$\mathrm{fpr}(x, G/H) < |x^G|^{-\frac{1}{2}+\frac{1}{2r}+\frac{1}{2r-2}} < \left(\frac{1}{4}\left(\frac{q}{q+1}\right) q^{4r-6}\right)^{-\frac{1}{2}+\frac{1}{2r}+\frac{1}{2r-2}} < \frac{2}{q^{r-1}} \tag{6.8}$$

for each $H \in \mathcal{M}(G,s)$. Therefore,

$$F(x,s) < \frac{2(2+\log_2 r)}{q^{r-1}} < \min\left\{\frac{3}{q^2}, \frac{3}{q^{r/2-3/2}}\right\}.$$

Next let us turn to case (c), so $G = \mathrm{P}\Omega^+_{2r}(q)$ and $r \geqslant 6$ is even. Fix an element $s = (r-2)^- \perp (r+2)^- \in G$. Then [10, Proposition 5.14] implies that $\mathcal{M}(G,s) = \{L, H_1, H_2\}$, where $L$ is a reducible subgroup of type $O^-_{r-2}(q) \times O^-_{r+2}(q)$ and $H_1, H_2$ are field extension

subgroups of type $O_r^+(q^2)$. By applying [24, Proposition 3.16] and the bound in (6.7), we get

$$F(x,s) < \left(\frac{3}{q^{r-2}} + \frac{1}{q^{r-1}} + \frac{1}{q^{r/2}}\right) + 4q^{-\frac{r(r-1)}{r+1}} < \min\left\{\frac{3}{q^2}, \frac{3}{q^{r/2-3/2}}\right\}. \tag{6.9}$$

Finally, we handle the two cases in (d). First assume $G = \mathrm{PSp}_8(q)$ and $q$ is odd. Take $s = 2 \perp 6 \in G$ and note that the proof of [24, Proposition 4.1] implies that $\mathcal{M}(G,s) = \{H\}$, where $H$ is of type $\mathrm{Sp}_2(q) \times \mathrm{Sp}_6(q)$. By applying [31, Proposition 3.5] we deduce that $F(x,s) < 2q^{-2}$ and the result follows. Finally, suppose $G = \mathrm{P}\Omega_8^+(q)$ with $q \geqslant 4$. Let $s \in G$ be an element of order $(q^2+1)/(q-1,2)$. By [10, Proposition 5.15], $\mathcal{M}(G,s)$ contains three subgroups of type $O_4^-(q) \wr S_2$, plus an additional subfield subgroup of type $O_8^-(q^{1/2})$ if $q$ is a square. Now $|x^G| \geqslant (q^2+1)^2(q^6-1)$ (minimal if $q$ is even and $x$ is an $a_2$ involution), so the main theorem of [12] implies that

$$F(x,s) < 4\left((q^2+1)^2(q^6-1)\right)^{-\frac{1}{2}+\frac{1}{8}} < \frac{3}{q^2}$$

and the result follows. This completes the proof of the lemma. □

We are now ready to complete the proof of Theorem 6.3.

**Proposition 6.17.** *Let $G$ be a finite simple classical group of rank $r$. Then*

$$\gamma_u(G) \leqslant 7r + 56.$$

*Proof.* We have already verified the bounds in parts (i), (ii) and (iii) of Theorem 6.3, so we may assume that $r > 1$ and $G \notin \mathcal{A} \cup \mathcal{B}$. In addition, we can assume that $G \notin \mathcal{C}$ (see Proposition 6.14) and $G \neq \mathrm{Sp}_4(2)' \cong A_6$ (see the remark following the statement of Theorem 6.3). Note that if $G$ is linear or unitary, then $|G| < q^{r^2+2r}$. In general, $|G| < q^{2r^2+\varepsilon r}$, where $\varepsilon = 1$ if $q$ is odd, otherwise $\varepsilon = -1$ (since the symplectic groups in even characteristic are contained in $\mathcal{B}$). We will use the notation from Lemma 2.5.

First assume $r \geqslant 7$ and $(r,q) \neq (7,2), (8,2)$. Choose $s \in G$ as in Lemma 6.16. If $G$ is linear or unitary, then we deduce that

$$\widehat{Q}(G,s,7r+56) < q^{r^2+2r} \cdot \left(\frac{4}{q^{r/2-3/2}}\right)^{7r+56} < 1,$$

so Lemma 2.5 implies that $\gamma_u(G) \leqslant 7r+56$. Similarly, if $G$ is symplectic or orthogonal, then

$$\widehat{Q}(G,s,7r+56) < q^{2r^2+\varepsilon r} \cdot \left(\frac{3}{q^{r/2-3/2}}\right)^{7r+56} < 1,$$

and once again we conclude that $\gamma_u(G) \leqslant 7r+56$.

Now assume $(r,q) = (7,2)$, so $\Omega_{14}^-(2)$ (recall that $G \notin \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$). As in the proof of Lemma 6.16, let $s \in G$ be a Singer cycle (so $|s| = 2^7+1$) and note that $\mathcal{M}(G,s) = \{H_1, H_2\}$, where $H_1$ is of type $\mathrm{GU}_7(2)$ and $H_2$ is of type $O_2^-(2^7)$. In view of the upper bound in (6.8), we deduce that $F(x,s) < 2^{-4}$ and this immediately implies that $\widehat{Q}(G,s,7r+56) < 1$.

Similar arguments apply when $(r,q) = (8,2)$. If $G = \mathrm{U}_9(2)$, then $|G| < 2^{80}$ and the upper bound on $F(x,s)$ in Lemma 6.16 is sufficient. If $G = \Omega_{16}^-(2)$ then we choose $s$ as in the proof of Lemma 6.16, so the subgroups in $\mathcal{M}(G,s)$ are of type $\mathrm{GU}_8(2)$ and $O_8^-(4)$ (one subgroup of each type). From the bound in (6.8) we get $F(x,s) < 2^{-5}$ and the desired result quickly follows. Similarly, if $G = \Omega_{16}^+(2)$ then the upper bound in (6.9) gives $F(x,s) < 2^{-2}$ and this implies that $\widehat{Q}(G,s,7r+56) < 1$ as required.

Finally, let us assume $r < 7$. First suppose $r \geqslant R(G)$, in which case we choose $s \in G$ as in Lemma 6.16. If $G = \mathrm{L}_7(q)$, then $r = 6$ and

$$\widehat{Q}(G, s, 7r + 56) < q^{r^2+2r} \cdot \left(\frac{4}{q^2}\right)^{7r+56},$$

which is less than 1 if $q \geqslant 3$ (note that $\mathrm{L}_7(2)$ is in the collection $\mathcal{C}$). Similarly, if $G \neq \mathrm{L}_7(q)$ then

$$\widehat{Q}(G, s, 7r + 56) < q^{2r^2+\varepsilon r} \cdot \left(\frac{3}{q^2}\right)^{7r+56}$$

and it just remains to handle the groups $\Omega^{\pm}_{12}(2)$ (for example, if $(r, q) = (5, 2)$ and $r \geqslant R(G)$ then $G = \mathrm{Sp}_{10}(2)$ or $\Omega^{+}_{10}(2)$, both of which belong to $\mathcal{A} \cup \mathcal{B}$). For $G = \Omega^{-}_{12}(2)$ we take a Singer cycle $s \in G$, in which case (6.8) implies that $F(x, s) < 3/16$ and we get $\widehat{Q}(G, s, 7r + 56) < 1$. Similarly, if $G = \Omega^{+}_{12}(2)$ and $s = 4^- \perp 8^-$ then the upper bound on $F(x, s)$ in (6.9) is good enough to give $\widehat{Q}(G, s, 7r + 56) < 1$.

To complete the proof, we may assume $r < R(G)$. As noted in Remark 6.15, there exists $s \in G$ such that $\mathcal{M}(G, s) = \{H\}$ for some subgroup $H$, so $\gamma_u(G) \leqslant b(G, G/H)$ by Corollary 2.2. If $H$ is reducible, then $b(G, G/H) \leqslant \dim V + 11$ by Proposition 6.5, where $V$ is the natural module for $G$. Otherwise, $b(G, G/H) \leqslant 5$ by the main theorem of [14]. In all cases, the result follows. □

This completes the proof of Theorem 6.3, and hence Theorem 4.

**Remark 6.18.** It is easy to improve the bound in Proposition 6.17 in special cases. For example, we have already shown that better bounds hold when $G$ is one of the groups covered by parts (i), (ii) or (iii) of Theorem 6.3. In other cases, the proof of Proposition 6.17 also yields better bounds. For instance, suppose $G = \mathrm{U}_{r+1}(q)$, with $r \geqslant 7$ and $q \geqslant 4$. Then $|G| < q^{r^2+2r}$ and one checks that

$$\widehat{Q}(G, s, 2r + 40) < q^{r^2+2r} \cdot \left(\frac{3}{q^{r/2-3/2}}\right)^{2r+40} < 1$$

for the element $s \in G$ given in Lemma 6.16. Therefore, $\gamma_u(G) \leqslant 2r + 40$.

## References


[1] J. Araújo, J.P. Araújo, P.J. Cameron, T. Dobson, A. Hulpke and P. Lopes, *Imprimitive permutations in primitive groups*, J. Algebra **486** (2017), 396–416.

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

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

[4] P.T. Bateman and R.M. Stemmler, *Waring's problem for algebraic number fields and primes of the form* $(p^r - 1)/(p^d - 1)$, Illinois J. Math. **6** (1962), 142–156.

[5] Á. Bereczky, *Maximal overgroups of Singer elements in classical groups*, J. Algebra **234** (2000), 187–206.

[6] W. Bosma, J. Cannon and C. Playoust, *The* Magma *algebra system I: The user language*, J. Symb. Comput. **24** (1997), 235–265.

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

[8] T. Breuer, *The* GAP *Character Table Library, Version 1.2.1*, GAP package, `http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib`, 2012.

[9] T. Breuer, *GAP computations concerning probabilistic generation of finite simple groups*, preprint (arxiv:0710.3267).

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

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

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

[13] T.C. Burness, *Fixed point ratios in actions of finite classical groups, II* J. Algebra **309** (2007), 80–138.
[14] T.C. Burness, *On base sizes for actions of finite classical groups*, J. London Math. Soc. **75** (2007), 545–562.
[15] T.C. Burness, *Simple groups, generation and probabilistic methods*, in Proceedings of Groups St Andrews 2017, preprint (arxiv:1710.10434).
[16] T.C. Burness and S. Guest, *On the uniform spread of almost simple linear groups*, Nagoya Math. J. **109** (2013), 35–109.
[17] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for symmetric groups*, Bull. London Math. Soc. **44** (2011), 386–391.
[18] T.C. Burness and S. Harper, *Computations concerning the uniform domination number of a finite simple group*, available at `http://seis.bristol.ac.uk/~tb13602/udncomp.pdf`.
[19] 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.
[20] T.C. Burness, E.A. O'Brien and R.A. Wilson, *Base sizes for sporadic groups*, Israel J. Math. **177** (2010), 307–333.
[21] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.
[22] J.D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.
[23] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.8.7, 2017, (`http://www.gap-system.org`).
[24] R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.
[25] R.M. Guralnick and K. Magaard, *On the minimal degree of a primitive permutation group*, J. Algebra **207** (1998), 127–145.
[26] R.M. Guralnick and G. Malle, *Products of conjugacy classes and fixed point spaces*, J. Amer. Math. Soc. **25** (2012), 77–121.
[27] 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.
[28] R.M. Guralnick and A. Shalev, *On the spread of finite simple groups*, Combinatorica **23** (2003), 73–87.
[29] Z. Halasi, *On the base size of the symmetric group acting on subsets*, Stud. Sci. Math. Hung. **49** (2012), 492–500.
[30] Z. Halasi, M.W. Liebeck and A. Maróti, *Base sizes of primitive groups: A bound with explicit constants*, preprint.
[31] S. Harper, *On the uniform spread of almost simple symplectic and orthogonal groups*, J. Algebra **470** (2017), 330–371.
[32] M.A. Henning, *A survey of selected recent results on total domination in graphs*, Discrete Math. **309** (2009), 32–63.
[33] G.A. Jones, *Cyclic regular subgroups of primitive permutation groups*, J. Group Theory **5** (2002), 403–407.
[34] W.M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.
[35] 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.
[36] 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.
[37] M.W. Liebeck, C.E. Praeger and J. Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), 365–383.
[38] M.W. Liebeck and J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces*, Proc. London Math. Soc. **63** (1991), 266–314.
[39] M.W. Liebeck, J. Saxl and G.M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proc. London Math. Soc. **65** (1992), 297–325.
[40] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.
[41] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.
[42] A. Maróti, *On the orders of primitive groups*, J. Algebra **258** (2002), 631–640.
[43] 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.
[44] A. Stein, $1\frac{1}{2}$*-generation of finite simple groups*, Beiträge Algebra Geom. **39** (1998), 349–358.

[45] R. Steinberg, *Generators for simple groups*, Canad. J. of Math. **14** (1962), 277–283.
[46] T.S. Weigel, *Generation of exceptional groups of Lie-type*, Geom. Dedicata **41** (1992), 63–87.
[47] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York (1964).
[48] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
*E-mail address*: t.burness@bristol.ac.uk

S. Harper, School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
*E-mail address*: scott.harper@bristol.ac.uk