FINITE GROUPS, 2-GENERATION
AND THE UNIFORM DOMINATION NUMBER

BY

TIMOTHY C. BURNESS AND SCOTT HARPER

School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
e-mail: t.burness@bristol.ac.uk, scott.harper@bristol.ac.uk

ABSTRACT

Let G be a finite 2-generated non-cyclic group. The spread of G is the
largest integer k such that for any nontrivial elements $x_1, \ldots, x_k$, there
exists $y \in G$ such that $G = \langle x_i, y \rangle$ for all i. The more restrictive notion
of uniform spread, denoted $u(G)$, requires y to be chosen from a fixed
conjugacy class of G, and a theorem of Breuer, Guralnick and Kantor
states that $u(G) \geqslant 2$ for every non-abelian finite simple group G. For any
group with $u(G) \geqslant 1$, we define the uniform domination number $\gamma_u(G)$ of
G to be the minimal size of a subset S of conjugate elements such that for
each nontrivial $x \in G$ there exists $y \in S$ with $G = \langle x, y \rangle$ (in this situation,
we say that S is a uniform dominating set for G). We introduced the
latter notion in a recent paper, where we used probabilistic methods to
determine close to best possible bounds on $\gamma_u(G)$ for all simple groups G.

In this paper we establish several new results on the spread, uniform
spread and uniform domination number of finite groups and finite simple
groups. For example, we make substantial progress towards a classification
of the simple groups G with $\gamma_u(G) = 2$, and we study the associated
probability that two randomly chosen conjugate elements form a uniform
dominating set for G. We also establish new results concerning the 2-
generation of soluble and symmetric groups, and we present several open
problems.

CONTENTS

1. Introduction

Let G be a finite non-cyclic group that can be generated by two elements. It is natural to study the properties of generating pairs for G and such problems have attracted a great deal of attention over several decades, especially in the context of finite simple groups. Here we begin by introducing the generation invariants and associated probabilities that will be the main focus of this paper.

In [10], Brenner and Wiegold define the **spread** of G, denoted $s(G)$, to be the largest integer k such that for any nontrivial elements $x_1, \ldots, x_k$ in G, there exists $y \in G$ such that $G = \langle x_i, y \rangle$ for all i. This leads naturally to the more restrictive notion of **uniform spread**, denoted $u(G)$, which was introduced more recently by Breuer, Guralnick and Kantor [13]. This is defined to be the largest integer k such that there is a conjugacy class C of G with the property that for any nontrivial elements $x_1, \ldots, x_k$ in G, there exists $y \in C$ such that $G = \langle x_i, y \rangle$ for all i. Clearly,

$$s(G) \geqslant u(G) \geqslant 0.$$

It is easy to see that if $s(G) \geqslant 1$, then every proper quotient of G is cyclic. In fact, it is conjectured that this condition on quotients is equivalent to the positive spread property; see [13, Conjecture 1.8], and recent progress towards a proof of this conjecture in [25, 48, 49].

In [27], we introduced some new generation invariants, which can be viewed as natural extensions of spread and uniform spread. Following [27], we say that a subset $S \subseteq G$ of nontrivial elements is a **total dominating set** (TDS) for G if for all nontrivial $x \in G$, there exists $y \in S$ such that $G = \langle x, y \rangle$. To explain the terminology, note that if $\Gamma(G)$ is the **generating graph** of G, whose vertices are the nontrivial elements of G and $x, y \in G$ are adjacent if and only if $G = \langle x, y \rangle$, then S is a TDS for G if and only if it is a total dominating set for $\Gamma(G)$ in the usual graph-theoretic sense. Consequently, if $s(G) \geqslant 1$, then the **total domination number** of G is defined by

$$\gamma_t(G) = \min\{|S| : S \text{ is a TDS for } G\}.$$

Similarly, if $u(G) \geqslant 1$, then G contains a **uniform dominating set** (UDS), which is defined to be a TDS of conjugate elements, and the **uniform domination number** of G is

$$\gamma_u(G) = \min\{|S| : S \text{ is a UDS for } G\}.$$

Observe that if $u(G) \geqslant 1$, then

$$2 \leqslant \gamma_t(G) \leqslant \gamma_u(G) \leqslant |C|$$

for some conjugacy class C of G (if $u(G) = 0$, then $\gamma_u(G)$ is undefined).

Probabilistic methods play an important role in the study of uniform spread and the uniform domination number. For an element $s \in G$ and a positive integer c, we define

$$(1) \quad P(G, s, c) = \frac{|\{(x_1, \ldots, x_c) \in (s^G)^c : \{x_1, \ldots, x_c\} \text{ is a UDS for } G\}|}{|s^G|^c},$$

the probability that c randomly chosen conjugates of s form a UDS for G. In addition, we define

$$(2) \qquad\qquad P_c(G) = \max\{P(G, s, c) : s \in G\},$$

so $\gamma_u(G) \leqslant c$ if and only if $P_c(G) > 0$.

There is a vast literature on the remarkable generation properties of finite simple groups. The starting point is a theorem of Steinberg [68], which states that every finite simple group of Lie type is 2-generated. It is easy to see that every alternating group is 2-generated and the same is true for all sporadic simple groups by a theorem of Aschbacher and Guralnick [1]. Therefore, by

appealing to the Classification of Finite Simple Groups, we conclude that every finite simple group is 2-generated (without the classification, there is no known bound on the number of generators needed for a finite simple group). This observation leads to many natural problems concerning the distribution of generating pairs across a simple group, which have been intensively studied in recent years (see the recent survey article [22] for more details).

The main result on the uniform spread of simple groups is the following theorem, which combines results from [13] and [46].

THEOREM ($\star$):

(i) If G is a finite non-abelian simple group, then $u(G) \geqslant 2$, with equality if and only if

$$G \in \{A_5, A_6, \Omega_8^+(2), \mathrm{Sp}_{2r}(2)\, (r \geqslant 3)\}.$$

(ii) Let (G_n) be a sequence of finite non-abelian simple groups with $|G_n| \to \infty$. Then either $u(G_n) \to \infty$, or there is an infinite subsequence consisting of either

(a) alternating groups of degree all divisible by a fixed prime; or
(b) odd-dimensional orthogonal groups over a field of fixed size; or
(c) symplectic groups over a field of even characteristic and fixed size.

Here part (i) is due to Breuer, Guralnick and Kantor [13, Theorem 1.2], extending earlier work of Guralnick and Kantor [45], and independently Stein [67], who established the weaker bound $u(G) \geqslant 1$. The asymptotic statement in part (ii) is a theorem of Guralnick and Shalev [46, Corollary 2.3]. Note that the cases described in parts (a)–(c) of part (ii) are genuine exceptions. For example, if $n \geqslant 6$ is composite, then [46, Proposition 2.4] gives

$$(3) \qquad s(A_n) < \binom{2p+1}{3},$$

where p is the smallest prime divisor of n. Similarly, [46, Proposition 2.5] states that $s(\mathrm{Sp}_{2m}(q)') \leqslant q$ if q is even and $s(\Omega_{2m+1}(q)) \leqslant \frac{1}{2}q(q+1)$ if q is odd, for all $m, q \geqslant 2$.

In view of Theorem ($\star$) it is natural to study the uniform domination number of simple groups. In [27], we developed probabilistic and computational methods to study $\gamma_u(G)$ and we used these techniques to determine close to best possible bounds for simple groups. For example, we showed that there are infinitely

many simple groups G with $\gamma_u(G) = 2$, including the alternating groups A_n when $n \geqslant 13$ is prime. In contrast, we proved that the uniform domination number is in general unbounded for finite simple groups; for instance,

$$\gamma_u(A_n) \geqslant \lceil \log_2 n \rceil - 1$$

for all even integers $n \geqslant 6$ (see [27, Theorems 1 and 2]).

A key observation in [27] is the connection between the uniform domination number and the classical concept of bases in permutation group theory, which allows us to apply recent work on bases for almost simple primitive groups. In order to explain this relationship, recall that if G acts faithfully on a finite set Ω, then a subset of Ω is a **base** for G if its pointwise stabiliser in G is trivial. We write $b(G, \Omega)$ for the **base size** of G, which is the minimal size of a base. The connection in [27] arises from the easy observation that if there is an element $s \in G$ contained in a unique maximal subgroup H of G, then $P(G, s, c) > 0$ if and only if $b(G, G/H) \leqslant c$, whence $\gamma_u(G) \leqslant b(G, G/H)$ (see Section 2.2 for further details).

Our initial investigations in [27] lead to a number of natural problems, which we seek to address in this paper. For example, one of our aims is to extend the study of the simple groups G with the extremal property $\gamma_u(G) = 2$, with a view towards a complete classification. For such a group G, we will also investigate the corresponding probability $P_2(G)$ (see (2)) and its asymptotic properties (with respect to a sequence of such groups). We will also revisit earlier work of Binder [5, 6, 7] from the 1960s on the spread of symmetric groups, together with results of Brenner and Wiegold [10] from the 1970s on soluble groups and the simple linear groups $L_2(q)$. In particular, we take the opportunity to bring together several important results on the 2-generation of finite groups that are somewhat scattered through the literature.

We now present the main results of the paper. Our first theorem concerns soluble groups.

THEOREM 1: *Let G be a finite non-abelian soluble group such that every proper quotient is cyclic. Then $G = N{:}H$, where $N = (C_p)^f$ for some prime p and integer $f \geqslant 1$, and H is cyclic and acts faithfully and irreducibly on N. Moreover, the following hold:*

(i) *$s(G) = |N| - \epsilon$ and $u(G) = |N| - 1$, where $\epsilon = 0$ if $|H|$ is a prime and $\epsilon = 1$ otherwise.*

(ii) *$\gamma_u(G) = 2$ and $P_2(G) = 1 - |N|^{-1}$.*

Remark 1: Let us make some comments on the statement of Theorem 1:

(a) In part (i), the result on $s(G)$ is due to Brenner and Wiegold (see [10, Theorem 2.01]).

(b) Let $G = N{:}H$ be a soluble group as in the theorem and let $s \in G$ be a nontrivial element. We will show that $P(G, s, 2) > 0$ if and only if s generates a complement of N (see Proposition 3.5), in which case any two distinct conjugates of s form a uniform dominating set and thus $P(G, s, 2) = 1 - |N|^{-1}$ since s is self-centralising.

(c) The corresponding result for a non-cyclic abelian group G is transparent. Indeed, the condition on quotients implies that $G = C_p \times C_p$ for some prime p and it is easy to see that $s(G) = p$ and $u(G) = 0$.

Next we turn to symmetric groups.

THEOREM 2: *Let $G = S_n$ with $n \geqslant 5$.*

(i) *We have*

$$s(G) = \begin{cases} 2 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd} \end{cases} \quad \text{and} \quad u(G) = \begin{cases} 0 & \text{if } n = 6, \\ 2 & \text{otherwise.} \end{cases}$$

(ii) *For all n,*

$$\gamma_u(G) \geqslant \gamma_t(G) \geqslant \lceil \log_2 n \rceil \geqslant 3.$$

(iii) *Suppose n is odd and Ω is the set of $\lfloor \frac{n}{2} \rfloor$-element subsets of $\{1, \ldots, n\}$. Then*

$$\gamma_u(G) = b(G, \Omega) \leqslant 2 \log_2 n.$$

(iv) *If n is even, then*

$$\gamma_u(G) \leqslant 3n \log_2 n.$$

Remark 2: Let us record some comments on the statement of Theorem 2:

(a) The equality $u(S_n) = 2$ for $n \neq 6$ is the main feature of part (i). Indeed, the calculation of $s(S_n)$ is due to Binder [5, 6]. In addition, Binder [7] showed that $u(S_n) \geqslant 1$ if $n \neq 6$ (as noted in [25, Theorem 2], we have $u(S_6) = 0$).

(b) For (iii), the upper bound (and its proof) is analogous to the upper bound on $\gamma_u(A_{2m})$ obtained in [27] (see Theorem 3(i) below). It is also worth noting that the base size $b(G, \Omega)$ is not known exactly (see [47]).

(c) It is easy to handle the small degree symmetric groups excluded in the theorem. By Theorem 1 we have $s(S_3) = 3$, $u(S_3) = 2$, $\gamma_u(S_3) = 2$ and $P_2(S_3) = \frac{2}{3}$. Since S_4 has a proper non-cyclic quotient, we see that $s(S_4) = u(S_4) = 0$.

For alternating groups, our main result is the following.

THEOREM 3: *Let $G = A_n$ with $n \geqslant 5$.*

(i) *If n is even, then*

$$s(G) = u(G) = \begin{cases} 2 & \text{if } n = 6 \\ 4 & \text{otherwise} \end{cases}$$

and

$$\log_2 n \leqslant \gamma_t(G) \leqslant \gamma_u(G) \leqslant 2 \log_2 n.$$

(ii) *If $n \geqslant 9$ is odd, then $u(G) \geqslant 4$ and*

$$\log_p n \leqslant \gamma_t(G) \leqslant \gamma_u(G) \leqslant 77 \log_2 n,$$

where p is the smallest prime divisor of n.

(iii) *We have $\gamma_u(G) = 2$ if and only if $n \geqslant 13$ is a prime.*

(iv) *If $n > 13$ is a prime, then $P_2(G) > 1 - n^{-1}$.*

Remark 3: Some remarks on the statement of Theorem 3:

(a) In part (i), the result on $s(G)$ and $u(G)$ is due to Brenner and Wiegold [10, (3.01)–(3.05)] and the upper bound on $\gamma_u(G)$ is taken from [27, Theorem 2]. The lower bound is established in Proposition 4.12.

(b) Part (ii) extends the bound $u(G) \geqslant 3$ established in [13] (with essentially the same proof). The excluded cases $n \in \{5, 7\}$ are genuine exceptions: it is straightforward to show that $s(A_5) = u(A_5) = 2$ and $s(A_7) = u(A_7) = 3$. The upper bound on $\gamma_u(G)$ is [27, Proposition 3.15] and the lower bound follows from Proposition 4.12.

(c) In stark contrast to the even degree case, the uniform spread of an odd-degree alternating group can be arbitrarily large. Indeed, this is a consequence of part (ii) of Theorem $(\star)$. More precisely, [46, Proposition 3.1] states that if n is composite and p is the smallest prime divisor of n, then

$$s(A_n) \geqslant cp \log p$$

for some (undetermined) absolute constant c. We refer the reader to [46, Propositions 3.2 and 3.3] for explicit bounds on $u(A_n)$ and $s(A_n)$ when n is a prime (also see [10, Section 4]).

(d) Part (iii) extends [27, Theorem 3.7(i)], which states that $\gamma_u(A_n) = 2$ if $n \geqslant 13$ is a prime. This can be viewed as a first step towards a classification of the finite simple groups G with $\gamma_u(G) = 2$ (see Corollary 7 below). In addition, if $n \geqslant 13$ is a prime, then $P(A_n, s, 2) > 0$ if and only if s is an n-cycle (see Proposition 5.5).

(e) In part (iv), the case $n = 13$ is an anomaly. Indeed, with the aid of MAGMA [9], one can show that

$$P_2(A_{13}) = \frac{4979}{46200}$$

(see Remark 5.10 for further details).

Next we consider the finite simple groups of Lie type. Our main result for exceptional groups is the following. Let

$$\mathcal{E} = \{{}^2B_2(q), {}^2G_2(q)\,(q \geqslant 27), {}^2F_4(q)\,(q \geqslant 8), {}^3D_4(q), E_6^\epsilon(q), E_7(q), E_8(q)\}.$$

THEOREM 4: *Let G be a finite simple exceptional group of Lie type over $\mathbb{F}_q$.*

  (i) *We have $\gamma_u(G) \leqslant 5$, with $\gamma_u(G) = 2$ if and only if $G \in \mathcal{E}$.*

 (ii) *If $\gamma_u(G) = 2$, then $P_2(G) > 1 - q^{-1}$.*

Remark 4: Let us make some remarks on the statement of Theorem 4:

(a) The bound on $\gamma_u(G)$ in part (i) strengthens the result $\gamma_u(G) \leqslant 6$ stated in [27, Theorem 5.2]. The same result states that $\gamma_u(G) = 2$ if G is ${}^2B_2(q)$, ${}^2G_2(q)$ (with $q \geqslant 27$), or $E_8(q)$, and the complete classification of the exceptional groups G with $\gamma_u(G) = 2$ is the main feature of Theorem 4.

(b) The lower bound on $P_2(G)$ in part (ii) is essentially best possible. For example, if $G = {}^2B_2(q)$, then

$$P_2(G) = 1 - \frac{(q^2 - 4)(q - \sqrt{2q} + 1) + 4}{q^2(q - 1)(q + \sqrt{2q} + 1)}$$

(see Lemma 6.7 and Remark 6.8). Stronger bounds are obtained in many cases. For instance, if $G = E_8(q)$ then $P_2(G) > 1 - q^{-30}$ by Lemma 6.11.

Finally, let us turn to the classical groups. The two-dimensional linear groups merit special attention and they are handled in the following result.

THEOREM 5: *Let $G = L_2(q)$ with $q \geqslant 4$.*

(i) *If $q \geqslant 11$ and $q \not\equiv 3 \pmod 4$, then*

$$s(G) = u(G) = \begin{cases} q - 1 & \text{if } q \equiv 1 \pmod 4, \\ q - 2 & \text{if } q \text{ is even.} \end{cases}$$

(ii) *If $q \equiv 3 \pmod 4$ and $q \geqslant 11$, then $u(G) \geqslant q - 4$ and $s(G) \geqslant q - 3$.*

(iii) *If $q \equiv 3 \pmod 4$ and $q \geqslant 11$ is a prime, then*

$$s(G) \geqslant \frac{1}{2}(3q - 7) \quad \text{and} \quad s(G) - u(G) = \frac{1}{2}(q + 1).$$

(iv) *We have*

$$\gamma_u(G) = \begin{cases} 4 & \text{if } q = 9, \\ 3 & \text{if } q \in \{5, 7\} \text{ or } q \text{ is even,} \\ 2 & \text{if } q \geqslant 11 \text{ is odd.} \end{cases}$$

(v) *If $q \geqslant 11$ is odd, then*

$$P_2(G) = \begin{cases} \frac{1}{2}(1 + \frac{1}{q}) & \text{if } q \equiv 1 \pmod 4 \\ \frac{1}{2}(1 - \frac{q+3}{q(q-1)}) & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

In particular, $P_2(G) \geqslant \frac{24}{55}$, with equality if and only if $q = 11$.

Remark 5: Let us make some comments on the statement of Theorem 5:

(a) The spread of $G = L_2(q)$ was first studied by Brenner and Wiegold in [10]. According to [10, Theorem 4.02], if $q \geqslant 11$ or q is even, then $s(G) = f(q)$ where

$$f(q) = \begin{cases} q - 1 & \text{if } q \equiv 1 \pmod 4, \\ q - 4 & \text{if } q \equiv 3 \pmod 4, \\ q - 2 & \text{if } q \text{ is even.} \end{cases}$$

However, the proof in [10] is incomplete and only the lower bound $s(G) \geqslant f(q)$ is established. With some additional work, we can show that $s(G) = f(q)$ when $q \not\equiv 3 \pmod 4$ and $q \geqslant 13$ (see Theorem 7.3), which establishes part (i) of Theorem 5. However, the case $q \equiv 3 \pmod 4$

is rather more complicated and we have been unable to compute $s(G)$ and $u(G)$ precisely. Note that part (ii) shows that the statement of [10, Theorem 4.02] is incorrect in this case.

(b) Part (iii) demonstrates that the difference $s(G) - u(G)$ can be arbitrarily large. As far as we are aware, this provides the first example of an infinite family of non-abelian finite groups with this property.

(c) It is straightforward to handle the small values of q excluded in parts (i), (ii) and (iii). Since $L_2(4) \cong L_2(5) \cong A_5$ and $L_2(9) \cong A_6$, we see that $s(G) = u(G) = 2$ if $q \in \{4, 5, 9\}$. If $q = 8$, then $s(G) = u(G) = 6$. Finally, for $q = 7$ one can check that $s(G) = 5$ and $u(G) = 3$.

(d) Part (iv) extends [27, Proposition 6.4], which states that $\gamma_u(L_2(q)) \leqslant 4$, with equality if and only if $q = 9$. We also note that $G = L_2(11)$ is the smallest simple group with $\gamma_u(G) = 2$.

(e) It is worth highlighting the expression for $P_2(G)$ in part (v), which shows that $P_2(G) \to \frac{1}{2}$ as q tends to infinity (cf. Corollary 8).

In order to state a result for all classical groups, it will be useful to write

$$\mathcal{A} = \{U_{r+1}(q) : r \geqslant 7 \text{ odd}\} \cup \{\mathrm{PSp}_{2r}(q) : r \geqslant 3 \text{ odd}, q \text{ odd}\}$$
$$\cup \{\mathrm{P\Omega}_{2r}^+(q) : r \geqslant 5 \text{ odd}\},$$
$$\mathcal{B} = \{\mathrm{Sp}_{2r}(q) : r \geqslant 2, q \text{ even}, (r, q) \neq (2, 2)\} \cup \{\Omega_{2r+1}(q) : r \geqslant 3, q \text{ odd}\},$$
$$\mathcal{C} = \{\mathrm{PSp}_{2r}(q) : r \geqslant 5 \text{ odd}, q \text{ odd}\} \cup \{\mathrm{P\Omega}_{2r}^\pm(q) : r \geqslant 4 \text{ even}\}.$$

In the statement of the following result, r denotes the (untwisted) Lie rank of G, which is the rank of the ambient simple algebraic group.

THEOREM 6: *Let G be a finite simple classical group over $\mathbb{F}_q$ of rank r.*

(i) *We have $\gamma_u(G) \leqslant 7r + 56$.*

(ii) *We have $\gamma_u(G) = 2$ only if one of the following holds:*

    (a) *$G = L_2(q)$ and $q \geqslant 11$ is odd.*

    (b) *$G = L_n^\epsilon(q)$, where n is odd and*

$$(n, q, \epsilon) \notin \{(3, 2, +), (3, 4, +), (3, 3, -), (3, 5, -)\}.$$

    (c) *$G \in \mathcal{C}$.*

Moreover, $\gamma_u(G) = 2$ for the groups in (a) and (b).

(iii) If $\gamma_u(G) = 2$ and $G \notin \mathcal{C} \cup \{L_2(q) : q \geqslant 11 \text{ odd}\}$, then either $P_2(G) > \frac{1}{2}$, or $G = U_5(2)$ and $P_2(G) = \frac{605}{1728}$. Moreover, $P_2(G) \to 1$ as $|G| \to \infty$.

Remark 6: Let us make some remarks on the statement of Theorem 6:

(a) The bound on $\gamma_u(G)$ in part (i) is from [27, Theorem 6.3], where we also showed that $\gamma_u(G) \leqslant 15$ if $G \in \mathcal{A}$ and $r \leqslant \gamma_u(G) \leqslant 7r$ if $G \in \mathcal{B}$.

(b) In part (ii), we have been unable to determine if $\gamma_u(G) = 2$ for the groups G in the collection $\mathcal{C}$. We refer the reader to Remarks 8.15 and 8.16 for further comments on the difficulties that arise in these special cases.

We now present some general results concerning all finite simple groups. Let us write $\mathcal{D}$ for the classical groups arising in parts (ii)(a) and (ii)(b) of Theorem 6, and recall the collection $\mathcal{E}$ from Theorem 4. In addition, write

$$\mathcal{S} = \{M_{23}, J_1, J_4, Ru, Ly, O'N, Fi_{23}, Fi'_{24}, Th, \mathbb{B}, \mathbb{M}\},$$
$$\mathcal{T} = \{J_3, He, Co_1, HN\}.$$

The following result is an immediate corollary of Theorems 3(iii), 4(i) and 6(ii), together with [27, Theorem 4.2] on sporadic groups. Note that $\gamma_u(G) \in \{2, 3\}$ for each of the groups in $\mathcal{T}$, but we have been unable to determine the exact value in these cases (see Remark 9.2).

COROLLARY 7: *Let G be a finite simple group. Then $\gamma_u(G) = 2$ only if*

(i) $G \in \{A_n : n \geqslant 13 \text{ prime}\} \cup \mathcal{D} \cup \mathcal{E} \cup \mathcal{S}$; *or*
(ii) $G \in \mathcal{C} \cup \mathcal{T}$.

Moreover, $\gamma_u(G) = 2$ for the groups in (i).

The next result follows from Theorems 3(iv), 4(ii) and 6(iii).

COROLLARY 8: *Let (G_n) be a sequence of finite simple groups such that $\gamma_u(G_n) = 2$, $G_n \notin \mathcal{C} \cup \{L_2(q) : q \geqslant 11 \text{ odd}\}$ and $|G_n| \to \infty$. Then $P_2(G_n) \to 1$ as $n \to \infty$.*

We will also establish the following non-asymptotic result on the probability $P_2(G)$ (this will be proved in Section 9).

THEOREM 9: *Let G be a finite simple group such that $\gamma_u(G) = 2$ and $G \notin \mathcal{C} \cup \mathcal{T}$. Then $P_2(G) \leqslant \frac{1}{2}$ if and only if one of the following holds:*

(i) $G = \mathrm{L}_2(q)$, $q \geqslant 11$, $q \equiv 3 \pmod 4$ and

$$\frac{24}{55} \leqslant P_2(G) = \frac{1}{2}\left(1 - \frac{q+3}{q(q-1)}\right).$$

(ii) $G \in \{A_{13}, \mathrm{U}_5(2), \mathrm{Fi}_{23}\}$ and

$$P_2(G) = \begin{cases} \frac{4979}{46200} & \text{if } G = A_{13}, \\ \frac{605}{1728} & \text{if } G = \mathrm{U}_5(2), \\ \frac{7700}{137241} & \text{if } G = \mathrm{Fi}_{23}. \end{cases}$$

Remark 7: In terms of the asymptotics of $P_2(G)$, it is natural to ask whether or not this probability is bounded away from zero. That is, is there an absolute constant $\epsilon > 0$ such that $P_2(G) \geqslant \epsilon$ for every simple group G with $\gamma_u(G) = 2$? By Theorem 9, this is true for the relevant groups $G \notin \mathcal{C}$. Therefore, in order to answer this question, it remains to consider the specific symplectic and orthogonal groups comprising the collection $\mathcal{C}$.

There is a natural generalisation of the uniform domination number for groups with uniform spread greater than one. Indeed, if G is a finite group with $u(G) \geqslant \ell$ for some positive integer ℓ, then let $\gamma_u^{(\ell)}(G)$ be the smallest size of a set S of conjugate elements such that for any nontrivial elements $x_1, \ldots, x_\ell \in G$, there exists $y \in S$ such that $G = \langle x_i, y \rangle$ for all i. Evidently, $\gamma_u^{(1)}(G) = \gamma_u(G)$. Since $u(G) \geqslant 2$ for all finite non-abelian simple groups G, it is natural to consider $\gamma_u^{(2)}(G)$ for these groups. With this in mind, we can state the following result (see Section 9).

THEOREM 10: *Let G be a finite simple group such that $\gamma_u(G) = 2$ and $G \notin \mathcal{C} \cup \mathcal{T}$. Then $\gamma_u^{(2)}(G) = 3$. Moreover, the following hold:*

(i) *If $G = A_n$ with $n > 13$ prime, then $\gamma_u^{(\ell)}(G) = \ell + 1$ for all $1 \leqslant \ell \leqslant n$.*

(ii) *If G is an exceptional group of Lie type over $\mathbb{F}_q$, then $\gamma_u^{(\ell)}(G) = \ell + 1$ for all $1 \leqslant \ell \leqslant q$.*

Remark 8: Let us comment on Theorem 10.

    (a) Lemma 2.7 states that if G is a finite non-cyclic group, then

$$\gamma_u^{(\ell)}(G) \geqslant \ell + 1,$$

    with equality if $P_2(G) > 1 - \ell^{-1}$ (this is clear for $\ell = 1$). Therefore, the probabilistic results in Corollary 8 and Theorem 9 are crucial to the proof of Theorem 10.

    (b) In certain cases, we can establish even stronger results on $\gamma_u^{(\ell)}(G)$. For example, if $G = E_8(q)$, then $\gamma_u^{(\ell)}(G) = \ell + 1$ for all $\ell \leqslant q^{30}$ (see Remark 4(b)).

Remark 9: Suppose G is a finite group with an element $s \in G$ that is contained in a unique maximal subgroup H of G. In this situation, the class s^G witnesses $\gamma_u(G) = 2$ if and only if $b(G, G/H) = 2$, and one needs further information on the bases of size two in order to determine if the same class witnesses $\gamma_u^{(\ell)}(G) = \ell + 1$ for some $\ell \geqslant 2$. It turns out that this is encoded in the so-called **Saxl graph** $\Sigma(G, G/H)$, which has vertex set G/H and two vertices are adjacent if and only if they form a base for G (see [24]). According to Lemma 2.8, $\gamma_u^{(\ell)}(G) = \ell + 1$ is witnessed by s^G if and only if $\Sigma(G, G/H)$ has an $(\ell+1)$-clique (that is, a complete subgraph with $\ell + 1$ vertices). In particular, the probabilistic condition in Remark 8(a) is just a special case of Turán's Theorem applied to the graph $\Sigma(G, G/H)$. In [24], it is conjectured that if $G \leqslant \mathrm{Sym}(\Omega)$ is a finite primitive group with $b(G, \Omega) = 2$, then any pair of vertices of $\Sigma(G, \Omega)$ have a common neighbour and thus $\Sigma(G, \Omega)$ contains a triangle. In the above setting, this would imply that $\gamma_u^{(2)}(G) = 3$.

    Finally, let us return to the total domination number $\gamma_t(G)$ and recall that $\gamma_t(G) \leqslant \gamma_u(G)$. It is natural to consider the relationship between these two numbers. For example, is there an absolute constant C such that

$$\gamma_u(G) \leqslant C\gamma_t(G)$$

for all non-abelian finite simple groups G? By the results stated above, this is true for all even-degree alternating groups and all exceptional groups of Lie type. It also holds for the classical groups in the collections denoted $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{D}$ above (indeed, one can modify the proof of [27, Theorem 6.3(iii)] to get $\gamma_t(G) \geqslant r$ for all $G \in \mathcal{B}$). It would be interesting to investigate if this relationship extends to the remaining classical groups, and also the alternating groups of odd degree.

NOTATION. Our group-theoretic notation is fairly standard. In particular, we adopt the notation from [53] for simple groups, so we write $L_n(q) = PSL_n(q)$ and $U_n(q) = PSU_n(q)$ for linear and unitary groups, and $P\Omega_n^\epsilon(q)$ is a simple orthogonal group, etc. In addition, if G is a finite group, then we write $G^\#$ for the set of nontrivial elements in G and $i_r(X)$ for the number of elements of order r in a subset X of G. For matrices, it will be convenient to write $[A_1^{n_1}, \ldots, A_k^{n_k}]$ for a block-diagonal matrix with a block A_i occurring with multiplicity n_i. In addition, J_i will denote a standard unipotent Jordan block of size i. Finally, for positive integers a and b, we write (a, b) for their greatest common divisor and we set $[a] = \{1, \ldots, a\}$.

2. Methods

In this section, we record some preliminary results which will be needed in the proofs of our main theorems. Throughout, let G be a finite 2-generated non-cyclic group and let $G^\#$ be the set of nontrivial elements of G.

2.1. SPREAD. Define the spread $s(G)$ and uniform spread $u(G)$ as in the introduction. We begin by outlining a probabilistic approach which was first used by Guralnick and Kantor in [45] to prove that $u(G) \geqslant 1$ for every non-abelian finite simple group G and has since been instrumental in establishing several related results on the uniform spread of simple and almost simple groups in [13, 25, 46, 48].

For $x, s \in G$, let

$$(4) \qquad P(x, s) = 1 - \frac{|\{z \in s^G : G = \langle x, z \rangle\}|}{|s^G|}$$

be the probability that x and a randomly chosen conjugate of s do not generate G. The following result is [25, Lemma 2.1].

LEMMA 2.1: *Let k be a positive integer and assume there is an element $s \in G$ such that*

$$\sum_{i=1}^{k} P(x_i, s) < 1$$

for all k-tuples $(x_1, \ldots, x_k)$ of prime order elements in G. Then $u(G) \geqslant k$ (with respect to the conjugacy class s^G).

We can use fixed point ratios to estimate the sum in Lemma 2.1. Recall that if G acts transitively on a finite set Ω, then

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

is the **fixed point ratio** of $x \in G$, where $C_\Omega(x)$ is the set of fixed points of x and H is a point stabiliser. By [25, Lemma 2.2], we have

(5)
$$P(x, s) \leqslant \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H),$$

where $\mathcal{M}(G, s)$ is the set of maximal subgroups of G which contain s. This yields the following corollary.

COROLLARY 2.2: *Let k be a positive integer and assume there is an element $s \in G$ such that*

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

for all $x \in G$ of prime order. Then $u(G) \geqslant k$.

Therefore, upper bounds on fixed point ratios can be used to bound the probability $P(x, s)$. In order to effectively apply this approach, one needs to identify an element $s \in G$ for which we can control the maximal overgroups in $\mathcal{M}(G, s)$ (ideally, s should be contained in very few maximal subgroups).

When it is feasible to do so, this probabilistic approach will be complemented by computational methods implemented in MAGMA [9]. These methods are outlined in [48, Section 2.3] and we refer the reader to Breuer's manuscript [12] for a more detailed discussion.

2.2. UNIFORM DOMINATION NUMBER. Let G be a finite group with $u(G) \geqslant 1$. Recall that a subset S of $G^{\#}$ is a total dominating set (TDS) for G if for all $x \in G^{\#}$, there exists $y \in S$ such that $G = \langle x, y \rangle$, and the uniform domination number of $\gamma_u(G)$ is the minimal size of a TDS for G consisting of conjugate

elements. This notion was first introduced in [27], where close to best possible bounds on $\gamma_u(G)$ for simple groups G were determined. Let us briefly recall the main methods developed in [27] to bound the uniform domination number.

Recall that if G acts faithfully on a finite set Ω, then a subset of Ω is a base for G if its pointwise stabiliser in G is trivial; the base size of G, written $b(G, \Omega)$, is the minimal size of a base. The following result reveals an important connection between bases and total dominating sets consisting of conjugate elements.

LEMMA 2.3: *Let* $s \in G^\#$, *let* $H \in \mathcal{M}(G, s)$ *and assume that* H *is core-free. Then*

$$\min\{|S| : S \subseteq s^G \text{ is a TDS for } G\} \geqslant b(G, G/H),$$

with equality if $\mathcal{M}(G, s) = \{H\}$. *In particular, if for each* $s \in G^\#$ *there exists* $H \in \mathcal{M}(G, s)$ *with* $b(G, G/H) \geqslant c$, *then* $\gamma_u(G) \geqslant c$.

Proof. This follows from [27, Corollaries 2.2 and 2.3]. ∎

Probabilistic methods also play a key role in [27]. As in the introduction, for an element $s \in G$ and integer $c \geqslant 1$, we define $P(G, s, c)$ to be the probability that c randomly chosen conjugates of s form a TDS for G (see (1)). Note that $\gamma_u(G) \leqslant c$ if and only if $P(G, s, c) > 0$ for some s. The next lemma provides a means of computing $P(G, s, 2)$ in an important special case.

LEMMA 2.4: *Suppose* $s \in G^\#$ *and* $\mathcal{M}(G, s) = \{H\}$ *with* H *core-free. Then*

$$P(G, s, 2) = \frac{r|H|^2}{|G|},$$

where r *is the number of regular orbits of* H *on* G/H.

Proof. First observe that if $\{x, y\}$ is a TDS for G, then so is $\{x^g, y^g\}$ for all $g \in G$, hence

$$P(G, s, 2) = \frac{|\{s^g \in s^G : \{s, s^g\} \text{ is a TDS for } G\}|}{|s^G|}.$$

Now $\{s, s^g\}$ is a TDS for G if and only if $H \cap H^g = 1$, so

$$P(G, s, 2) = \frac{|\{g \in G : H \cap H^g = 1\}|}{|C_G(s)||s^G|} = \frac{r|H|^2}{|G|}$$

as required. ∎

The next result, which is [27, Lemma 2.5], shows that fixed point ratios can be used to bound the complementary probability $Q(G, s, c) = 1 - P(G, s, c)$.

LEMMA 2.5: Let $s \in G^{\#}$ and $c \in \mathbb{N}$. Then

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

where the x_i represent the conjugacy classes in G of elements of prime order.

We can use the following result to estimate the bound that arises in Lemma 2.5 (see [27, Lemma 2.7]).

LEMMA 2.6: 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

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

for all positive integers c.

Recall the definition of $\gamma_u^{(\ell)}(G)$ from the introduction, where ℓ is a positive integer. In particular, notice that $\gamma_u^{(1)}(G) = \gamma_u(G)$.

LEMMA 2.7: Let ℓ be a positive integer. Then $\gamma_u^{(\ell)}(G) \geqslant \ell + 1$, with equality if $Q(G, s, 2) < 1/\ell$ for some $s \in G$.

Proof. Fix $s \in G$ and consider a subset $S = \{z_1, z_2, \ldots, z_\ell\}$ of s^G of size ℓ. Since G is not cyclic, there is no j such that $G = \langle z_i, z_j \rangle$ for all $i \in [\ell]$, whence $\gamma_u^{(\ell)}(G) \geqslant \ell + 1$.

Now assume that $Q(G, s, 2) < 1/\ell$. We will use induction on ℓ to prove that there exists a subset S of s^G of size $\ell + 1$ such that $\{z, z'\}$ is a TDS for G for all distinct $z, z' \in S$. The base case $\ell = 1$ is clear, so let us assume $\ell \geqslant 2$. Since $Q(G, s, 2) < 1/\ell < 1/(\ell - 1)$, by induction, there exist $z_1, \ldots, z_\ell \in s^G$ such that $\{z_i, z_j\}$ is a TDS for all distinct $i, j \in [\ell]$. For $i \in [\ell]$, let $N_i \subseteq s^G$ be the set of conjugates z of s such that $\{z_i, z\}$ is not a TDS for G. The bound $Q(G, s, 2) < 1/\ell$ implies that $|N_i| < |s^G|/\ell$, so there exists $z_{\ell+1} \in s^G$ such that

$$z_{\ell+1} \notin \bigcup_{i=1}^{\ell} N_i$$

and hence $\{z_i, z_j\}$ is a TDS for all distinct $i, j \in [\ell + 1]$.

Now fix $S \subseteq s^G$ such that $|S| = \ell + 1$ and $\{z, z'\}$ is a TDS for G for all distinct $z, z' \in S$. Let $x_1, \ldots, x_\ell \in G^\#$ be arbitrary elements. We claim that there exists $z \in S$ such that $G = \langle x_i, z \rangle$ for all $i \in [\ell]$. Seeking a contradiction, suppose that for all $z \in S$, there exists $i \in [\ell]$ such that $G \neq \langle x_i, z \rangle$. Since $|S| > \ell$, there exists $i \in [\ell]$ and distinct $z, z' \in S$ such that $G \neq \langle x_i, z \rangle$ and $G \neq \langle x_i, z' \rangle$, but this contradicts the fact that $\{z, z'\}$ is a TDS. This completes the proof of the lemma. ∎

Recall that if G is a group acting faithfully on a set Ω, then the Saxl graph $\Sigma(G, \Omega)$ has vertex set Ω and $\alpha, \beta \in \Omega$ are adjacent if and only if $\{\alpha, \beta\}$ is a base for the action of G on Ω (see [24]).

LEMMA 2.8: *Fix $s \in G$ and assume that $\mathcal{M}(G, s) = \{H\}$ for a core-free subgroup H with $b(G, G/H) = 2$. Then $\gamma_u^{(\ell)}(G) = \ell + 1$ is witnessed by s^G if and only if $\Sigma(G, G/H)$ has an $(\ell + 1)$-clique.*

Proof. First assume that $\Sigma(G, G/H)$ has an $(\ell+1)$-clique. Then there exist $\ell + 1$ distinct conjugates $H^{g_1}, \ldots, H^{g_{\ell+1}}$ such that $H^{g_i} \cap H^{g_j} = 1$ for all $i \neq j$, which is equivalent to $\{s^{g_i}, s^{g_j}\}$ being a TDS. Therefore, by the proof of Lemma 2.7, $\{s^{g_1}, \ldots, s^{g_{\ell+1}}\}$ witnesses $\gamma_u^{(\ell)}(G) = \ell + 1$.

Now suppose $\gamma_u^{(\ell)}(G) = \ell + 1$ is witnessed by a set $S = \{s^{g_1}, \ldots, s^{g_{\ell+1}}\}$. To prove that $\Sigma(G, G/H)$ has an $(\ell + 1)$-clique, it suffices to prove that

$$H^{g_i} \cap H^{g_j} = 1$$

for all $i \neq j$. Suppose otherwise, say $1 \neq x \in H^{g_1} \cap H^{g_2}$. Then there is no element $z \in S$ such that $G = \langle y, z \rangle$ for all $y \in \{x, s^{g_3}, \ldots, s^{g_{\ell+1}}\}$, which contradicts S witnessing $\gamma_u^{(\ell)}(G) = \ell + 1$. This completes the proof. ∎

In addition to the techniques described above, we will also use computational methods in GAP [41] and MAGMA [9] to study $\gamma_u(G)$. We refer the reader to [27, Section 2.3] and [28] for a detailed discussion of these methods.

3. Soluble groups

In this section we will prove Theorem 1. With this goal in mind, we begin by recording an elementary lemma on the structure of the finite soluble groups we are interested in. Throughout this section, it will be convenient to let $\mathcal{S}$ be the set of finite non-abelian soluble groups with the property that every proper quotient is cyclic.

LEMMA 3.1: *Each $G \in \mathcal{S}$ is a primitive Frobenius group of the form $G = N{:}H$, where N, the socle of G, is an elementary abelian p-group for some prime p, and $H = \langle h \rangle$ acts faithfully and irreducibly on N. In particular, $H = C_G(h)$ has $|N|$ distinct N-conjugates and these subgroups intersect pairwise trivially.*

Proof. This is straightforward; see the proof of [14, Proposition 1.1], for example. ∎

Since the spread of soluble groups has been studied by Brenner and Wiegold in [10, Theorem 2.01], we may focus on the uniform spread and the uniform domination number.

PROPOSITION 3.2: *Let $G = N{:}H \in \mathcal{S}$ as above. Let $1 \leqslant k \leqslant |N| - 1$ and let S be a subset of h^G of size $k + 1$. Then for any k nontrivial elements $x_1, \ldots, x_k$ in G, there exists $s \in S$ such that $G = \langle x_i, s \rangle$ for all i.*

Proof. Write $S = \{h^n : n \in M\}$ where M is a subset of N of size $k + 1$. Let $x_1, \ldots, x_k$ be arbitrary nontrivial elements of G. Since the distinct conjugates of H have pairwise trivial intersection, each x_i is contained in at most one conjugate of H. Therefore, there exists $n \in M$ such that $x_i \notin H^n$ for all i. Fix $1 \leqslant i \leqslant k$ and write $x_i = n_i h_i$ with $n_i \in N$ and $h_i \in H^n$. Note that $n_i \neq 1$ since $x_i \notin H^n$. We claim that $G = \langle x_i, h^n \rangle$. To see this, first observe that $H^n \leqslant \langle x_i, h^n \rangle$ since $H^n = \langle h^n \rangle$. In addition, $n_i \in \langle x_i, h^n \rangle$ and $N = \langle n_i^{H^n} \rangle$ since H^n acts irreducibly on N. Therefore $G = \langle x_i, h^n \rangle$ and the result follows. ∎

COROLLARY 3.3: *If $G = N{:}H \in \mathcal{S}$ as above, then $u(G) = |N| - 1$.*

Proof. Since $u(G) \geqslant |N| - 1$ by Proposition 3.2, it suffices to show that

$$u(G) \leqslant |N| - 1.$$

Seeking a contradiction, suppose that G has uniform spread $|N|$ with respect to an element $s \in G$. Consider the set $\{h^n : n \in N\}$ of $|N|$ nontrivial elements. Since G has uniform spread $|N|$ with respect to s, it follows that there exists $g \in G$ such that $G = \langle s^g, h^n \rangle$ for all $n \in N$. Therefore,

$$s^g \in G \setminus \bigcup_{n \in N} H^n = N$$

and thus $s \in N$. However, $\langle n, s^x \rangle \leqslant N < G$ for all $n \in N$ and $x \in G$, which is a contradiction. Therefore, $u(G) \leqslant |N| - 1$ and the proof is complete. ∎

COROLLARY 3.4: *If $G = N{:}H \in \mathcal{S}$ as above, then $\gamma_u(G) = 2$ and*

$$P(G, h, 2) = 1 - |N|^{-1}.$$

Proof. Both claims follow from the special case of Proposition 3.2 with $k = 1$, noting that any two distinct G-conjugates of h form a uniform dominating set. ∎

Finally, we determine the conjugacy classes that witness the properties established above. This completes the proof of Theorem 1.

PROPOSITION 3.5: *If $G = N{:}H \in \mathcal{S}$ as above, then the following are equivalent:*

 (i) *s^G witnesses $u(G) \geqslant 1$.*
 (ii) *s^G witnesses $\gamma_u(G) = 2$.*
 (iii) *s generates a complement of N.*

In particular, $P_2(G) = 1 - |N|^{-1}$.

Proof. Proposition 3.2 proves that (iii) implies (ii), and evidently (ii) implies (i). We will prove that (i) implies (iii). Suppose that $u(G) \geqslant 1$ with respect to s^G. Then for $1 \neq n \in N$, there exists $g \in G$ such that $G = \langle n, s^g \rangle$. In particular, $G/N = \langle Nn, Ns^g \rangle = \langle Ns^g \rangle$. Since Ns^g generates G/N, the element s^g generates a complement of N. ∎

Remark 3.6: It follows from the proofs of Propositions 3.2 and 3.5 that two elements of $G = N{:}H \in \mathcal{S}$ form a total dominating set if and only if they generate distinct complements of N.

4. Symmetric groups

In this section, we will focus on symmetric groups and our main aim is to prove Theorem 2; alternating groups will be handled in Section 5.

The spread of symmetric groups has been the subject of many papers, spanning several decades. In 1939, Piccard [63] proved that if $n \geqslant 3$, then S_n has positive spread if and only if $n \neq 4$. In addition, she showed that the alternating group A_n has positive spread for $n \geqslant 4$. Building on these results, the spread and uniform spread of symmetric and alternating groups were studied by Binder in a series of papers [5, 6, 7, 8] in the late 1960s. In particular, he

shows that

$$
(6) \qquad s(S_n) = \begin{cases} 0 & \text{if } n = 4 \\ 2 & \text{if } n \neq 4 \text{ is even} \\ 3 & \text{if } n \text{ is odd} \end{cases}
$$

for $n \geqslant 3$ (see [5, 6]). Here Binder uses the term k-fold coherent to describe a group G with $s(G) \geqslant k$, and he refers to a total dominating set as a complete set of complements (the term spread was first introduced by Brenner and Wiegold in [10]). Binder studies the uniform spread of symmetric groups in [7], proving that $u(S_n) \geqslant 1$ for $n \notin \{4, 6\}$. Note that the two excluded cases are genuine exceptions. Indeed, $s(S_4) = u(S_4) = 0$ since S_4 has a non-cyclic proper quotient, and one can check that $u(S_6) = 0$ (see [25, Theorem 2], for example).

As a consequence of Binder's work, it follows that $u(S_n) \in \{1, 2\}$ if $n \geqslant 8$ is even, and $u(S_n) \in \{1, 2, 3\}$ if n is odd. Our first aim is to determine the exact uniform spread of S_n for all n; the main results are Theorems 4.3 and 4.11. Along the way, we will also prove (6). With this goal in mind, the following preliminary result will be useful.

LEMMA 4.1: *Let* $G = S_n$ *with* $n \geqslant 9$, *let* $s = (1, 2, \ldots, n) \in G$ *and let* $i, j, k, l \in [n]$ *be distinct numbers.*

 (i) $G = \langle (i, j), s \rangle$ *if and only if* $j - i$ *and* n *are coprime.*
 (ii) $\langle (i, j, k), s \rangle \geqslant A_n$ *if and only if* $j - i$ *and* $k - j$ *are coprime.*
 (iii) $\langle (i, j)(k, l), s \rangle \geqslant A_n$ *if* $j - i$ *and* n *are coprime and* $i, j, k, l \leqslant n/2$.

Proof. Let x be (i, j), (i, j, k) and $(i, j)(k, l)$ in parts (i), (ii) and (iii), respectively. In all three cases, it suffices to show that $\langle x, s \rangle$ acts primitively on $[n]$ since any primitive permutation group of degree $n \geqslant 9$ and minimal degree at most 4 must contain A_n (see [35, Example 3.3.1]). Cases (i) and (ii) are straightforward, so let us consider (iii). Let Π be a nontrivial partition of $[n]$ stabilised by s. Then each part of Π is a congruence class modulo a, where $1 < a < n$ and a divides n. If x also stabilises Π, then either each cycle of x is contained in a part of Π, or $a = n/2$ and either $\{i, k\}$ and $\{j, l\}$ are parts of Π, or $\{i, l\}$ and $\{j, k\}$ are parts of Π. The first of these possibilities is excluded by the condition that $j - i$ and n are coprime, and the second is ruled out by the condition $i, j, k, l \leqslant n/2$ since each part of Π contains a number greater than $n/2$. The result follows. ∎

Remark 4.2: By Lemma 4.1(i), if $z \in S_n$ is an n-cycle then $S_n = \langle z, (i, iz) \rangle$ for each $i \in [n]$.

Finally, we will refer to the **shape** of a permutation $x \in S_n$ to mean the list of lengths of the disjoint cycles comprising x. For example, $(1, 2)(3, 4) \in S_7$ has shape $[2^2, 1^3]$.

4.1. UNIFORM SPREAD FOR ODD DEGREES. We will first determine the uniform spread of odd-degree symmetric groups, which is significantly easier than the even-degree case. We will also compute the spread of these groups.

THEOREM 4.3: *Let $G = S_n$ with $n \geqslant 5$ odd. Then $u(G) = 2$ and $s(G) = 3$.*

Proof. The case $n = 5$ can be handled using MAGMA, so let us assume $n \geqslant 7$. We begin by establishing lower bounds. Write $n = 2m + 1$ and let C be the class of elements of shape $[m, m + 1]$. Let x_1, x_2 and x_3 be nontrivial elements of G and assume that

$$\{x_1, x_2, x_3\} \neq \{(1, 2), (2, 3), (1, 3)\}^g$$

for all $g \in G$. Therefore, we may fix two disjoint subsets $\{a_1, a_2, a_3\}$, $\{b_1, b_2, b_3\}$ of $\{1, 2, \ldots, n\}$ such that $a_i x_i = b_i$ for each i. Choose $z \in C$ so that a_1, a_2, a_3 are contained in the m-cycle of z, and b_1, b_2, b_3 are contained in the $(m + 1)$-cycle. Clearly, z is contained in a unique maximal intransitive subgroup H. Since $(m, m + 1) = 1$, z is not contained in a transitive imprimitive subgroup. In addition, since z is odd and z^{m+1} is an m-cycle, a theorem of Marggraf (see [73, Theorem 13.5]) implies that z is not contained in a primitive maximal subgroup. Therefore, $\mathcal{M}(G, z) = \{H\}$ with $H = S_m \times S_{m+1}$. However, by construction $\langle x_i, z \rangle$ is transitive for each i, so

$$G = \langle x_1, z \rangle = \langle x_2, z \rangle = \langle x_3, z \rangle.$$

In particular, by setting $x_3 = x_2$ in the above paragraph, we have shown that $u(G) \geqslant 2$ with respect to the class C. Moreover, to show that $s(G) \geqslant 3$, it suffices to prove that there exists an element $w \in G$ such that

$$G = \langle (1, 2), w \rangle = \langle (2, 3), w \rangle = \langle (1, 3), w \rangle.$$

By Lemma 4.1(i), we can take $w = (1, 2, \ldots, n)$, hence $s(G) \geqslant 3$.

Let us now turn to upper bounds. Let $s \in G$ be such that

$$G = \langle (1,2), s \rangle = \langle (1,3), s \rangle = \langle (2,3), s \rangle.$$

Suppose s stabilises a k-element subset A of $[n]$ with $k < n$, and let B be the complement of A. Since $G = \langle (1,2), s \rangle$, we may assume, without loss of generality, $1 \in A$ and $2 \in B$. Since $G = \langle (1,3), s \rangle$ and $1 \in A$ we must have $3 \in B$. However, this gives $\langle (2,3), s \rangle \leqslant G_{\{B\}} < G$, which is a contradiction. Therefore, s is an n-cycle.

Let us draw two conclusions from this observation. First, suppose that $u(G) \geqslant 3$ is witnessed by a class s^G. We have just demonstrated that s is an n-cycle. However, n is odd, so $s \in A_n$ and thus $\langle (1,2,3), s^g \rangle \leqslant A_n < G$ for all $g \in G$, which is a contradiction. Therefore, $u(G) \leqslant 2$ and thus $u(G) = 2$. Second, suppose that $s(G) \geqslant 4$. Then there exists $t \in G$ such that

$$G = \langle (1,2), t \rangle = \langle (2,3), t \rangle = \langle (1,3), t \rangle = \langle (1,2,3), t \rangle.$$

As before, t must be an n-cycle and once again we reach a contradiction since $\langle (1,2,3), t \rangle \leqslant A_n < G$. Therefore, $s(G) \leqslant 3$ and the proof is complete. ∎

4.2. UNIFORM SPREAD FOR EVEN DEGREES. Now let us turn to the uniform spread of symmetric groups of even degree. Our main aim is to prove the following result.

THEOREM 4.4: *Let $G = S_n$ with $n \geqslant 8$ even. Then $u(G) \geqslant 2$.*

Our proof of Theorem 4.4 relies on the probabilistic method described in Section 2.1 and it is based on the arguments in [45, Section 7] and [13, Section 6]. In addition, we use some of the ideas in Binder's proof of the weaker bound $u(G) \geqslant 1$ in [7].

Our first priority is to establish some fixed point ratio estimates for the action of $G = S_n$ on partitions. For a divisor l of n with $1 < l < n$, let Π_l be the set of partitions of $[n]$ into l parts of equal size. Then G has a natural action on Π_l and for each $x \in G$ we write $\mathrm{Fix}_l(x)$ for the set of partitions in Π_l stabilised by x. Whenever we refer to partitions we mean partitions whose parts have equal size.

We will establish the following bounds, which may be of independent interest (note that in both lemmas, there are no conditions on the parity of n).

LEMMA 4.5: *Let $G = S_n$ with $n \geqslant 8$ and assume that $x \in G$ has shape $[p^k, 1^{n-pk}]$ where p is an odd prime and $k \geqslant 1$. Then*

$$\mathrm{fpr}(x, \Pi_l) < \begin{cases} 1/l^2 & \text{if } (p,k) = (3,1) \text{ or } l > n/6, \\ 1/l^3 & \text{otherwise.} \end{cases}$$

LEMMA 4.6: *Let $G = S_n$ with $n \geqslant 14$ and assume that $x \in G$ has shape $[2^k, 1^{n-2k}]$ where $k \geqslant 1$. Then*

$$\mathrm{fpr}(x, \Pi_l) < \begin{cases} 1/l & \text{if } k = 1, \\ 6/n^2 & \text{if } k = 2 \text{ and } l = n/2, \\ 1/l^2 & \text{if } k = 2 \text{ and } 2 < l < n/2, \\ 33/128 & \text{if } k = 2 \text{ and } l = 2, \\ 1/l^2 & \text{if } k \geqslant 3 \text{ and } l > n/6, \\ 1/l^3 & \text{if } k \geqslant 3 \text{ and } l \leqslant n/6. \end{cases}$$

Remark 4.7: Let us comment on Lemmas 4.5 and 4.6.

  (a) In [13, Proposition 6.7], similar upper bounds on $\mathrm{fpr}(x, \Pi_l)$ are obtained when n is odd and $x \in A_n$ has prime order. Therefore, we can view Lemmas 4.5 and 4.6 as an extension of this result to all n and all $x \in S_n$ of prime order.

  (b) When n is small, it is straightforward to verify the bounds in Lemmas 4.5 and 4.6 with the aid of MAGMA. Indeed, we will prove these results in this way for $n < 30$.

We begin by recording some preliminary results (once again, note that there are no conditions on the parity of n in Lemmas 4.8 and 4.9).

LEMMA 4.8: *Let $G = S_n$ and assume that $x \in G$ has shape $[p^k, 1^{n-pk}]$, where p is an odd prime and $k \geqslant 1$.*

  (i) *If $l \leqslant \frac{n}{3}$, then*
$$\mathrm{fpr}(x, \Pi_l) \leqslant \mathrm{fpr}((1,2,3), \Pi_l).$$

  (ii) *If $p \geqslant 5$ and $l \leqslant \frac{n}{5}$, then*
$$\mathrm{fpr}(x, \Pi_l) \leqslant \mathrm{fpr}((1,2,3,4,5), \Pi_l).$$

  (iii) *If $p = 3$, $k \geqslant 2$ and $l \leqslant \frac{n}{6}$, then*
$$\mathrm{fpr}(x, \Pi_l) \leqslant \mathrm{fpr}((1,2,3)(4,5,6), \Pi_l).$$

Proof. The bound in part (i) is obtained by constructing an injection

$$f \colon \mathrm{Fix}_l(x) \to \mathrm{Fix}_l((1,2,3)),$$

as in the proof of [13, Proposition 6.7(c1)]. Similarly, we refer the reader to [45, Proposition 7.4(ii)] for parts (ii) and (iii), which are established in a similar fashion. ∎

LEMMA 4.9: *Let $G = S_n$ with $n \geqslant 30$ and let $x = (1,2)(3,4)\cdots(2k-1,2k) \in G$ with $k \geqslant 2$.*

(i) *If $3 \leqslant l \leqslant \frac{n}{3}$, then*

$$\mathrm{fpr}(x, \Pi_l) \leqslant \mathrm{fpr}((1,2)(3,4), \Pi_l).$$

(ii) *If $k \geqslant 3$ and $3 \leqslant l \leqslant \frac{n}{6}$, then*

$$\mathrm{fpr}(x, \Pi_l) \leqslant \mathrm{fpr}((1,2)(3,4)(5,6), \Pi_l).$$

In the proof of Lemma 4.9 we will make use of the convenient notation for partitions introduced by Guralnick and Kantor in [45, Section 7].

Notation: When defining a map f between subsets of Π_l, for a partition Π we will specify the image $f(\Pi)$ by giving some of the elements of $\{1,2,\ldots,n\}$, separating parts by / and assuming that the unspecified points, denoted by $*$, are in the same parts of $f(\Pi)$ as they are in Π. For

$$x = (1,2)(3,4)\cdots(2k-1,2k) \in S_n$$

and $i \in [n]$ in the support of x, we will write $i' = i - 1$ if i is even and $i' = i + 1$ if i is odd (so (i, i') is the cycle of x containing i).

Proof of Lemma 4.9. To establish part (i), we proceed as in the proof of [13, Proposition 6.7(c2)] (note that in [13], it is assumed that k is even and n is odd). The claim is clear if $k = 2$, so let us assume $k \geqslant 3$. Define a map

$$f \colon \mathrm{Fix}_l(x) \to \mathrm{Fix}_l((1,2)(3,4))$$

as follows. Let $\Pi \in \mathrm{Fix}_l(x)$. If $\Pi \in \mathrm{Fix}_l((1,2)(3,4))$, then set $f(\Pi) = \Pi$. Otherwise, by considering the possible types of partitions in $\mathrm{Fix}_l(x) \backslash \mathrm{Fix}_l((1,2)(3,4))$, we define $f(\Pi)$ as in Table 1. Note that

$$f(\Pi) \in \mathrm{Fix}_l((1,2)(3,4)) \setminus \mathrm{Fix}_l(x)$$

in each case.

Table 1. The map f in the proof of Lemma 4.9(i)

(I)	$(1, a, b, * \ / \ 2, a', b', * \ / \ 3, * \ / \ 4, * \ / \ldots)$ $\mapsto (1, 2, a, * \ / \ 3, 4, b, * \ / \ a', * \ / \ b', * \ / \ldots)$
(II)	$(1, 2, a, * \ / \ 3, b, * \ / \ 4, b', * \ / \ldots)$ $\mapsto (1, 2, b, * \ / \ 3, 4, * \ / \ a, b', * \ / \ldots)$
(III)	$\begin{cases} (3, 4, a, * \ / \ 1, b, * \ / \ 2, b', * \ / \ldots) & \text{if } \frac{n}{l} \geqslant 4 \\ \quad \mapsto (3, 4, b, * \ / \ 1, 2, * \ / \ a, b', * \ / \ldots) & \\ (3, 4, a \ / \ 1, b, c \ / \ 2, b', c' \ / \ d, * \ / \ldots) & \text{if } \frac{n}{l} = 3 \\ \quad \mapsto (3, 4, c' \ / \ 1, 2, d \ / \ a, b, c \ / \ b', * \ / \ldots) & \end{cases}$
(IV)	$(1, 3, * \ / \ 2, 4, * \ / \ldots)$ $\mapsto (1, 2, * \ / \ 3, 4, * \ / \ldots)$
(V)	$(1, 4, a, * \ / \ 2, 3, a', * \ / \ b, c, d, * \ / \ldots)$ where $b' \notin \{c, d\}$ $\mapsto (1, 2, a, * \ / \ 3, 4, b, * \ / \ a', c, d, * \ / \ldots)$

In order to establish the desired bound in part (i), it suffices to show that f is injective. To do this, let Σ be a partition in the image of f and write $f(\Pi) = \Sigma$ for some $\Pi \in \mathrm{Fix}_l(x)$. We need to show that there is a unique choice for Π. Clearly, if $\Sigma \in \mathrm{Fix}_l(x)$ then $\Pi = \Sigma$, so let us assume $\Sigma \notin \mathrm{Fix}_l(x)$. Note that in every case, $\{1, 2\}$ is a subset of a part A of Σ, and $\{3, 4\}$ is a subset of some other part B.

From the definition of f, we see that there are three separate cases to consider, according to the number $m \in \{2, 3, 4\}$ of parts of Σ that are not mapped to parts of Σ by x. We will refer to the **type** of Π by the label recorded in the first column of Table 1.

First assume $m = 4$, so Π has type (I) or (III) (with $n/l = 3$ in the latter case). If no point in any of these four parts is fixed by x, then Π has type (I). To prove that Π is uniquely determined in this case, it suffices to show that a and b are uniquely determined (indeed, these numbers determine a' and b' and, together with Σ, these four values determine Π). Now a is the unique point in $A \setminus \{1, 2\}$ which is not mapped by x into B, and similarly b is the unique point in $B \setminus \{3, 4\}$ not mapped into A. Therefore, Π is uniquely determined by Σ. Now assume Π has type (III) and $n/l = 3$. Here, d is the unique point in $A \setminus \{1, 2\}$ and c' is the unique point in $B \setminus \{3, 4\}$, so we have determined c

and d. Now a is the unique point fixed by x in the part of Σ containing c, and b is the remaining point in this part. The values of a, b, c and d, together with the partition Σ, uniquely determine Π.

Now assume $m = 3$, so Π is of type (II), (III) (with $n/l \geqslant 4$) or (V). Necessarily, A and B are two of the three parts of Σ that are not mapped to parts of Σ by x. Let C be the third such part. We begin by demonstrating that the type of Π is determined by Σ. First assume that $n/l = 3$. If a point of B is mapped by x into C, then Π has type (II), otherwise, Π has type (V). Now assume that $n/l \geqslant 4$. If a point of A is mapped by x into B, then Π has type (V). Otherwise, if at least two points of A are mapped into C by x, then Π has type (III); else Π has type (II).

We now show that Π is determined by Σ when $m = 3$. First assume that Π has type (II). The unique point of A not mapped into A by x is b, and the unique point in $C \setminus \{b'\}$ not mapped into B is a; this determines Π. Next assume that $n/l \geqslant 4$ and Π has type (III). The unique point in B not mapped into B is b, and the unique point in $C \setminus \{b'\}$ not mapped into A is a; this determines Π. Finally, suppose Π has type (V). Now a is the unique point in A not mapped by x into B, and b is the unique point in B not mapped into A; this determines Π (since c and d are not moved by f).

Finally, suppose $m = 2$. Here Π has type (IV) and thus Π is the partition obtained by interchanging 2 and 3 in Σ. Therefore, Π is uniquely determined in this case.

We have now shown that the map f is injective, which completes the proof of part (i).

Now consider (ii) and note that we may assume $k \geqslant 4$. We define a map

$$f \colon \mathrm{Fix}_l(x) \to \mathrm{Fix}_l((1,2)(3,4)(5,6))$$

as follows. Let $\Pi \in \mathrm{Fix}_l(x)$. If $\Pi \in \mathrm{Fix}_l((1,2)(3,4)(5,6))$, then we define $f(\Pi) = \Pi$. Now assume that $\Pi \notin \mathrm{Fix}_l((1,2)(3,4)(5,6))$. For brevity, we will handle multiple possibilities at once by letting

(7) $$\sigma \in \{1, (1,3,5)(2,4,6), (1,5,3)(2,6,4)\}$$

and writing $\mathbf{i} = i\sigma$ for $1 \leqslant i \leqslant 6$. With this notation, we define f as in Table 2. Note that

$$f(\Pi) \in \mathrm{Fix}_l((1,2)(3,4)(5,6)).$$

Table 2. The map f in the proof of Lemma 4.9(ii). (In cases (IX)–(XI), $\{a, b, d\} \cap \{a', b', d'\} = \emptyset$. In case (XII), if c' or d' is in $\{c, d, e, g, *\}$ then $c' = d$, and if e' or g' is in $\{c, d, e, g, *\}$ then $e' = g$.)

(I)	$(1, a, b, * \,/\, 2, a', b', * \,/\, 3, c, * \,/\, 4, c', * \,/5, * \,/6, * \,/ \dots)$ $\mapsto (1, 2, a, * \,/\, 3, 4, b, * \,/\, 5, 6, * \,/\, c, a', * \,/\, b', * \,/\, c', * \,/ \dots)$
(II)	$(\mathbf{1}, \mathbf{2}, * \,/\, \mathbf{3}, a, b, * \,/\, \mathbf{4}, a', b', * \,/5, * \,/\, \mathbf{6}, * \,/ \dots)$ $\mapsto (\mathbf{1}, \mathbf{2}, * \,/\, \mathbf{3}, \mathbf{4}, a, * \,/5, \mathbf{6}, b, * \,/\, a', * \,/\, b', * \,/ \dots)$
(III)	$(\mathbf{1}, \mathbf{2}, * \,/\, \mathbf{3}, \mathbf{4}, a, * \,/\, \mathbf{5}, b, * \,/\, \mathbf{6}, b', * \,/ \dots)$ $\mapsto (\mathbf{1}, \mathbf{2}, * \,/\, \mathbf{3}, \mathbf{4}, b, * \,/\, \mathbf{5}, \mathbf{6}, * \,/\, a, b', * \,/ \dots)$
(IV)	$(\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, a, * \,/\, \mathbf{5}, b, * \,/\, \mathbf{6}, b', * \,/ \dots)$ $\mapsto (\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, b, * \,/\, \mathbf{5}, \mathbf{6}, * \,/\, a, b', * \,/ \dots)$
(V)	$(\mathbf{1}, \mathbf{2}, * \,/\, \mathbf{3}, \mathbf{5}, * \,/\, \mathbf{4}, \mathbf{6}, * \,/ \dots)$ $\mapsto (\mathbf{1}, \mathbf{2}, * \,/\, \mathbf{3}, \mathbf{4}, * \,/\, \mathbf{5}, \mathbf{6}, * \,/ \dots)$
(VI)	$(\mathbf{1}, \mathbf{2}, a, * \,/\, \mathbf{3}, \mathbf{6}, b, * \,/\, \mathbf{4}, \mathbf{5}, * \,/ \dots)$ $\mapsto (\mathbf{1}, \mathbf{2}, b, * \,/\, \mathbf{3}, \mathbf{4}, a, * \,/\, \mathbf{5}, \mathbf{6}, * \,/ \dots)$
(VII)	$(\mathbf{1}, \mathbf{3}, a, * \,/\, \mathbf{2}, \mathbf{4}, a', * \,/\, \mathbf{5}, b, * \,/\, \mathbf{6}, b', * \,/ \dots)$ $\mapsto (\mathbf{1}, \mathbf{2}, a, * \,/\, \mathbf{3}, \mathbf{4}, b, * \,/\, \mathbf{5}, \mathbf{6}, * \,/\, a', b', * \,/ \dots)$
(VIII)	$(\mathbf{1}, \mathbf{4}, a, * \,/\, \mathbf{2}, \mathbf{3}, a', * \,/\, \mathbf{5}, b, c, * \,/\, \mathbf{6}, b', c', * \,/ \dots)$ $\mapsto \begin{cases} (\mathbf{1}, \mathbf{2}, a, * \,/\, \mathbf{3}, \mathbf{4}, a', * \,/\, \mathbf{5}, \mathbf{6}, c, * \,/\, b, b', c', * \,/ \dots) \text{ if } b \text{ is even} \\ (\mathbf{1}, \mathbf{2}, a, * \,/\, \mathbf{3}, \mathbf{4}, c, * \,/\, \mathbf{5}, \mathbf{6}, a', * \,/\, b, b', c', * \,/ \dots) \text{ if } b \text{ is odd} \end{cases}$
(IX)	$(1, 3, 5, * \,/\, 2, 4, 6, c, * \,/\, a, b, d, * \,/ \dots)$ $\mapsto (1, 2, a, * \,/\, 3, 4, b, d, * \,/\, 5, 6, c, * \,/ \dots)$
(X)	$(1, 3, 6, * \,/\, 2, 4, 5, c, * \,/\, a, b, d, * \,/ \dots)$ $\mapsto (3, 4, a, * \,/\, 5, 6, b, d, * \,/\, 1, 2, c, * \,/ \dots)$
(XI)	$(1, 4, 5, * \,/\, 2, 3, 6, c, * \,/\, a, b, d, * \,/ \dots)$ $\mapsto (5, 6, a, * \,/\, 1, 2, b, d, * \,/\, 3, 4, c, * \,/ \dots)$
(XII)	$(1, 4, 6, a, b, * \,/\, 2, 3, 5, a', b', * \,/\, c, d, e, g, * \,/ \dots)$ $\mapsto (1, 2, a, c, d, * \,/\, 3, 4, b, e, g, * \,/\, 5, 6, a', b', * \,/ \dots)$

We claim that f is injective. To see this, let $\Sigma = f(\Pi)$ be a partition in the image of f. As before, we need to show that Π is uniquely determined by Σ. We may assume that $\Sigma \notin \mathrm{Fix}_l(x)$.

First assume that $\{1,2\}$, $\{3,4\}$ and $\{5,6\}$ are not subsets of distinct parts of Σ, so Π has type (IV). Here b is the unique point in the part of Σ containing $\mathbf{1}$, $\mathbf{2}$, $\mathbf{3}$ and $\mathbf{4}$ which is not mapped by x into that part. In addition, there is a unique part all of whose points other than exactly two are mapped into the part containing $\mathbf{5}$ and $\mathbf{6}$; a is the unique point other than b' in this part not mapped into the part containing $\mathbf{5}$ and $\mathbf{6}$. This determines Π.

For the remainder, we may assume that $\{1,2\}$, $\{3,4\}$ and $\{5,6\}$ are subsets of distinct parts A, B and C of Σ. Where appropriate, we will write $\mathbf{A} = A\sigma$, $\mathbf{B} = B\sigma$ and $\mathbf{C} = C\sigma$ for σ as in (7). There are four cases to consider, according to the number $m \in \{2,3,4,6\}$ of parts of Σ that are not mapped to parts of Σ by x.

First assume $m = 6$, so Π has type (I). The unique point in $A \setminus \{1,2\}$ not mapped into B by x is a, and the unique point in $B \setminus \{3,4\}$ not mapped into A is b. There is a unique part of Σ all of whose points other than exactly two are mapped into C, and c is the unique such point other than a'. This determines Π.

Next assume $m = 4$, so Π has type (II), (VII) or (VIII). If one of A, B or C is fixed by x, then Π has type (II). In this case, the unique point in $\mathbf{B} \setminus \{\mathbf{3},\mathbf{4}\}$ not mapped into $\mathbf{C}$ is a, and the unique point in $\mathbf{C} \setminus \{\mathbf{5},\mathbf{6}\}$ not mapped into $\mathbf{B}$ is b; this determines Π. Now assume that none of the parts A, B and C are fixed by x. Let P be the unique part of Σ other than $\mathbf{A}$, $\mathbf{B}$ or $\mathbf{C}$ which is not mapped to a part by x. There are two cases to consider. First suppose P contains a cycle Z of x, in which case Π has type (VIII) and $Z = \{b, b'\}$. If $\mathbf{A} \setminus \{\mathbf{1},\mathbf{2}\}$ and $\mathbf{B} \setminus \{\mathbf{3},\mathbf{4}\}$ are interchanged by x, then b is even; otherwise, b is odd and c is the unique point in $\mathbf{B}$ not mapped into $\mathbf{A}$. In both cases, this uniquely determines Π (since c is not moved by f when b is even). Now suppose that P does not contain a cycle of x, so Π has type (VII). Here, the unique point in $\mathbf{A} \setminus \{\mathbf{1},\mathbf{2}\}$ not mapped into $\mathbf{B}$ by x is a, and the unique point in $\mathbf{B} \setminus \{\mathbf{3},\mathbf{4}\}$ not mapped into $\mathbf{A}$ by x is b; this determines Π.

Now suppose $m = 3$, so Π has type (III), (VI) or (IX)–(XII). First assume one of A, B or C is fixed by x, so Π has type (III). The unique point in $\mathbf{B}$ not mapped back into $\mathbf{B}$ is b. There is a unique part of Σ all of whose points other than exactly two are mapped into $\mathbf{C}$, and a is the unique such point other than b'. This determines Π.

Now assume none of A, B and C are fixed by x. If all but one point of one of A, B or C is mapped back into that part, then Π has type (VI). Here the unique point in $\mathbf{A}$ not mapped back into $\mathbf{A}$ is b, and the unique point in $\mathbf{B} \setminus \{\mathbf{3, 4}\}$ not mapped into $\mathbf{C}$ is a; this determines Π.

To complete the analysis of the case $m = 3$, we may assume that Π is of type (IX)–(XII). If all but one point of $A \setminus \{1, 2\}$ are mapped into B, then Π has type (IX). The unique point in $A \setminus \{1, 2\}$ not mapped into B is a, the point in C that is mapped into A is c and the points in $B \setminus \{3, 4\}$ not mapped into A are b and d; this determines Π. If all but one point of $B \setminus \{3, 4\}$ are mapped into C, then Π has type (X), and if all but one point of $C \setminus \{5, 6\}$ are mapped into A, then Π has type (XI); in both cases Π is determined as before. Finally, suppose Π has type (XII). The point in A mapped into C is a, and the point in B mapped into C is b. In addition, the two points in $A \setminus \{1, 2, a\}$ not mapped into B are c and d, and the two points in $B \setminus \{3, 4, b\}$ not mapped into A are e and g. This determines Π.

Finally, if $m = 2$ then Π has type (V) and we can determine Π by interchanging $\mathbf{4}$ and $\mathbf{5}$ in Σ.

This proves that f is injective and completes the proof of (ii). ∎

LEMMA 4.10: *Let $G = S_n$ with $n \geqslant 30$ even and suppose $x \in G$ has shape $[p^k, 1^{n-pk}]$, where p is a prime, $k \geqslant 1$ and $(p, k) \notin \{(2, 1), (2, 2), (2, 3), (3, 2)\}$. If $l = \frac{n}{2}$, then $\mathrm{fpr}(x, \Pi_l) < \frac{1}{l^2}$.*

Proof. First assume that p is odd. Let $\Pi \in \mathrm{Fix}_l(x)$. Since $n/l = 2 < p$, no cycle of x is contained in a part of Π. Consequently, if k is odd, then $\mathrm{Fix}_l(x)$ is empty, so we will assume that $k \geqslant 2$ is even. Then x moves $t = pk/2$ parts in $k/2$ orbits of size p and thus $l - t$ parts of Π are fixed by x. With this in mind, let us compute $\mathrm{fpr}(x, \Pi_l)$.

First observe that $|\Pi_l| = (2l)!/(l! \, 2^l)$. To construct an x-stable partition in Π_l, we must first partition the $2l - 2t$ fixed points of x into $l - t$ parts of size 2. The number of ways this can be done is $(2l - 2t)!/((l - t)! \, 2^{l-t})$. We must then partition the remaining $2t = pk$ points into $pk/2$ parts of size 2, which are permuted by x in $k/2$ orbits of size p. This amounts to partitioning the $pk/2$ parts into $k/2$ sets of the form

$$\{\{i_1, j_1\}, \ldots, \{i_p, j_p\}\}$$

where $(i_1, \ldots, i_p)$ and $(j_1, \ldots, j_p)$ are cycles of x. Therefore, an x-stable partition of these pk points corresponds to a partition of the cycles of x into pairs, together with a choice of partition $\{\{i_1, j_{i\sigma}\}, \ldots, \{i_p, j_{p\sigma}\}\}$ for each pair $\{(i_1, \ldots, i_p), (j_1, \ldots, j_p)\}$, where σ is a power of $(1, 2, \ldots, p)$. There are $k!/((k/2)!\, 2^{k/2})$ ways of partitioning the k cycles of x into pairs, and for each pair there are p choices for σ. Therefore, there are $p^{k/2} \cdot k!/((k/2)!\, 2^{k/2})$ different ways to partition the pk points moved by x. In this way, we conclude that

$$\mathrm{fpr}(x, \Pi_l) = p^{k/2} \cdot \frac{k!}{(\frac{k}{2})!\, 2^{k/2}} \cdot \frac{(2l - 2t)!}{(l - t)!\, 2^{l-t}} \cdot \frac{l!\, 2^l}{(2l)!}.$$

By applying Stirling's approximation, we calculate

$$
\begin{aligned}
\mathrm{fpr}(x, \Pi_l) =\; & p^{k/2} \cdot \frac{k!}{(\frac{k}{2})!\, 2^{k/2}} \cdot \frac{(2l - 2t)!}{(l - t)!\, 2^{l-t}} \cdot \frac{l!\, 2^l}{(2l)!} \\
\leqslant\; & \frac{e^3}{2^{3/2}\pi^{3/2}} \cdot \frac{p^{k/2} k^{k+1/2} e^{-k} 2^{2l-2t+1/2}(l-t)^{2l-2t+1/2}}{k^{k/2+1/2} e^{-k/2} 2^{k/2}(l-t)^{l-t+1/2}} \\
& \times \frac{e^{-(2l-2t)} l^{l+1/2} e^{-l} 2^l 2^{k/2+1/2}}{e^{-(l-t)} 2^{l-t} l^{2l+1/2} e^{-2l} 2^{2l+1/2}} \\
=\; & \frac{e^3}{2\pi^{3/2}} \cdot \left(\frac{e}{2t}\right)^{(p-1)k/2} \cdot \frac{t^t(l-t)^{l-t}}{l^l}
\end{aligned}
$$

which in turn is at most

$$\frac{t^t(l-t)^{l-t}}{l^l} \leqslant \frac{5^5(l-5)^{l-5}}{l^l} < \frac{5^5}{15^3} \cdot \frac{1}{l^2} < \frac{1}{l^2}$$

since $l = n/2 \geqslant 15$ and $t = pk/2 \geqslant 5$ (because $p \geqslant 3$ and we are assuming $(p, k) \neq (3, 2)$).

Now assume that $p = 2$ and $k \geqslant 4$. In this case, a partition $\Pi \in \mathrm{Fix}_l(x)$ has i pairs of parts interchanged by x, and $l - 2i$ parts stabilised by x. Moreover, $l - k$ of these $l - 2i$ parts are fixed pointwise. Therefore, by counting as we did above,

$$\mathrm{fpr}(x, \Pi_l) = \left(\sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k!}{(k-2i)!\, i!\, 2^i} \cdot 2^i\right) \cdot \frac{(2l - 2k)!}{(l - k)!\, 2^{l-k}} \cdot \frac{l!\, 2^l}{(2l)!}.$$

Observe that

$$\sum_{i=0}^{\lfloor k/2 \rfloor} \frac{\lfloor k/2 \rfloor!}{(k-2i)!\,i!} = \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{\lfloor k/2 \rfloor}{i} \frac{(\lfloor k/2 \rfloor - i)!}{(k-2i)!}$$

$$\leqslant \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{\lfloor k/2 \rfloor}{i} \frac{1}{(\lfloor k/2 \rfloor - i + 1)^{\lfloor k/2 \rfloor - i}}$$

which is at most

$$\sum_{i=0}^{\lfloor k/2 \rfloor} \binom{\lfloor k/2 \rfloor}{i} \frac{1}{2^i} = \left(\frac{3}{2}\right)^{\lfloor k/2 \rfloor}.$$

Therefore,

$$\mathrm{fpr}(x, \Pi_l) \leqslant \left(\frac{3}{2}\right)^{\lfloor k/2 \rfloor} \cdot \frac{k!}{\lfloor k/2 \rfloor!} \cdot \frac{(2l - 2k)!}{(l-k)!\,2^{l-k}} \cdot \frac{l!\,2^l}{(2l)!}$$

$$\leqslant \left(\frac{3}{2}\right)^{\lfloor k/2 \rfloor} \cdot \lceil k/2 \rceil \cdot 2^{k/2} \cdot \frac{k!}{\lceil k/2 \rceil!\,2^{k/2}} \cdot \frac{(2l - 2k)!}{(l-k)!\,2^{l-k}} \cdot \frac{l!\,2^l}{(2l)!}.$$

By arguing as above, we get

$$\mathrm{fpr}(x, \Pi_l) \leqslant \left(\frac{3}{2}\right)^{\lfloor k/2 \rfloor} \left\lceil \frac{k}{2} \right\rceil \frac{e^3}{2\pi^{3/2}} \left(\frac{e}{2k}\right)^{k/2} \frac{k^k(l-k)^{l-k}}{l^l}$$

$$\leqslant \frac{3e^4}{8\pi^{3/2}} \left(\frac{3e}{4k}\right)^{k/2-1} \frac{k^k(l-k)^{l-k}}{l^l}.$$

If $k \geqslant 5$, then

$$\mathrm{fpr}(x, \Pi_l) \leqslant \frac{k^k(l-k)^{l-k}}{l^l} \leqslant \frac{5^5(l-5)^{l-5}}{l^l} < \frac{5^5}{15^3} \frac{1}{l^2} < \frac{1}{l^2},$$

and for $k = 4$ we get

$$\mathrm{fpr}(x, \Pi_l) \leqslant \frac{3e^4}{8\pi^{3/2}} \frac{3e}{16} \frac{4^4 11^{11}}{15^{13}} \frac{1}{l^2} < \frac{1}{l^2}.$$

This completes the proof. ∎

We can now establish the main fixed point ratio bounds.

Proof of Lemma 4.5. Let $x \in G$ have shape $[p^k, 1^{n-pk}]$, where p is an odd prime and $k \geqslant 1$. For $n < 30$ we can verify the desired bound using MAGMA, so assume that $n \geqslant 30$.

First assume $(p, k) = (3, 1)$. Up to conjugacy, we may assume $x = (1, 2, 3)$. A partition in Π_l is stabilised by x if and only if it has a part containing $\{1, 2, 3\}$. By counting the partitions with this property, we deduce that

$$\mathrm{fpr}(x, \Pi_l) \leqslant \frac{(n-3)!}{(\frac{n}{l} - 3)! \, ((\frac{n}{l})!)^{l-1} \, (l-1)!} \cdot \frac{((\frac{n}{l})!)^l \, l!}{n!}$$

$$= \frac{(\frac{n}{l})(\frac{n}{l} - 1)(\frac{n}{l} - 2) l}{n(n-1)(n-2)} < \frac{1}{l^2}.$$

A similar calculation shows that $\mathrm{fpr}(x, \Pi_l) < \frac{1}{l^4}$ when $(p, k) = (5, 1)$.

Next assume $(p, k) = (3, 2)$, say $x = (1, 2, 3)(4, 5, 6)$. If $l < n/2$, then a partition stabilised by x either has a part containing $\{1, 2, 3, 4, 5, 6\}$, or a part containing $\{1, 2, 3\}$ and another containing $\{4, 5, 6\}$. Therefore,

$\mathrm{fpr}(x, \Pi_l)$

$$\leqslant \left(\frac{(n-6)!}{(\frac{n}{l} - 6)! \, ((\frac{n}{l})!)^{l-1} \, (l-1)!} + \frac{(n-6)!}{((\frac{n}{l} - 3)!)^2 \, ((\frac{n}{l})!)^{l-2} \, (l-2)!} \right) \cdot \frac{((\frac{n}{l})!)^l \, l!}{n!}$$

$$< \frac{1}{l^5} + \frac{l-1}{l^5} \cdot \frac{n(n-1)(n-2)}{(n-3)(n-4)(n-5)} < \frac{1}{l^5} + \frac{1.4}{l^4}$$

and thus $\mathrm{fpr}(x, \Pi_l) < \frac{1}{l^3}$. Now assume $l = n/2$, so $l \geqslant 15$. Here we must also consider the partitions containing three parts for which $\{1, 2, 3\}$ and $\{4, 5, 6\}$ are transversals. The proportion in Π_l of such partitions is

$$3 \cdot \frac{(n-6)!}{2^{l-3} \, (l-3)!} \cdot \frac{2^l \, l!}{n!} \leqslant \frac{3}{(2l-3)(2l-4)(2l-5)} \leqslant \frac{0.6}{l^3}$$

and this gives $\mathrm{fpr}(x, \Pi_l) < \frac{1}{l^5} + \frac{1.4}{l^4} + \frac{0.6}{l^3} < \frac{1}{l^3}$.

Now assume $(p, k) \notin \{(3, 1), (3, 2)\}$. If $l = n/2$, then the desired result follows from Lemma 4.10. Similarly, if $n/6 < l \leqslant n/3$, then we combine Lemma 4.8(i) with the above calculation in the case $(p, k) = (3, 1)$. Finally, let us assume $l \leqslant n/6$. If $p = 3$ and $k \geqslant 3$, then we appeal to Lemma 4.8(iii) and the above calculation for $(p, k) = (3, 2)$. Similarly, if $p \geqslant 5$ then the desired bound follows via Lemma 4.8(ii) and the case $(p, k) = (5, 1)$ handled above. ∎

Proof of Lemma 4.6. Set $x = (1, 2)(3, 4) \cdots (2k - 1, 2k)$. As in the proof of Lemma 4.5, we may assume that $n \geqslant 30$. The desired bound is straightforward to verify when $k = 1$ or 2 (we proceed as in the proof of Lemma 4.5 with $(1, 2, 3)$ and $(1, 2, 3)(4, 5, 6)$, respectively).

Next assume $k = 3$ and $l \leqslant n/6$. The partitions stabilised by x are exactly those which have a part containing $\{1, 2, 3, 4, 5, 6\}$, or a part containing the union of two of $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$ and another part containing the third, or a part containing $\{1, 2\}$, another containing $\{3, 4\}$ and a third which contains $\{5, 6\}$. Therefore,

$$
\begin{aligned}
\mathrm{fpr}(x, \Pi_l) \leqslant & \Big(\frac{(n-6)!}{(\frac{n}{l} - 6)! \, ((\frac{n}{l})!)^{l-1} \, (l-1)!} + \frac{3(n-6)!}{(\frac{n}{l} - 2)! \, (\frac{n}{l} - 4)! \, ((\frac{n}{l})!)^{l-2} \, (l-2)!} \\
& + \frac{(n-6)!}{((\frac{n}{l} - 2)!)^3 \, ((\frac{n}{l})!)^{l-3} \, (l-3)!} \Big) \cdot \frac{((\frac{n}{l})!)^l \, l!}{n!} \\
< & \frac{1}{l^5} + \frac{3(l-1)}{l^5} + \frac{(l-1)(l-2)}{l^5} \leqslant \frac{1}{l^3}.
\end{aligned}
$$

Now assume $k = 3$ and $l = n/2$. Here there are three additional types of partition to consider. In one case, we consider those partitions which contain two parts for which $\{1, 2\}$ and $\{3, 4\}$ are transversals and a third part which is $\{5, 6\}$. We calculate that the proportion of l-part partitions satisfying this condition is equal to

$$
\frac{(n-6)!}{2^{l-3} \, (l-3)!} \cdot \frac{2^l \, l!}{n!} \leqslant \frac{1}{(n-3)(n-4)(n-5)} \leqslant \frac{1.6}{n^3}.
$$

The two other cases arise from interchanging the roles of $\{1, 2\}$, $\{3, 4\}$ and $\{5, 6\}$, so we obtain the same proportion and $\mathrm{fpr}(x, \Pi_l) < \frac{8}{n^3} + \frac{4.8}{n^3} < \frac{1}{l^2}$.

To complete the argument, we may assume that either $k = 3$ and $n/6 < l < n/2$, or $k \geqslant 4$. If $k \geqslant 4$ and $l = n/2$ then Lemma 4.10 gives $\mathrm{fpr}(x, \Pi_l) < \frac{1}{l^2}$ as required, so we may assume $l < n/2$. Here Lemma 4.9 and the above bounds imply that

$$
\mathrm{fpr}(x, \Pi_l) \leqslant \begin{cases} \mathrm{fpr}((1, 2)(3, 4)(5, 6), \Pi_l) < 1/l^3 & \text{if } 3 \leqslant l \leqslant n/6, \\ \mathrm{fpr}((1, 2)(3, 4), \Pi_l) < 1/l^2 & \text{if } n/6 < l < n/2. \end{cases}
$$

Therefore, to complete the proof of the lemma, we may assume that $l = 2$.

First assume $k < n/2$. If $\Pi \in \mathrm{Fix}_l(x)$, then each cycle of x must be contained in one of the two parts of Π, so $\mathrm{Fix}_l(x) \subseteq \mathrm{Fix}_l((1, 2)(3, 4)(5, 6))$ and

$$
\mathrm{fpr}(x, \Pi_l) \leqslant \mathrm{fpr}((1, 2)(3, 4)(5, 6), \Pi_l) < \frac{1}{l^3}.
$$

Finally, suppose $k = n/2$. If $\Pi \in \mathrm{Fix}_l(x)$, then either each cycle of x is contained in a part of Π, or each cycle of x contains a point from each part of Π. Since there are at most $2^{n/2-1}$ partitions of each of these types, it follows that

$$\mathrm{fpr}(x, \Pi_l) \leqslant 2 \cdot 2^{n/2-1} \cdot \frac{2\left(\left(\frac{n}{2}\right)!\right)^2}{n!} \leqslant 2^{n/2} \cdot \frac{2\left(\frac{n}{2}\right)^{n+1} e^{-n} e^2}{n^{n+1/2} e^{-n} (2\pi)^{1/2}} < \frac{1}{8} = \frac{1}{l^3},$$

noting that $n \geqslant 30$. This completes the proof. ∎

We are now in a position to prove Theorem 4.4.

Proof of Theorem 4.4. If $n < 30$, then the result can be verified computationally with MAGMA (see the end of Section 2.1). Now assume $n \geqslant 30$.

Let $G = S_n$ and let s be an n-cycle. Then $\mathcal{M}(G, s) = \mathcal{I} \cup \mathcal{P}$, where $\mathcal{I}$ consists of exactly one imprimitive subgroup $S_{n/l} \wr S_l$ for each divisor $1 < l < n$ of n, and $\mathcal{P}$ contains primitive subgroups of the form $\mathrm{P\Gamma L}_d(q)$ for pairs (q, d) satisfying $n = (q^d - 1)/(q - 1)$ (see [52, Theorem 3]). Moreover, by the proof of [13, Proposition 6.7] we see that $\mathcal{P}$ contains at most $(n - 1)/d$ subgroups of the form $\mathrm{P\Gamma L}_d(q)$ for each pair (q, d).

Suppose $x \in G$ has prime order and let $H \in \mathcal{M}(G, s)$. First assume $H \in \mathcal{P}$, say $H = \mathrm{P\Gamma L}_d(q)$ with $n = (q^d - 1)/(q - 1)$. Then $|H| \leqslant n^{\log_2 n + 1}$ and

$$|x^G| \geqslant \frac{2^{3n/4}\left(\frac{n}{e}\right)^{n/4}}{8\sqrt{\pi n}},$$

by [13, Lemma 6.6]. Since $|\mathcal{P}| \leqslant \frac{1}{2}(n-1)\log_2 n$ (see [27, Lemma 3.9]), it follows that

$$\sum_{H \in \mathcal{P}} \mathrm{fpr}(x, G/H) \leqslant \sum_{H \in \mathcal{P}} \frac{|H|}{|x^G|} \leqslant \frac{1}{2}(n - 1)\log_2 n \cdot \frac{8n^{\log_2 n + 1}\sqrt{\pi n}}{2^{3n/4}\left(\frac{n}{e}\right)^{n/4}}$$

$$\leqslant \frac{n^{\log_2 n + 3} 4\sqrt{\pi}}{n^{n/4}\left(\frac{8}{e}\right)^{n/4}} < 0.01.$$

Now assume $H \in \mathcal{I}$, say $H = S_{n/l} \wr S_l$. Note that the action of G on G/H is equivalent to the action of G on Π_l. Therefore, if

$$x \notin (1, 2)^G \cup (1, 2)(3, 4)^G \cup (1, 2, 3)^G,$$

then Lemmas 4.5 and 4.6 imply that

$$\sum_{H \in \mathcal{I}} \mathrm{fpr}(x, G/H) < \sum_{\substack{l \mid n \\ 1 < l \leqslant \frac{n}{6}}} \frac{1}{l^3} + \frac{5^2 + 4^2 + 3^2 + 2^2}{n^2}$$

$$< \sum_{l=2}^{\infty} \frac{1}{l^3} + \frac{54}{n^2} < 0.21 + \frac{54}{30^2} < 0.27.$$

Similarly, if $x \in (1,2)(3,4)^G \cup (1,2,3)^G$, then

$$\sum_{H \in \mathcal{I}} \mathrm{fpr}(x, G/H) < \frac{33}{128} + \sum_{\substack{l \mid n \\ 2 < l < \frac{n}{2}}} \frac{1}{l^2} + \frac{6}{n^2} < \frac{33}{128} + \frac{\pi^2}{6} - \frac{5}{4} + \frac{6}{30^2} < 0.66.$$

In order to establish the desired bound $u(G) \geqslant 2$, it suffices to show that if $x, y \in G$ have prime order, then there exists an n-cycle z such that

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

Let $P(x, s)$ be the probability that x and a randomly chosen conjugate of s do not generate G (see (4)). Then by Lemma 2.1, it is sufficient to show that

$$P(x, s) + P(y, s) < 1.$$

There are three cases to consider, according to the possibilities for x and y.

CASE 1. $x, y \notin (1,2)^G$ and either x or y is not in $(1,2)(3,4)^G \cup (1,2,3)^G$.

By applying the bound in (5), together with the above fixed point ratio estimates, we obtain

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

$$< 0.02 + 0.27 + 0.66 = 0.95$$

and the result follows.

CASE 2. $x \in (1,2)^G$.

Without loss of generality, we may assume that $x = (i, j)$ and

$$y = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \cdots ((k-1)p+1, (k-1)p+2, \ldots, kp)$$

for some prime p and integer $k \geqslant 1$. In the proof of [7, Theorem 2], Binder constructs an n-cycle z such that $G = \langle y, z \rangle$. Typically, we will show that there exists $g \in N_G(\langle y \rangle)$ such that $G = \langle x^g, z \rangle$, whence $G = \langle x, z^{g^{-1}} \rangle = \langle y, z^{g^{-1}} \rangle$ (in one particular case below, we work with a different n-cycle to the one given by

Binder). Let $\mathcal{S} \subseteq [n]$ be the set of points moved by both x and y. We will consider five cases.

CASE 2(a). $k = 1$.

Set $z = (1, 2, \ldots, n)$ and note that $G = \langle y, z \rangle$. By conjugating by an element of $N_G(\langle y \rangle)$ if necessary, we may assume that x is $(p+1, p+2)$, $(p, p+1)$ or $(1, 2)$ if $|\mathcal{S}| = 0, 1$ or 2, respectively. In each case, $G = \langle x, z \rangle$ by Lemma 4.1(i) and the result follows.

CASE 2(b). $k \geqslant 2$, $p \geqslant 3$ and $kp < n$.

Let $u = 1$ if 3 divides $n - kp$ and $u = 0$ otherwise. Then consider the n-cycle

$$z = (1, \alpha_1, p+1, 2p+1, \ldots, (k-1)p+1,$$
$$kp, kp-1, \ldots, 3, \beta_1, \beta_2, \ldots, \beta_t, 2, \gamma_1, \ldots, \gamma_u),$$

where the first ellipsis represents an arithmetic sequence with difference p and the second ellipsis represents the entire decreasing sequence from $kp - 2$ to 4, omitting any numbers that occur earlier in the cycle. By [7, Theorem 2], we have $G = \langle y, z \rangle$.

By arguing as in Case 2(a), we may assume that $x = (1, \alpha_1)$ if $|\mathcal{S}| = 1$ and $x = (kp-1, kp)$ or $x = (p, p+2)$ if $|\mathcal{S}| = 2$. In both cases, $G = \langle x, z \rangle$ (see Remark 4.2). Now assume $|\mathcal{S}| = 0$, so $n - kp \geqslant 2$. If $n - kp > 2$ then we may assume that $x = (\beta_1, \beta_2)$ and again $G = \langle x, z \rangle$.

Therefore, to complete the analysis of Case 2(b), we may assume that $n - kp = 2$ and $x = (kp+1, kp+2)$. Here we must deviate from the proof of [7, Theorem 2] and we choose a different n-cycle z. (Indeed, if 3 divides n, then $x = (\alpha_1, \beta_1)$ and $\beta_1 z^3 = \alpha_1$, so it is straightforward to see that $G \neq \langle x, z \rangle$.) In particular, let

$$z = (p+1, 2p+1, \ldots, (k-1)p+1, kp, \ldots, 2, 1, kp+1, kp+2)$$

(adopting the same conventions as above for the ellipses) and observe that

$$yz = (p+1, p, kp+1, kp+2)(2p, 2p+1) \cdots ((k-1)p, (k-1)p+1),$$
$$(yz)^2 = (p+1, kp+1)(p, kp+2).$$

First we claim that $G = \langle y, z \rangle$. To see this, suppose that $\langle y, z \rangle$ stabilises a nontrivial partition Π of $[n]$ (into parts of equal size). Then $(yz)^2$ stabilises Π. If $(yz)^2$ acts nontrivially on the set of parts of Π, then each part has size two and two parts of Π are either $\{p, p+1\}$ and $\{kp+1, kp+2\}$, or $\{p, kp+1\}$ and $\{p+1, kp+2\}$. However, since z stabilises Π, the parts of Π

must be of the form $\{a, az^{n/2}\}$ with $a \in [n]$. Since $kp + 2 = (kp + 1)z$ and $p + 1 = (kp + 2)z$, both of these options are impossible and we have reached a contradiction. Therefore, each cycle of $(yz)^2$ is contained in a part of Π. Let A be the part of Π containing p and $kp + 2$. Since y fixes $kp + 2$, we conclude that y fixes A. In particular, $1, 2, \ldots, p \in A$. Since z stabilises Π, we know that

$$A = \{1z^{li} \mid 1 \leqslant i \leqslant n/l\}$$

for some divisor $1 < l < n$. But this is a contradiction since $2z = 1 \in A$ and we conclude that $\langle y, z \rangle$ does not stabilise a nontrivial partition of $[n]$. In particular, $\langle y, z \rangle$ is a primitive subgroup of G containing a double transposition, so $G = \langle y, z \rangle$ (see [35, Example 3.3.1], noting that z is odd).

Finally, $G = \langle x, z \rangle$ since $x = (kp + 1, kp + 2)$ and $(kp + 1)z = kp + 2$ (see Remark 4.2).

CASE 2(c). $k \geqslant 2$, $p \geqslant 3$ and $kp = n$.

Here we set

$$z = (1, 2, p + 1, \ldots, (k - 1)p + 1, pk, pk + 1, \ldots, 3)$$

and we note that $G = \langle y, z \rangle$ by the proof of [7, Theorem 2]. By replacing x by a suitable $N_G(\langle y \rangle)$-conjugate, we may assume that $x = (1, 2)$ or $x = (pk, pk + 1)$. In both cases, it is easy to see that $G = \langle x, z \rangle$.

CASE 2(d). $k \geqslant 2$, $p = 2$ and $2k < n$.

Here we define

$$z = (1, 2k + 1, 2k + 2, \ldots, n, 2, 3, 5, \ldots, 2k - 1, 2k, 2k - 2, \ldots, 6, 4).$$

Again, we have $G = \langle y, z \rangle$ by the proof of [7, Theorem 2], and without loss of generality we may assume that x is one of $(2k-1, 2k)$, $(2k-2, 2k)$, $(2k+1, 2k+2)$ or $(1, 2k + 1)$. In every case, one checks that $G = \langle x, z \rangle$.

CASE 2(e). $k \geqslant 2$, $p = 2$ and $2k = n$.

Set

$$z = (1, 3, 2, 4, 5, 7, \ldots, 2k - 1, 2k, 2k - 2, \ldots, 6)$$

and note that $G = \langle y, z \rangle$ by the proof of [7, Theorem 2]. Without loss of generality, we may assume that $x = (1, 3)$ or $x = (2k - 1, 2k)$ and in both cases we have $G = \langle x, z \rangle$.

CASE 3. $x, y \in (1,2)(3,4)^G \cup (1,2,3)^G$.

If $x, y \in (1,2,3)^G$, then we may assume that $x = (1,2,3)$ and depending on the size of $\mathcal{S}$ we may assume that the support of y is one of $\{2,3,4\}$, $\{3,4,5\}$ and $\{4,5,6\}$. Moreover, since we are at liberty to replace y by y^{-1}, we may assume that

$$y \in \{(2,3,4),\ (3,4,5),\ (4,5,6)\}.$$

Similarly, if $x \in (1,2)(3,4)^G$ and $y \in (1,2,3)^G$, then we may assume that $x = (1,2)(3,4)$ and

$$y \in \{(1,2,3),\ (1,2,5),\ (2,3,5),\ (4,5,6),\ (5,6,7)\}.$$

Finally, if $x, y \in (1,2)(3,4)^G$, then we may assume that $x = (1,2)(3,4)$ and

$$y \in \{(1,3)(2,4),\ (1,2)(3,5),\ (1,2)(5,6),\ (2,3)(5,6),$$
$$(3,6)(4,5),\ (1,6)(4,5),\ (1,5)(6,7),\ (5,6)(7,8)\}.$$

In all three cases, Lemma 4.1 implies that $G = \langle x, z \rangle = \langle y, z \rangle$ for $z = (1, 2, \ldots, n)$, unless $x = (1,2)(3,4)$ and $y = (1,3)(2,4)$. In this exceptional case,

$$z = (1, 2, \ldots, n)^{(2,3)}$$

has the desired property.

This completes the proof of Theorem 4.4. ∎

We can now determine the spread and uniform spread of even-degree symmetric groups.

THEOREM 4.11: *Let $G = S_n$ with $n \geqslant 8$ even. Then $s(G) = u(G) = 2$.*

Proof. By Theorem 4.4, we have $2 \leqslant u(G) \leqslant s(G)$, so it suffices to prove that $s(G) \leqslant 2$. As noted in the proof of Proposition 4.3, if

$$G = \langle (1,2), s \rangle = \langle (2,3), s \rangle = \langle (1,3), s \rangle,$$

then s is an n-cycle. By Lemma 4.1(i), if

$$G = \langle (1,2), (1,2,\ldots,n)^g \rangle = \langle (2,3), (1,2,\ldots,n)^g \rangle,$$

then $1g \not\equiv 2g \pmod{2}$ and $2g \not\equiv 3g \pmod{2}$. This implies that $1g \equiv 3g \pmod{2}$ and thus $G \neq \langle (1,3), (1,2,\ldots,n)^g \rangle$. This shows that $s(G) \leqslant 2$, as required. ∎

4.3. UNIFORM DOMINATION. In order to complete the proof of Theorem 2, it remains to establish the bounds on the total and uniform domination numbers. We begin by establishing lower bounds on the total domination numbers (for use in Section 5, it is convenient to include alternating groups in the following proposition).

PROPOSITION 4.12: *Let $n \geqslant 5$ and let p be the smallest prime divisor of n.*

(i) $\gamma_t(S_n) \geqslant \log_2 n$.
(ii) $\gamma_t(A_n) \geqslant \log_p n$.
(iii) $\gamma_t(A_n) \geqslant 3$ *if n is composite.*

Proof. Let G be S_n or A_n and let $S = \{s_1, \ldots, s_c\}$ be a total dominating set for G. Without loss of generality, assume that $s_1, \ldots, s_j$ are n-cycles and $s_{j+1}, \ldots, s_c$ are not n-cycles (we allow $j = 0$). To begin with, we will prove that

$$\gamma_t(G) \geqslant \log_p n.$$

This is clear if n is prime, so we may assume n is composite.

If $1 \leqslant i \leqslant j$ then s_i stabilises a partition C_i of $[n]$ with parts $C_{i1}, \ldots, C_{ip}$ of size n/p. Similarly, if $j < i \leqslant c$ then s_i stabilises a proper subset A_i of $[n]$. For $j < i \leqslant c$, it will be convenient to write

$$C_i = (C_{i1}, C_{i2}) = (A_i, [n] \setminus A_i).$$

Set $R = [p]^j \times [2]^{c-j}$ and define $f \colon [n] \to R$ as $f(x) = (l_1, \ldots, l_c)$ where $x \in C_{il_i}$. For $1 \leqslant i \leqslant j$, let G_{C_i} be the stabiliser in G of the partition C_i (so G_{C_i} is isomorphic to $(S_{n/p} \wr S_p) \cap G$). Similarly, if $j < i \leqslant c$ then let $G_{\{A_i\}}$ be the setwise stabiliser of A_i.

We claim that $|R| \geqslant n - 1$. To see this, suppose that $f(x) = f(y) = f(z)$ for three distinct points $x, y, z \in [n]$. Then (x, y, z) is contained in G_{C_i} for $i \leqslant j$ and $G_{\{A_i\}}$ for $i > j$. Therefore, $G \neq \langle s_i, (x, y, z) \rangle$ for all $1 \leqslant i \leqslant c$, which is a contradiction since S is a total dominating set for G. It follows that the preimage under f of any point has size at most two. In fact, if $f(x) = f(y)$ and $f(z) = f(w)$ for four distinct points $x, y, z, w \in [n]$, then $(x, y)(z, w) \in G$ is contained in G_{C_i} for $i \leqslant j$ and in $G_{\{A_i\}}$ for $i > j$. As before, this is a contradiction and we deduce that at most one point in R has a preimage of size two. This justifies the claim.

Now $|R| = p^j 2^{c-j} \leqslant p^c$, so $p^c \geqslant n-1$. Since p divides n, it follows that $p^c \geqslant n$ and thus $\gamma_t(G) \geqslant \log_p n$. This establishes part (ii) of the proposition, and also part (i) when n is even. Therefore, it remains to prove part (iii), together with part (i) when n is odd.

In view of part (ii), in order to prove (iii) we may assume that $G = A_n$ and $n = p^2$, so p is odd. Suppose $\gamma_t(G) = 2$, say $\{s_1, s_2\}$ is a total dominating set. If s_1 and s_2 are both n-cycles, then $s_1 \in H_1$ and $s_2 \in H_2$ for stabilisers H_1 and H_2 of p-part partitions of $[n]$. But Lemma 2.3 implies that G has a base of size two in its action on the set Π_p of p-part partitions, which is a contradiction (see [50, Remark 5.3]). Therefore, we may assume that s_2 is not an n-cycle, so $2p \geqslant |R| \geqslant n - 1 = p^2 - 1$, which is absurd. We conclude that $\gamma_t(G) \geqslant 3$.

Finally, let us assume $G = S_n$ and n is odd. Here we allow n to be prime. As above, if $i > j$, then s_i stabilises a proper subset A_i of $[n]$ and we write $(C_{i1}, C_{i2}) = (A_i, [n] \setminus A_i)$. Also observe that $s_1, \ldots, s_j \in A_n$, so for each $g \in A_n$ there exists $j < i \leqslant c$ such that $S_n = \langle g, s_i \rangle$. In particular, note that $j < c$.

Define a map $f' \colon [n] \to [2]^{c-j}$ as $f'(x) = (l_{j+1}, \ldots, l_c)$ where $x \in C_{il_i}$. First assume that $j = 0$. Suppose that there exist two distinct points $x, y \in [n]$ such that $f'(x) = f'(y)$. Then $(x, y) \in G$ is contained in $G_{\{A_i\}}$ for all i, so $G \neq \langle s_i, (x, y) \rangle$ and we have reached a contradiction. Therefore, f' is injective, which implies that $2^c \geqslant n$ and $\gamma_t(G) \geqslant \log_2 n$. Now assume $j \geqslant 1$. The above argument for f implies that the map f' has the property that the preimage of any point has size at most two, and at most one point has a preimage of size two. Therefore, $2^{c-j} \geqslant n - 1$ and $\gamma_t(G) \geqslant \log_2(n-1) + j \geqslant \log_2 n$. ∎

COROLLARY 4.13: *Let $G = S_n$ with $n \geqslant 5$. Then $\gamma_u(G) \geqslant 3$.*

Proof. Since $n \geqslant 5$, Proposition 4.12 implies that

$$\gamma_u(G) \geqslant \gamma_t(G) \geqslant \lceil \log_2 n \rceil \geqslant 3. \quad \blacksquare$$

We will now complete the proof of Theorem 2 when n is odd.

PROPOSITION 4.14: *Let $G = S_n$ with $n = 2m + 1$ and $m \geqslant 2$. Then*

$$\log_2 n \leqslant \gamma_t(G) \leqslant \gamma_u(G) = b(G, \Omega) \leqslant 2 \log_2 n,$$

where Ω is the set of m-element subsets of $[n]$.

Proof. By Proposition 4.12, we have

$$\log_2 n \leqslant \gamma_t(G) \leqslant \gamma_u(G).$$

Let $s \in G$ be a witness to the bound $u(G) \geqslant 1$. Since s must be an odd permutation, it follows that $s \in H = S_k \times S_{n-k}$ for some $1 \leqslant k \leqslant m$. Now [47, Corollary 2.2] gives

$$b(G, G/H) \geqslant b(G, \Omega)$$

and thus $\gamma_u(G) \geqslant b(G, \Omega)$ by Lemma 2.3. Now fix an element $s \in G$ of shape $[m, m+1]$. As explained in the proof of Theorem 4.3, we have $\mathcal{M}(G, s) = \{H\}$ with $H = S_m \times S_{m+1}$. Therefore,

$$\gamma_u(G) \leqslant b(G, G/H) = b(G, \Omega).$$

This proves that $\gamma_u(G) = b(G, \Omega)$. Finally, by applying [47, Theorem 4.2], we conclude that

$$b(G, \Omega) \leqslant \log_{\lceil \frac{n}{m} \rceil} n \cdot \left\lceil \frac{m+1}{m} \right\rceil \leqslant 2 \log_2 n,$$

and the result follows. ∎

It remains to prove Theorem 2 when n is even.

PROPOSITION 4.15: *Let* $G = S_n$ *with* $n \geqslant 6$ *even. Then*

$$\gamma_u(G) \leqslant 3n \log_2 n.$$

Proof. Let $s = (1, 2, \ldots, n)$ and $x \in \mathcal{P}$, where $\mathcal{P}$ is the set of elements of prime order in G. If $x \notin (1, 2)^G$, then $P(x, s) < 0.67$ by the proof of Theorem 4.4. Therefore,

$$\sum_{x \in \mathcal{P} \setminus (1,2)^G} P(x, s)^{2n \log_2 n} < n! \cdot 0.67^{-n \log_{0.67} n} = n!/n^n < 1.$$

Consequently, there exists a subset $A \subseteq s^G$ such that $|A| \leqslant 2n \log_2 n$ and for all $x \in \mathcal{P} \setminus (1, 2)^G$ there exists $z \in A$ with $G = \langle x, z \rangle$.

Let $1 \leqslant k < n$. If $(k, n) = 1$, then let

$$B_k = \{(1, 1 + k, 1 + 2k, \ldots, 1 + (n-1)k)\},$$

where addition is carried out modulo n. If $(k, n) = d > 1$, then write $l = n/d - 1$ and let

$$B_k = \{b_k, c_k\}$$

where

$$b_k = (1, 1+k, 1+2k, \ldots, 1+lk,$$
$$2, 2+k, 2+2k, \ldots, 2+lk, \ldots, d, d+k, d+2k, \ldots, d+lk),$$
$$c_k = (1+k, 1+2k, \ldots, 1+lk,$$
$$1, 2+k, 2+2k, \ldots, 2+lk, 2, \ldots, d+k, d+2k, \ldots, d+lk, d).$$

Set

$$B = \bigcup_{k=1}^{n-1} B_k$$

and note that $|B| \leqslant 2(n-1)$. Let $x = (i,j) \in (1,2)^G$ with $k = j-i > 0$. Then there exists $z \in B_k$ such that $iz = j$, which implies that $G = \langle x, z \rangle$.

We conclude that for all $x \in \mathcal{P}$, there exists $z \in A \cup B$ such that $G = \langle x, z \rangle$. Moreover,

$$|A \cup B| \leqslant 2n \log_2 n + 2(n-1) \leqslant 3n \log_2 n$$

and the proof of the proposition is complete. ∎

Remark 4.16: By combining Propositions 4.12 and 4.15, we deduce that

$$\log_2 n \leqslant \gamma_u(S_n) \leqslant 3n \log_2 n$$

when n is even. It would be interesting to see if it is possible to close the gap between the lower and upper bounds on $\gamma_u(S_n)$ in this case.

5. Alternating groups

In this section we prove Theorem 3. We start by recording the spread and uniform spread of even-degree alternating groups, which were determined by Brenner and Wiegold in [10, (3.01)–(3.05)]. If $n \geqslant 4$ is even, then

$$s(A_n) = u(A_n) = \begin{cases} 2 & \text{if } n = 6, \\ 4 & \text{otherwise.} \end{cases}$$

The situation for odd-degree alternating groups is more complicated. With the aid of MAGMA, one can check that

$$s(A_5) = u(A_5) = 2, \quad s(A_7) = u(A_7) = 3.$$

Now assume $G = A_n$ with $n \geqslant 9$ odd. By [13, Proposition 6.7], we have $u(G) \geqslant 3$ and by making a minor modification to the proof of this result, we can establish the following slightly stronger bound.

PROPOSITION 5.1: *Let $G = A_n$ with $n \geqslant 9$ odd. Then $u(G) \geqslant 4$.*

Proof. If $n \leqslant 29$, then the result can be verified computationally (see [13, Table 6]). Now assume $n \geqslant 31$ and let $s \in G$ be an n-cycle. As in the proof of [13, Proposition 6.7], we have

$$\mathcal{M}(G, s) = \mathcal{I} \cup \mathcal{P}_1 \cup \mathcal{P}_2,$$

where $\mathcal{I}$ consists of exactly one imprimitive subgroup $(S_{n/l} \wr S_l) \cap G$ for each divisor l of n with $1 < l < n$, $\mathcal{P}_1$ contains at most $(n-1)/d$ subgroups isomorphic to $\mathrm{P\Gamma L}_d(q) \cap G$ for each pair (q, d) with $n = (q^d - 1)/(q - 1)$, and $\mathcal{P}_2 = \{N_G(\langle s \rangle)\}$ if n is prime (otherwise $\mathcal{P}_2$ is empty).

Suppose $x \in G$ has prime order. As in the proof of [13, Proposition 6.7], we have

$$\sum_{H \in \mathcal{P}_1} \mathrm{fpr}(x, G/H) \leqslant \frac{n^{\log_2 n + 3} 4\sqrt{\pi}}{n^{n/4} (\frac{8}{e})^{n/4}} < 10^{-6},$$

$$\sum_{H \in \mathcal{P}_2} \mathrm{fpr}(x, G/H) \leqslant 2 \left(\frac{4}{n+1} \right)^{(n-3)/2} < 10^{-8}.$$

The action of G on the set of cosets of $H = (S_{n/l} \wr S_l) \cap G$ is equivalent to the action on Π_l, so by applying Lemmas 4.5 and 4.6, noting that x is even and $2 < l < \frac{n}{2}$ since n is odd, we see that $\mathrm{fpr}(x, \Pi_l) < \frac{1}{l^2}$. Therefore,

$$\sum_{H \in \mathcal{I}} \mathrm{fpr}(x, G/H) \leqslant \sum_{\substack{l \mid n \\ 1 < l < n}} \frac{1}{l^2} < \sum_{m=1}^{\infty} \frac{1}{(2m+1)^2} = \frac{\pi^2}{8} - 1$$

and thus

$$\sum_{H \in \mathcal{M}(G, s)} \mathrm{fpr}(x, G/H) < \frac{\pi^2}{8} - 1 + 10^{-6} + 10^{-8} < \frac{1}{4}.$$

By applying Corollary 2.2, we conclude that $u(G) \geqslant 4$. ∎

Remark 5.2: As noted in Remark 3(c), the uniform spread of odd-degree alternating groups can be arbitrarily large. Indeed, [46, Theorem 1.1] states that if (n_i) is a sequence of natural numbers tending to infinity, then $u(A_{n_i})$ tends to infinity if and only if the least prime divisor of n_i tends to infinity (see Theorem $(\star)$(ii) and (3)).

We now turn to uniform domination.

PROPOSITION 5.3: *Let $G = A_n$ with $n \geqslant 5$ and let p be the smallest prime divisor of n. Then*

$$\log_p n \leqslant \gamma_t(G) \leqslant \gamma_u(G) \leqslant c \log_2 n$$

where $c = 2$ if n is even and $c = 77$ if n is odd.

Proof. This is a combination of Proposition 4.12(ii) and [27, Theorem 2]. ∎

Remark 5.4: Let us consider the upper bound in Proposition 5.3. Let $G = A_n$, where $n = 2m \geqslant 8$ is even, and let k be the greatest odd integer strictly less than m. For $1 < \ell < n$, let Σ_ℓ be the set of ℓ-element subsets of $[n]$. To establish the upper bound on $\gamma_u(G)$ in the proposition, we show that if $s \in G$ has shape $[k, n - k]$ then $\mathcal{M}(G, s) = \{H\}$ with $H = (S_k \times S_{n-k}) \cap G$ and thus $\gamma_u(G) \leqslant b(G, \Sigma_k)$. This is very similar to Proposition 4.14 for odd-degree symmetric groups, where we showed that $\gamma_u(S_{2m+1}) = b(S_{2m+1}, \Omega)$ for the set Ω of m-element subsets of $[2m + 1]$. Therefore, it is natural to ask if equality holds, that is, do we have $\gamma_u(G) = b(G, \Sigma_k)$?

Let $S \subseteq s^G$ be a TDS for G and note that s acts intransitively on $[n]$ since n is even. By [47, Corollary 2.2(2)], $b(G, \Sigma_i) \geqslant b(G, \Sigma_j)$ if $i \leqslant j \leqslant m$. Therefore, we can conclude that $|S| \geqslant b(G, \Sigma_k)$ unless s has shape $[m, m]$, or m is odd and s has shape $[m + 1, m - 1]$. In particular, if $\gamma_u(G) < b(G, \Sigma_k)$, then this has to be witnessed by a conjugacy class s^G of elements of shape $[m, m]$, or of shape $[m + 1, m - 1]$ if m is odd. In these two cases, s could be contained in several imprimitive maximal overgroups and since the base size $b(G, \Sigma_k)$ is not known exactly, it is difficult to use our probabilistic method to determine if s^G does indeed witness $\gamma_u(G) < b(G, \Sigma_k)$.

PROPOSITION 5.5: *Let $G = A_n$ with $n \geqslant 5$.*
   (i) *$\gamma_u(G) = 2$ if and only if $n \geqslant 13$ is a prime number.*
   (ii) *If $\gamma_u(G) = 2$, then $P(G, s, 2) > 0$ if and only if s is an n-cycle.*

Proof. If $\gamma_u(G) = 2$, then Proposition 4.12(iii) implies that n is prime and thus part (i) follows via [27, Proposition 3.8 and Remark 3.12]. For (ii), if $s \in G$ is not an n-cycle, then s is contained in a maximal intransitive subgroup H and thus Lemma 2.3 implies that $P(G, s, 2) = 0$ since $b(G, G/H) \geqslant 3$. ∎

Remark 5.6: The proof of Proposition 5.5 shows that if $G = A_n$ with $n \geqslant 13$, then $\gamma_t(G) = 2$ if and only if n is prime. Moreover, the only possible witnesses are two (not necessarily conjugate) n-cycles.

In order to complete the proof of Theorem 3, it remains to consider the probability $P_2(A_n)$ when $n \geqslant 13$ is a prime. Set

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

and observe that $3, 5, 7, 13, 17, 31, 73, 127, 257, 307$ are the ten smallest primes in $\mathcal{H}$.

PROPOSITION 5.7: *Let $G = A_n$, where $n \geqslant 13$ is a prime with $n \notin \mathcal{H}$. Then*

$$P_2(G) > 1 - n^{-2}.$$

Proof. By Proposition 5.5, we have $P_2(G) = P(G, s, 2)$ where $s \in G$ is an n-cycle. To begin with, let us assume $n \neq 23$. Then $\mathcal{M}(G, s) = \{H\}$, where $H = N_G(\langle s \rangle) = C_n{:}C_{(n-1)/2}$, and we have $P_2(G) = 1 - Q(G, s, 2)$. Moreover, Lemma 2.5 gives

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

where the x_i represent the conjugacy classes in G of elements of prime order.

Let $x \in H$ be an element of prime order t. If $t = n$ then

$$|x^G \cap H| = \frac{1}{2}(n-1) = a \quad \text{and} \quad |x^G| = \frac{1}{2}(n-1)! = b.$$

Now assume t divides $(n-1)/2$. Here x has a unique fixed point on $[n]$, so

$$|x^G \cap H| = i_t(H) = n(t-1) = a_t, \quad |x^G| = \frac{n!}{((n-1)/t)! \, t^{(n-1)/t}} = b_t$$

and thus

$$\widehat{Q}(G, s, 2) = a^2/b + \sum_{t \in \pi} a_t^2/b_t,$$

where π is the set of prime divisors of $(n-1)/2$. Now $|\pi| \leqslant \log_2((n-1)/2)$ and one checks that $a_t^2/b_t \leqslant a_2^2/b_2$ for all $t \in \pi$, so

$$P_2(G) \geqslant 1 - \frac{n-1}{2(n-2)!} - \log_2((n-1)/2) \cdot \frac{n^2((n-1)/2)! \, 2^{(n-1)/2}}{n!}$$

and the desired bound follows.

Finally, let us assume that $n = 23$. Here $\mathcal{M}(G, s) = \{H, K\}$ with $H \cong K \cong M_{23}$ and with the aid of MAGMA we calculate that

$$\widehat{Q}(G, s, 2) = 4 \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H)^2 = \frac{27704}{178562475}.$$

The result follows. ∎

Remark 5.8: In the previous proposition, it is easy to compute $P_2(G)$ precisely when $m = (n-1)/2$ is a prime and $n \neq 23$. As before, let $s \in G$ be an n-cycle and write $\mathcal{M}(G, s) = \{H\}$. Let r be the number of regular orbits of H on G/H. By arguing as in the proof of [24, Proposition 3.2] we calculate that

$$r = \frac{|G : H| - n(m^2 - m - 1) - 1}{|H|}$$

and thus

$$P_2(G) = 1 - \frac{n^3 - 4n^2 - n + 4}{4(n-2)!}$$

by Lemma 2.4.

PROPOSITION 5.9: *Let $G = A_n$, where $n > 13$ is a prime. Then*

$$P_2(G) > 1 - n^{-1}.$$

Proof. In view of the previous proposition, we may assume $n \in \mathcal{H}$. Let $s \in G$ be an n-cycle, so $P_2(G) = P(G, s, 2)$. If $n \geqslant 73$, then by arguing as in the proof of [27, Proposition 3.8], we obtain

$$P_2(G) > 1 - \left(\frac{2 \log_2 n}{n-1}\right)^2$$

and the result follows if $n > 257$. For $n \in \{73, 127, 257\}$, the desired bound is easily obtained by inspecting the proof of [27, Proposition 3.8]. For example, the proof gives

$$P_2(G) > 1 - \left(\frac{\ell}{C}\right)^2,$$

where $\ell = 1 + (n-1) \sum_{(q,d)} \frac{1}{d}$ and $C = n(n-1)/2$ (the sum in the expression for ℓ is over all prime powers q and integers $d \geqslant 2$ with $n = (q^d - 1)/(q - 1)$). For $n = 73$ we have $n = (8^3 - 1)/(8 - 1)$ only, so $\ell = 25$, $C = 2628$ and the desired bound quickly follows. The cases when n is 127 or 257 are just as straightforward.

Finally, if $n = 17$ then $\mathcal{M}(G, s) = \{H, K\}$, where H and K are non-conjugate maximal subgroups isomorphic to $\mathrm{P\Gamma L}_2(16)$. Here we calculate

$$\widehat{Q}(G, s, 2) = \frac{335848}{42567525} < \frac{1}{17}$$

and the result follows. Similarly, if $n = 31$ then $\widehat{Q}(G, s, 2) < \frac{1}{31}$. ∎

Remark 5.10: The case $G = A_{13}$ requires special attention. As above, we have $P_2(G) = P(G, s, 2)$ with $s \in G$ a 13-cycle and we observe that

$$\mathcal{M}(G, s) = \{H, K_1, K_2, L_1, L_2\},$$

where $H = N_G(\langle s \rangle) = C_{13}{:}C_6$ and each of the remaining subgroups are isomorphic to $\mathrm{P\Gamma L}_3(3)$, with K_1, K_2 conjugate, and L_1, L_2 conjugate. One checks that

$$\widehat{Q}(G, s, 2) = \frac{4230997}{1108800} > 1,$$

so the probabilistic approach does not yield $P_2(G) > 0$. However, as noted in the proof of [27, Proposition 3.8], by randomly choosing conjugates of a fixed 13-cycle, we can identify a TDS for G. For example,

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

has the desired property (see [28, Section 1.2.4] for further details). This shows that $P_2(G) > 0$, but further work is needed to compute this probability precisely. To do this, we use the fact that $\{s, s^g\}$ is a TDS for G if and only if $A \cap B = 1$ for all $A \in \mathcal{M}(G, s)$ and all $B \in \mathcal{M}(G, s^g)$ (see [27, Lemma 2.1]). In this way, we can use MAGMA to show that

$$P_2(G) = \frac{|\{s^g \in s^G : \{s, s^g\} \text{ is a TDS for } G\}|}{|s^G|} = \frac{4979}{46200}$$

and we conclude that A_{13} is a genuine exception to the bound in Proposition 5.9.

6. Exceptional groups of Lie type

In this section, we assume G is a finite simple exceptional group of Lie type over $\mathbb{F}_q$. Our aim is to prove Theorem 4. Note that Theorem $(\star)$ (see the introduction) implies that $u(G) \geqslant 3$, and $u(G) \to \infty$ as $q \to \infty$.

Remark 6.1: By applying Corollary 2.2, it is possible to determine explicit lower bounds on $u(G)$ in terms of q. For example, suppose $G = {}^2B_2(q)$ with $q = 2^{2m+1}$ and $m \geqslant 1$. Let $s \in G$ be an element of order $q - \sqrt{2q} + 1$. By

inspecting [69, Theorem 9], which lists the maximal subgroups of G, one can show that $\mathcal{M}(G, s) = \{H\}$ with $H = N_G(\langle s \rangle) = C_{q - \sqrt{2q} + 1} : C_4$ (see the proof of Lemma 6.7). Let $x \in G$ be an element of prime order r. Since G contains a unique conjugacy class of involutions, it follows that

$$\mathrm{fpr}(x, G/H) = \frac{i_2(H)}{i_2(G)} = \frac{q - \sqrt{2q} + 1}{(q^2 + 1)(q - 1)} = \frac{1}{(q + \sqrt{2q} + 1)(q - 1)}$$

if $r = 2$. Similarly, if r is odd then we may assume r divides $q - \sqrt{2q} + 1$ (otherwise $\mathrm{fpr}(x, G/H) = 0$), so $|C_G(x)| = q - \sqrt{2q} + 1$ and we deduce that

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

Therefore, Corollary 2.2 implies that

$$u(G) \geqslant (q + \sqrt{2q} + 1)(q - 1) - 1.$$

Let us now turn to the uniform domination number. In [27, Theorem 5.2], we established the bound $\gamma_u(G) \leqslant 6$ for every finite simple exceptional group G. By applying recent work of the first author in [23], we can prove a stronger result.

THEOREM 6.2: *If G is a finite simple exceptional group of Lie type, then $\gamma_u(G) \leqslant 5$.*

Proof. First assume there exists an element $s \in G$ with $\mathcal{M}(G, s) = \{H\}$ for some maximal subgroup H of G. Then Lemma 2.3 implies that $\gamma_u(G) = b(G, H)$ and by applying the main theorem of [23], noting that H is non-parabolic, it follows that $\gamma_u(G) \leqslant 5$.

By arguing as in the proof of [27, Theorem 5.2], it remains to consider the cases

    (a) $G = F_4(q)$, $q = 2^a$, $a \geqslant 2$; and
    (b) $G = G_2(q)$, $q = 3^a$, $a \geqslant 2$.

First consider (a). As noted in the proof of [27, Theorem 5.2], there exists an element $s \in G$ with $\mathcal{M}(G, s) = \{H, K\}$ and $H \cong K \cong {}^3D_4(q).3$. It suffices to show that

$$(8) \qquad \widehat{Q}(G, s, 5) := 32 \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H)^5 < 1,$$

where $x_1, \ldots, x_k$ are representatives of the conjugacy classes in G of elements of prime order. Let $\bar{G} = F_4$ and $\bar{H} = D_4$ be the corresponding algebraic groups

defined over the algebraic closure of $\mathbb{F}_q$. Let V_{26} be one of the 26-dimensional irreducible modules for $\bar{G}$ and note that

$$(9) \qquad\qquad V_{26} \downarrow \bar{H} = V(\lambda_1) \oplus V(\lambda_3) \oplus V(\lambda_4) \oplus 0^2,$$

where $V(\lambda_1)$ is the natural module for $\bar{H}$, $V(\lambda_3)$ and $V(\lambda_4)$ are the two spin modules and 0 is the trivial module (see [70, Chapter 12], for example). Let $x \in H$ be an element of prime order r.

First assume $r = 2$, so $x \in {}^3D_4(q)$. There are two classes of involutions in ${}^3D_4(q)$, labelled A_1 and A_1^3 in the notation of [66]. As elements of $\bar{H}$, the involutions in the first class are of type a_2 and those in the second are of type c_4 (in the notation of [2]). By considering the decomposition in (9), we deduce that if x is in the A_1 class of ${}^3D_4(q)$, then it has Jordan form $[J_2^6, J_1^{14}]$ on V_{26}, and similarly $[J_2^{12}, J_1^2]$ if it is in the class labelled A_1^3. By inspecting [54, Table 3], we conclude that the involutions in the A_1 class of ${}^3D_4(q)$ are in the G-class labelled A_1, and the others are in G-class $A_1\tilde{A}_1$. The relevant class sizes in G are given in [59, Table 22.2.4] and we deduce that the contribution to $\widehat{Q}(G, s, 5)$ from involutions is precisely $32(a_1b_1^5 + a_2b_2^5)$, where

$$a_1 = (q^4 + 1)(q^{12} - 1), \quad b_1 = \frac{1}{q^6 + q^4 + q^2 + 1}$$

and

$$a_2 = q^4(q^4 + q^2 + 1)(q^8 - 1)(q^{12} - 1), \quad b_2 = \frac{1}{q^2(q^2 + 1)(q^8 - 1)}.$$

Now assume $r > 2$, so x is semisimple. By arguing as in the proof of [23, Lemma 3.17], we deduce that the combined contribution to $\widehat{Q}(G, s, 5)$ from the elements with $C_{\bar{G}}(x)^0 = B_3T_1$ or C_3T_1 is at most

$$32 \cdot 2q^{15}(q^4 + 1)(q^{12} - 1) \cdot \left(\frac{48(q + 1)}{q^9(q - 1)^4}\right)^5 < q^{-7}.$$

Similarly, the contribution from regular semisimple elements is less than $32q^{-33}$. For all other semisimple elements, the bound in [23, (17)] gives

$$\mathrm{fpr}(x, G/H) < q^{-11}$$

and it follows that the remaining contribution is less than $32q^{50}(q^{-11})^5 = 32q^{-5}$. In conclusion,

$$\widehat{Q}(G, s, 5) < 32(a_1b_1^5 + a_2b_2^5) + q^{-7} + 32q^{-33} + 32q^{-5} < 1$$

and thus $\gamma_u(G) \leqslant 5$.

Finally, let us consider case (b). Here there is an element $s \in G$ such that $\mathcal{M}(G, s) = \{H, K\}$ with $H \cong K \cong \mathrm{SU}_3(q).2$ and so it suffices to show that (8) holds. Let $x \in H$ be an element of prime order r. Let $\bar{G} = G_2$ and $\bar{H} = A_2$ be the corresponding algebraic groups over the algebraic closure of $\mathbb{F}_q$.

First assume $r = 3$, so $x \in \mathrm{SU}_3(q)$. Let V_7 be one of the 7-dimensional irreducible modules for $\bar{G}$ and note that

$$V_7 \downarrow \bar{H} = V_3 \oplus V_3^* \oplus 0,$$

where V_3 is the natural module for $\bar{H}$ (and V_3^* is its dual). If $x \in H$ has Jordan form $[J_2, J_1]$ on V_3, then the above decomposition implies that $[J_2^2, J_1^3]$ is the Jordan form of x on V_7. Similarly, the regular unipotent elements in H have Jordan form $[J_3^2, J_1]$. By inspecting [54, Table 1], we deduce that x belongs to the G-classes labelled A_1 and $G_2(a_1)$ in the two respective cases, whence the contribution to $\widehat{Q}(G, s, 5)$ from elements of order 3 is precisely $32(a_1 b_1^5 + a_2 b_2^5)$, where

$$a_1 = q^6 - 1, \quad b_1 = \frac{1}{q^2 + q + 1}, \quad a_2 = \frac{1}{2} q^2 (q^2 - 1)(q^6 - 1), \quad b_2 = \frac{2}{q(q^3 - 1)}.$$

Next assume $r = 2$. Now G contains $a_3 = q^4(q^4 + q^2 + 1)$ involutions, which form a single conjugacy class, and thus

$$|x^G \cap H| = i_2(H) = \frac{|\mathrm{GU}_3(q)|}{|\mathrm{GU}_2(q)||\mathrm{GU}_1(q)|} + \frac{|\mathrm{SU}_3(q)|}{|\mathrm{SO}_3(q)|} = q^2(q^2 - q + 1)(q + 2).$$

Therefore,

$$\mathrm{fpr}(x, G/H) = \frac{q^2(q^2 - q + 1)(q + 2)}{q^4(q^4 + q^2 + 1)} = \frac{(q^2 - q + 1)(q + 2)}{q^2(q^4 + q^2 + 1)} = b_3$$

and $32 a_3 b_3^5$ is the contribution from involutions. Finally, if $r \geqslant 5$ then the proof of [29, Lemma 4.31] gives

$$\mathrm{fpr}(x, G/H) < \frac{4(q + 1)^2}{(q - 1)^2} \cdot q^{-4} \leqslant \frac{25}{4} q^{-4}$$

and thus the total contribution to $\widehat{Q}(G, s, 5)$ from elements of order at least 5 is less than

$$32q^{14} \cdot \left(\frac{25}{4} q^{-4} \right)^5 < 6q^{-1}.$$

We conclude that

$$\widehat{Q}(G, s, 5) < 32 \sum_{i=1}^{3} a_i b_i^5 + 6q^{-1} < 1.$$

The result follows. ∎

By [27, Theorem 5.2], we have $\gamma_u(G) = 2$ if G is one of ${}^2B_2(q)$, ${}^2G_2(q)$ (with $q \geqslant 27$) or $E_8(q)$. The following theorem, which is the main result of this section, completely determines the simple exceptional groups G with $\gamma_u(G) = 2$.

THEOREM 6.3: *Let G be a finite simple exceptional group of Lie type over $\mathbb{F}_q$. Then $\gamma_u(G) = 2$ if and only if*

$$G \in \{{}^2B_2(q),\ {}^2G_2(q)\ (q \geqslant 27),\ {}^2F_4(q)\ (q \geqslant 8),\ {}^3D_4(q),\ E_6^\epsilon(q),\ E_7(q),\ E_8(q)\}.$$

Moreover, if $\gamma_u(G) = 2$ then $P_2(G) > 1 - q^{-1}$.

In order to prove Theorem 6.3, we need to record some preliminary results.

LEMMA 6.4: *Let G be a finite simple group of Lie type and let $\mathcal{P}$ be the union of the parabolic subgroups of G. Then $G \setminus \mathcal{P}$ is the set of regular semisimple elements that are not contained in a maximal torus of a Levi factor of a parabolic subgroup of G.*

Proof. If $u \in G$ is a nontrivial unipotent element, then $C_G(u)$ is contained in a parabolic subgroup of G. Therefore, each $x \in G \setminus \mathcal{P}$ is a regular semisimple element and the result follows. ∎

Recall that if G is a finite simple exceptional group and H is a maximal subgroup of G, then $b(G, G/H) \leqslant 6$ by the main theorem of [29]. The next two lemmas, which may be of independent interest, show that $b(G, G/H) = 2$ in two special cases. These results will play an essential role in the proof of Theorem 6.3 when $G = E_7(q)$ or $E_6^\epsilon(q)$.

Notation: In Lemmas 6.5 and 6.6, we use the notation $P(G, H, 2)$ to denote the probability that $H \cap H^g = 1$ for a randomly chosen conjugate H^g. Equivalently, this is the probability that two randomly chosen points in G/H form a base for G, with respect to the natural action of G on G/H. In particular, $b(G, G/H) = 2$ if and only if $P(G, H, 2) > 0$. Moreover, if $Q(G, H, 2) = 1 - P(G, H, 2)$ denotes the complementary probability, then

$$(10) \qquad Q(G, H, 2) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H)^2 =: \widehat{Q}(G, H, 2),$$

where $x_1, \ldots, x_k$ represent the conjugacy classes of elements of prime order in G (see the proof of [61, Theorem 1.3], for example).

LEMMA 6.5: *If $G = E_7(q)$ and $H = (\mathrm{L}_2(q^3) \times {}^3D_4(q)).3$, then*

$$P(G, H, 2) > 1 - q^{-2}.$$

Proof. It suffices to show that $\widehat{Q}(G, H, 2) < q^{-2}$. Let $\bar{G} = E_7$ and $\bar{H} = A_1^3 D_4.S_3$ be the corresponding ambient algebraic groups over the algebraic closure of $\mathbb{F}_q$. Let $\mathcal{L}(\bar{G})$ be the Lie algebra of $\bar{G}$ and let V_{56} be the 56-dimensional irreducible module for $\bar{G}$. Fix a set of fundamental dominant weights $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ for the D_4 factor of $\bar{H}$. It will be useful to record the restrictions

$$
(11) \quad
\begin{aligned}
\mathcal{L}(\bar{G}) \downarrow A_1^3 D_4 = & \mathcal{L}(A_1^3 D_4) \oplus (V_2 \otimes V_2 \otimes 0 \otimes V(\lambda_4)) \\
& \oplus (V_2 \otimes 0 \otimes V_2 \otimes V(\lambda_3)) \oplus (0 \otimes V_2 \otimes V_2 \otimes V(\lambda_1)),
\end{aligned}
$$

$$
(12) \quad
\begin{aligned}
V_{56} \downarrow A_1^3 D_4 = & (V_2 \otimes V_2 \otimes V_2 \otimes 0) \oplus (V_2 \otimes 0 \otimes 0 \otimes V(\lambda_1)) \\
& \oplus (0 \otimes V_2 \otimes 0 \otimes V(\lambda_3)) \oplus (0 \otimes 0 \otimes V_2 \otimes V(\lambda_4))
\end{aligned}
$$

(see [70, Chapter 12], for example). Here V_2 and 0 denote the natural and trivial modules for A_1, respectively, and we write $V(\lambda_i)$, with $i = 1, 3, 4$, for the 8-dimensional irreducible module for D_4 with highest weight λ_i (so $V(\lambda_1)$ is the natural module, and $V(\lambda_3), V(\lambda_4)$ are the two spin modules).

Set $H = H_0.\langle \tau \rangle = H_0.3$, where $H_0 = \mathrm{L}_2(q^3) \times {}^3D_4(q)$ and τ induces a field automorphism φ on $\mathrm{L}_2(q^3)$ and a graph automorphism on ${}^3D_4(q)$. If we view H_0 as a subgroup of the connected component $\bar{H}^0$, then we may assume that

$$H_0 = \{(x, x^\varphi, x^{\varphi^2}, y) : x \in \mathrm{L}_2(q^3), \; y \in {}^3D_4(q)\} < \bar{H}^0.$$

In particular, note that τ cyclically permutes the three A_1 factors of $\bar{H}^0$. Write

$$(13) \qquad\qquad \widehat{Q}(G, H, 2) = \alpha + \beta,$$

where α and β denote the contributions from unipotent and semisimple elements, respectively. We refer the reader to [59, Table 22.2.2] and [40, Section 3] for detailed information on the unipotent and semisimple conjugacy classes in G (including centraliser orders). In particular, we will adopt the notation from [59] for labelling the unipotent classes in $\bar{G}$, which is consistent with the standard Bala–Carter notation.

Let $x \in H$ be an element of prime order r and write $q = p^f$ with p a prime. First assume $r = p = 2$. If x is a long root element, then [56, Proposition 1.13(iii)] implies that $x^G \cap H$ is the set of long root elements in the ${}^3D_4(q)$ factor of H_0, so $|x^G \cap H| < q^{10}$, $|x^G| > \frac{1}{2}q^{34}$ and the contribution to α is less

than $2q^{-14}$. In the remaining cases, we have $|x^G| > \frac{1}{2}q^{52}$ and we note that

$$i_2(H) = (i_2(\mathrm{L}_2(q^3)) + 1)(i_2(^3D_4(q)) + 1) - 1 < q^{21},$$

so the contribution to α from these elements is less than $\frac{1}{2}q^{52}(2q^{-31})^2 = 2q^{-10}$. Therefore, $\alpha < 2q^{-14} + 2q^{-10}$ when $p = 2$.

Next assume $r = p \geqslant 3$. If $x \in H \setminus H_0$ then $r = 3$ and x belongs to one of the G-classes labelled A_2^2 or $A_2^2A_1$ (see the proof of [26, Proposition 5.12]). Therefore, $|x^G| > \frac{1}{2}q^{84}$ and thus the contribution to α is less than $\frac{1}{2}q^{84}(2q^{-45})^2 = 2q^{-6}$ since $|H| < q^{39}$. Now assume $x^G \cap H \subseteq H_0$. If $\dim x^{\bar{G}} \geqslant 64$ then $|x^G| > \frac{1}{2}q^{64}$ and thus the contribution to α from these elements is less than $\frac{1}{2}q^{64}(2q^{-34})^2 = 2q^{-4}$ since H_0 contains fewer than $q^6 \cdot q^{24} = q^{30}$ elements of order p. Now assume $\dim x^{\bar{G}} < 64$, in which case x belongs to one of the $\bar{G}$-classes labelled A_1, A_1^2 or $(A_1^3)^{(1)}$. As above, the contribution from long root elements is less than $2q^{-14}$. More generally, we can use (12) to calculate the Jordan form of each unipotent element $x \in H_0$ on V_{56}, which in turn allows us to determine the $\bar{G}$-class of x by inspecting [54, Table 7].

For example, suppose $x = yz \in H_0$, where $y \in \mathrm{L}_2(q^3)$ is a long root element and $z \in {}^3D_4(q)$ is in the class labelled A_2' in [66]. In terms of (12), y has Jordan form $[J_2]$ on V_2 and z has Jordan form $[J_3^2, J_1^2]$ on each $V(\lambda_i)$. Therefore, x has Jordan form

$$(J_2 \otimes J_2 \otimes J_2) \oplus (J_2 \otimes [J_3^2, J_1^2])^3 = \begin{cases} [J_4^7, J_2^{14}] & \text{if } p \geqslant 5 \\ [J_3^{14}, J_2^7] & \text{if } p = 3 \end{cases}$$

on V_{56} and by inspecting [54, Table 7] we conclude that x is in the $\bar{G}$-class $A_2A_1^3$.

In this way, we see that there are no unipotent elements in H_0 that belong to the $\bar{G}$-class A_1^2. Similarly, the elements in the class $(A_1^3)^{(1)}$ correspond to long root elements in the $\mathrm{L}_2(q^3)$ factor. Therefore, if x is in $(A_1^3)^{(1)}$ then $|x^G| > \frac{1}{2}q^{54}$, $|x^G \cap H| < q^6$ and so the contribution from these elements is less than $\frac{1}{2}q^{54}(2q^{-48})^2 = 2q^{-42}$. To summarise, we have

$$\alpha < 2q^{-6} + 2q^{-4} + 2q^{-14} + 2q^{-42}$$

for all $q \geqslant 2$.

Now let us turn to β. If $r = 2$ then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{55}$ and we calculate that

$$i_2(H) = (i_2(\mathrm{L}_2(q^3)) + 1)(i_2(^3D_4(q)) + 1) - 1 < (q^6 + 1)(q^8(q^8 + q^4 + 1) + 1) < q^{23},$$

which means that the contribution to β from involutions is less than $4q^{-8}$. Now assume $r \geqslant 3$. If $\dim x^{\bar{G}} \geqslant 84$ then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{85}$ and since $|H| < q^{39}$ we see that the contribution to β from these elements is less than $4q^{-6}$.

Finally, let us assume $r \geqslant 3$ and $\dim x^{\bar{G}} < 84$, so $C_{\bar{G}}(x)^0 = D_6 T_1$ or $E_6 T_1$. Set $V = \mathcal{L}(\bar{G})$ and note that

$$\dim C_V(x) = \dim C_{\bar{G}}(x)$$

(see [32, Section 1.14]). If $x \in H \setminus H^0$ then $r = 3$ and by considering (11) we calculate that $\dim C_V(x) = 35 + a$, where $a = \dim C_{\mathcal{L}(D_4)}(x)$. Since $a \leqslant 28$ we have $\dim C_V(x) \leqslant 63$ and thus $C_{\bar{G}}(x)^0 \notin \{D_6 T_1, E_6 T_1\}$. For the remainder, we may assume that $x^G \cap H \subseteq H_0$. Write $x = yz \in H_0$, where $y \in \mathrm{L}_2(q^3)$ and $z \in {}^3D_4(q)$.

We claim that $\dim C_V(x) < 67$ if $y \neq 1$ and $z \neq 1$. To see this, let d denote the codimension of the largest eigenspace of z on the natural D_4-module $V(\lambda_1)$. Since $z \in {}^3D_4(q)$, it follows that d is also the codimension of the largest eigenspace of z on both $V(\lambda_3)$ and $V(\lambda_4)$. In addition, $d \geqslant 4$ and $\dim C_{D_4}(z) \leqslant 10$ (see the proof of [20, Lemma 2.12], for example). Set

$$W_1 = \mathcal{L}(A_1^3 D_4), \quad W_2 = V_2 \otimes V_2 \otimes 0 \otimes V(\lambda_4).$$

Then $\dim C_{W_1}(x) \leqslant 1 + 1 + 1 + 10 = 13$ and by applying [60, Lemma 3.7] we deduce that $\dim C_{W_2}(x) \leqslant 32 - 4d \leqslant 16$. Similarly, the 1-eigenspace of x on each of the other two summands in the decomposition (11) has dimension at most 16, so $\dim C_V(x) \leqslant 13 + 48 = 61$ and the claim follows. In a similar fashion, one checks that $\dim C_V(x) < 79$ if $y = 1$ and $z \neq 1$. It follows that H contains fewer than q^9 semisimple elements x with $C_{\bar{G}}(x) = E_6 T_1$, and since $|x^G| > \frac{1}{2}(q+1)^{-1}q^{55}$ we deduce that their contribution to β is less than q^{-34}. Similarly, if $C_{\bar{G}}(x) = D_6 T_1$ then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{67} = b$ and there are fewer than $a = q^9 + q^{28}$ semisimple elements $x \in H_0$ of the form $x = yz$ with $y = 1$ or $z = 1$, so the contribution here is less than q^{-8}.

We conclude that

$$\beta < 4q^{-8} + 4q^{-6} + q^{-34} + q^{-8}.$$

By combining this estimate with the above bound on α, we see that

$$\widehat{Q}(G, H, 2) < 2q^{-6} + 2q^{-4} + 2q^{-14} + 2q^{-42} + 4q^{-8} + 4q^{-6} + q^{-34} + q^{-8} < q^{-2}$$

and the result follows.   ∎

LEMMA 6.6: *If $G = E_6^\epsilon(q)$ and $H = L_3^\epsilon(q^3).3$, then $P(G, H, 2) > 1 - q^{-4}$.*

Proof. It suffices to show that $\widehat{Q}(G, H, 2) < q^{-4}$. Let $\bar{G} = E_6$ and $\bar{H} = A_2^3.S_3$ be the corresponding algebraic groups over the algebraic closure of $\mathbb{F}_q$ and let $V = \mathcal{L}(\bar{G})$ be the Lie algebra of $\bar{G}$. We have

$$(14) \qquad V \downarrow A_2^3 = \mathcal{L}(A_2^3) \oplus (V_3 \otimes V_3 \otimes V_3) \oplus (V_3^* \otimes V_3^* \otimes V_3^*),$$

where V_3 denotes the natural module for A_2. It will be convenient to set

$$W_1 = \mathcal{L}(A_2^3), \quad W_2 = V_3 \otimes V_3 \otimes V_3.$$

Also set $\mathbb{F} = \mathbb{F}_{q^{3u}}$, where $u = 1$ if $\epsilon = +$ and $u = 2$ if $\epsilon = -$.

Write $H = H_0.\langle\varphi\rangle = H_0.3$, where $H_0 = L_3^\epsilon(q^3)$ and φ is a field automorphism of order 3. Without any loss of generality, we may assume that

$$H_0 = \{(x, x^\varphi, x^{\varphi^2}) : x \in L_3^\epsilon(q^3)\} < \bar{H}^0,$$

so φ cyclically permutes the three A_2 factors of $\bar{H}^0$. In order to estimate α and β, as defined in (13), we will refer repeatedly to the information on unipotent and semisimple conjugacy classes in [59, Table 22.2.3] and [40, Section 2], respectively. As in the proof of the previous lemma, we will use the notation from [59] for labelling unipotent classes.

Write $q = p^f$, with p a prime, and let $x \in H$ be an element of prime order r. We begin by considering α. First assume $r = p = 2$. Here H_0 has a unique class of involutions (with Jordan form $[J_2, J_1]$ on V_3) and by considering the decomposition in (14) we calculate that x has Jordan form $[J_2^{38}, J_1^2]$ on V. By inspecting [54, Table 6], it follows that x is in the $\bar{G}$-class A_1^3, so $|x^G| > \frac{1}{2}q^{40}$, $|x^G \cap H| = i_2(H) = (q^3 + \epsilon)(q^9 - \epsilon)$ and we deduce that $\alpha < 2q^{-15}$ when $p = 2$.

Now assume $r = p \geqslant 3$. If $x \in H \setminus H_0$ then $r = 3$ and the proof of [26, Proposition 5.13] implies that x is in one of the $\bar{G}$-classes labelled A_2^2 or $A_2^2 A_1$. Therefore, $|x^G| > \frac{1}{2}q^{48} = a$ and we note that there are fewer than $i_3(H) < 2q^{15}(q^3 + 1) = b$ such elements in H (see [57, Proposition 1.3]). It follows that the contribution to α from these elements is less than $a(b/a)^2 < q^{-10}$. Now assume $x^G \cap H \subseteq H_0$, so $x \in H_0$. As above, we calculate that the long root elements $x \in H_0$ are contained in the $\bar{G}$-class labelled A_1^3. In this case, $|x^G| > \frac{1}{2}q^{40}$, $|x^G \cap H| < 2q^{12}$ and thus the contribution is less than q^{-14}.

Similarly, if $x \in H_0$ is a regular unipotent element then it has Jordan form

$$\begin{cases} [J_5, J_3]^3 \\ [J_3^2, J_1^2]^3 \end{cases} \oplus (J_3 \otimes J_3 \otimes J_3)^2 = \begin{cases} [J_5^{11}, J_3^7, J_1^2] & \text{if } p \geqslant 5 \\ [J_3^{24}, J_2^3] & \text{if } p = 3 \end{cases}$$

on V. By inspecting [54, Table 6], it follows that x is in the $\bar{G}$-class $A_2^2 A_1$ if $p = 3$ and $D_4(a_1)$ if $p \geqslant 5$. Therefore $|x^G| > \frac{1}{6} q^{54}$ and there are fewer than $2q^{18}$ such elements in H, so the contribution to α is less than q^{-15}. We conclude that

$$\alpha < q^{-10} + q^{-14} + q^{-15}.$$

To complete the proof, it remains to estimate β. Set $\bar{D} = C_{\bar{G}}(x)$ and let us first assume $\dim x^{\bar{G}} = 54$, in which case $\bar{D}^0 = A_2^3$, $r = 3$ and $|x^G| > \frac{1}{6} q^{54}$. Since $i_3(H) < 2q^{15}(q^3 + 1)$ by [57, Proposition 1.3], it follows that the contribution to β from these elements is less than $2q^{-14}$. Similarly, if $\dim x^{\bar{G}} \geqslant 56$ then $|x^G| > \frac{1}{2}(q+1)^{-1} q^{57} = a$, $r \geqslant 5$ and the bound $|H_0| < q^{24}$ implies that the contribution to β is less than $2q^{-7}$.

For the remainder, we may assume that $\dim x^{\bar{G}} \leqslant 52$ and thus

$$\bar{D}^0 \in \{D_5 T_1, A_5 A_1, A_5 T_1, D_4 T_2, A_4 A_1 T_1, A_4 T_2\}.$$

Suppose $r = 2$. Now H has a unique conjugacy class of involutions and by considering (14) we calculate that $\dim C_V(x) = 38$ and thus $\bar{D}^0 = A_5 A_1$. Therefore, $|x^G| > \frac{1}{2} q^{40}$ and $|x^G \cap H| = i_2(H) = q^6(q^6 + \epsilon q^3 + 1)$, so the contribution to β from involutions is less than q^{-15}.

Now assume $r \geqslant 3$. If $x \in H \setminus H_0$ then $r = 3$ and x acts as a field automorphism on H_0, inducing a cyclic permutation on the three factors of $\bar{H}^0$. It follows that $\dim C_{W_1}(x) = 8$ and $\dim C_{W_2}(x) = \dim C_{W_2^*}(x) = 11$, so $\dim C_V(x) = 30$ and thus $\bar{D}^0 = D_4 T_2$. Therefore, $|x^G| > \frac{1}{6}(q+1)^{-2} q^{50}$ and there are fewer than $i_3(H) < 2q^{15}(q^3 + 1)$ such elements in H, so the contribution to β is less than q^{-5}. For the remainder, we may assume $r \geqslant 3$ and $x^G \cap H \subseteq H_0$. In particular, $x \in H_0$.

If x is a regular semisimple element of H_0 then $\dim C_{W_1}(x) = 6$ and by applying [60, Lemma 3.7] we deduce that

$$\dim C_{W_2}(x) = \dim C_{W_2^*}(x) \leqslant 9. \tag{15}$$

Therefore, $\dim C_V(x) \leqslant 24$ and thus $\dim x^{\bar{G}} \geqslant 54$, which means that the contribution from these elements has already been accounted for. Now assume x is non-regular, so r divides $q^3 - \epsilon$ and we may assume x lifts to an element of $\mathrm{GL}_3^\epsilon(q^3)$ with eigenvalues $1, 1, \lambda$ for some nontrivial r-th root of unity $\lambda \in \mathbb{F}$. In

particular, note that $r \leqslant q^2 + q + 1$. Now $\dim C_{W_1}(x) = 12$ and one checks that (15) holds, which gives $\dim x^{\bar{G}} \geqslant 48$. Therefore, $|x^G| > \frac{1}{6}(q+1)^{-2}q^{50} = a$ and we calculate that there are fewer than

$$\sum_{r \in \pi}(r-1) \cdot \frac{|\mathrm{GL}_3^\epsilon(q^3)|}{(q^3 - \epsilon)|\mathrm{GL}_2^\epsilon(q^3)|} < \log(q^3 + 1) \cdot q(q+1) \cdot 2q^{12} = b$$

such elements in H, where π is the set of odd prime divisors of $q^3 - \epsilon$. It follows that the combined contribution to β from these elements is less than $a(b/a)^2 < q^{-10}$. Therefore,

$$\beta < 2q^{-14} + 2q^{-7} + q^{-15} + q^{-5} + q^{-10}$$

and by combining this with the above estimate for α, we deduce that

$$\widehat{Q}(G, H, 2) < q^{-10} + q^{-14} + q^{-15} + 2q^{-14} + 2q^{-7} + q^{-15} + q^{-5} + q^{-10} < q^{-4}$$

as required. ∎

We are now ready to prove Theorem 6.3. We partition the proof into a sequence of lemmas. We begin by handling the rank 1 groups $G \in \{{}^2B_2(q), {}^2G_2(q)\}$ where we can compute $P(G, s, 2)$ precisely for an appropriate element $s \in G$.

LEMMA 6.7: Let $G = {}^2B_2(q)$, where $q = 2^{2m+1}$ and $m \geqslant 1$, and let $s \in G$ be an element of order $q - \sqrt{2q} + 1$. Then

$$P(G, s, 2) = 1 - \frac{(q^2 - 4)(q - \sqrt{2q} + 1) + 4}{q^2(q-1)(q + \sqrt{2q} + 1)} > 1 - q^{-1}$$

and thus $\gamma_u(G) = 2$.

Proof. First we claim that $\mathcal{M}(G, s) = \{H\}$, where

$$H = N_G(\langle s \rangle) = K{:}L$$

and K, L are cyclic groups of order $q - \sqrt{2q} + 1$ and 4, respectively. By considering the orders of the maximal subgroups of G (see [69, Theorem 9]), we see that every subgroup in $\mathcal{M}(G, s)$ is a conjugate of H. Now, if r is a prime divisor of $|K|$, then H has a unique subgroup J of order r, which is contained in K. Therefore, if $g \in G$ and $J \leqslant H \cap H^g$, then $J = J^g$ and thus $g \in N_G(J) = H$. Therefore, $|H \cap H^g| \in \{1, 2, 4\}$ for all $g \in G \setminus H$ and thus $\mathcal{M}(G, s) = \{H\}$ as claimed. Moreover, it follows that the nontrivial, non-regular H-orbits on $\Omega = G/H$ have length $q - \sqrt{2q} + 1$ and $2(q - \sqrt{2q} + 1)$.

Let t be the number of regular orbits of H on Ω. Then Lemma 2.4 gives

$$(16) \qquad\qquad P(G, s, 2) = \frac{t|H|^2}{|G|}$$

and so it remains to determine t. By [69, Proposition 18], G has two (non-real) conjugacy classes of elements of order 4, both of size $|G|/2q$ (see [37, Lemma 3.2], for example). Similarly, H also has two classes of such elements, both of size $q - \sqrt{2q} + 1$, which are not fused in G. Also note that G and H both have unique conjugacy classes of involutions, of size $|G|/q^2$ and $q - \sqrt{2q} + 1$, respectively.

Write $H = G_\alpha$ for a point $\alpha \in \Omega$. Any element $x \in H$ of order 4 has

$$\frac{|x^G \cap H|}{|x^G|} \cdot |G : H| = \frac{1}{2}q$$

fixed points on $\Omega = G/H$, one of which is α. Clearly, x acts fixed-point-freely on the orbits of length $2(q - \sqrt{2q} + 1)$ and $4(q - \sqrt{2q} + 1)$. If $\Gamma = H/J$ with $J = C_4$, then x has

$$\frac{|x^H \cap J|}{|x^H|} \cdot |H : J| = 1$$

fixed point on Γ. This implies that H has precisely $q/2 - 1$ orbits of size $q - \sqrt{2q} + 1$. Similarly, any element $y \in H$ of order 2 has $\frac{1}{4}q^2$ fixed points on Ω, which are distributed so that y has 1 fixed point on each H-orbit of length $q - \sqrt{2q} + 1$ and 2 on those of length $2(q - \sqrt{2q} + 1)$. It follows that H has

$$\frac{\frac{1}{4}q^2 - 1 - (\frac{1}{2}q - 1)}{2} = \frac{1}{8}q(q - 2)$$

orbits of length $2(q - \sqrt{2q} + 1)$ and we conclude that

$$t = \frac{|G : H| - \frac{1}{2}(q - 2) \cdot (q - \sqrt{2q} + 1) - \frac{1}{8}q(q - 2) \cdot 2(q - \sqrt{2q} + 1) - 1}{|H|}.$$

The result follows. ∎

Remark 6.8: Define G and s as in Lemma 6.7. We claim that

$$P_2(G) = P(G, s, 2),$$

which shows that the general bound $P_2(G) > 1 - q^{-1}$ in Theorem 6.3 is essentially best possible. To see this, let x be any nontrivial element of G and observe that x is either contained in a Borel subgroup B of G, or it normalises a cyclic maximal torus of order $q + \epsilon\sqrt{2q} + 1$ with $\epsilon = \{+, -\}$ (this follows from

Lemma 6.4). If $x \in B$, then $P(G, x, 2) = 0$ since $b(G, G/B) > 2$. Therefore, we may assume x is a regular semisimple element and $H^\epsilon \in \mathcal{M}(G, x)$, where

$$H^\epsilon = N_G(\langle y \rangle) = C_{q+\epsilon\sqrt{2q}+1} : C_4$$

for some element $y \in G$ of order $q + \epsilon\sqrt{2q} + 1$. Note that

$$|C_G(x)| = |C_G(y)| = q + \epsilon\sqrt{2q} + 1 \quad \text{and} \quad \mathcal{M}(G, y) = \{H^\epsilon\},$$

so $P(G, x, 2) \leqslant P(G, y, 2)$. If $\epsilon = -$, then $P(G, y, 2) = P(G, s, 2)$. On the other hand, if $\epsilon = +$, then

$$P(G, y, 2) = \frac{r|H^+|^2}{|G|},$$

where r is the number of regular orbits of H^+ on G/H^+. By arguing as in the proof of Lemma 6.7, we deduce that

$$r = \frac{|G : H^+| - \frac{1}{2}(q-2) \cdot (q + \sqrt{2q} + 1) - \frac{1}{8}q(q-2) \cdot 2(q + \sqrt{2q} + 1) - 1}{|H^+|}$$

and one checks that $P(G, y, 2) < P(G, s, 2)$. This justifies the claim.

LEMMA 6.9: *Let $G = {}^2G_2(q)$, where $q = 3^{2m+1}$ and $m \geqslant 1$, and let $s \in G$ be an element of order $q - \sqrt{3q} + 1$. Then*

$$P(G, s, 2) = 1 - \frac{(q^3 + 2q^2 - 3q - 6)(q - \sqrt{3q} + 1) + 6}{q^3(q^2 - 1)(q + \sqrt{3q} + 1)} > 1 - q^{-2}$$

and thus $\gamma_u(G) = 2$.

Proof. This is very similar to the proof of Lemma 6.7. Firstly, we observe that $\mathcal{M}(G, s) = \{H\}$ and $H = K{:}L$, where K and L are cyclic groups of order $q + \sqrt{3q} + 1$ and 6, respectively. In view of (16), it suffices to compute t, the number of regular H-orbits on $\Omega = G/H$. By arguing as in the proof of Lemma 6.7, we see that $|H \cap H^g| \in \{1, 2, 3, 6\}$ for all $g \in G \backslash H$, so the nontrivial, non-regular H-orbits on Ω have length $c(q - \sqrt{3q} + 1)$ for $c \in \{1, 2, 3\}$.

In order to compute t, we need to consider the conjugacy classes of elements of order 2, 3 and 6 in both G and H (the conjugacy classes of G are determined in [71] and we refer the reader to [51, Section 3] for a convenient summary of the main facts we need). Both G and H have unique conjugacy classes of involutions, of size $q - \sqrt{3q} + 1$ and $|G|/q(q^2 - 1)$, respectively. Similarly, H has two (non-real) classes of elements of order 3, both of size $q - \sqrt{3q} + 1$, and the same is true for elements of order 6. Now G has three classes of elements

of order 3, two of size $|G|/2q^2$ and one of size $|G|/q^3$; the first two classes are non-real and they both meet H (see [38, Lemma 2.3(b)]). Similarly, G has two (non-real) classes of elements of order 6, both of size $|G|/2q$.

Let $x \in H$ be an element of order 6. In the usual manner, we calculate that x has $q/3$ fixed points on Ω. Moreover, if $\Gamma = H/J$ is an H-orbit of length $q - \sqrt{3q} + 1$, then x has a unique fixed point on Γ, whence H has $q/3 - 1$ orbits of length $q - \sqrt{3q} + 1$. Next suppose $y \in H$ has order 3 and note that y has $\frac{1}{3}q^2$ fixed points on Ω. Then y has a unique fixed point on each H-orbit of length $q - \sqrt{3q} + 1$, and two fixed points on the orbits of length $2(q - \sqrt{3q} + 1)$. This implies that H has

$$\frac{\frac{1}{3}q^2 - (\frac{1}{3}q - 1) - 1}{2} = \frac{1}{6}q(q - 1)$$

orbits of length $2(q - \sqrt{3q} + 1)$. Finally, let $z \in H$ be an involution. First we calculate that z has $q(q^2 - 1)/6$ fixed points on Ω. Now z has a unique fixed point on each H-orbit of length $q - \sqrt{3q} + 1$, and three fixed points on the H-orbits of length $3(q - \sqrt{3q} + 1)$. Therefore, H has

$$\frac{\frac{1}{6}q(q^2 - 1) - (\frac{1}{3}q - 1) - 1}{3} = \frac{1}{18}q(q^2 - 3)$$

orbits of length $3(q - \sqrt{3q} + 1)$.

Putting this together, we conclude that

$$t = \frac{|G : H| - (\frac{1}{3}q - 1)a - \frac{1}{3}q(q - 1)a - \frac{1}{6}q(q^2 - 3)a - 1}{|H|},$$

where $a = q - \sqrt{3q} + 1$. The result follows. ∎

Remark 6.10: Note that $^2G_2(3)' \cong L_2(8)$, so $\gamma_u(^2G_2(3)') = 3$ by Proposition 7.10.

To complete the proof of Theorem 6.3, it remains to handle the simple exceptional groups of rank at least two.

LEMMA 6.11: *Let $G = E_8(q)$ and let $s \in G$ be an element of order*

$$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1.$$

Then $P(G, s, 2) > 1 - q^{-30}$ and $\gamma_u(G) = 2$.

Proof. This follows from the proof of [27, Theorem 5.2]. ∎

LEMMA 6.12: *If $G = {}^2F_4(q)'$, then $\gamma_u(G) = 2$ if and only if $q \geqslant 8$. Moreover, if $q \geqslant 8$ and $s \in G$ has order $q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$, then $P(G, s, 2) > 1 - q^{-3}$.*

Proof. First assume $q = 2$. Here

$$G = \bigcup_{g \in G} H^g \cup \bigcup_{g \in G} K^g,$$

where $H = 2.[2^8].5.4$ and $K = \mathrm{L}_3(3).2$ (see [62], for example), and it is easy to check that

$$b(G, G/H) = b(G, G/K) = 3.$$

Therefore $\gamma_u(G) \geqslant 3$. In fact, by carrying out a random search in MAGMA (see [28, Section 1.2.4]) we can demonstrate that $\gamma_u(G) = 3$ (witnessed by the class 16A in the notation of the ATLAS [33]).

Now assume $q \geqslant 8$ and let $s \in G$ be an element of order

$$\ell = q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1.$$

By [72, Section 4(c)], we have $\mathcal{M}(G, s) = \{H\}$ with $H = C_\ell{:}C_{12}$. Since

$$|x^G| > \frac{1}{2}q^{11}$$

for all $1 \neq x \in G$ (see [65]), by applying Lemma 2.6 we deduce that

$$\widehat{Q}(G, s, 2) < \frac{1}{2}q^{11}(2q^{-11} \cdot |H|)^2 < q^{-3}$$

and the result follows. ∎

LEMMA 6.13: *Let $G = {}^3D_4(q)$ and let $s \in G$ be an element of order $q^4 - q^2 + 1$. Then $P(G, s, 2) > 1 - q^{-4}$ and $\gamma_u(G) = 2$.*

Proof. By [72, Section 4(e)], we have $\mathcal{M}(G, s) = \{H\}$ with $H = C_{q^4-q^2+1}{:}C_4$. Let $x \in H$ be an element of prime order r. We claim that $|x^G| > q^{16}$. If x is semisimple, then $|x^G|$ can be read off from [34, Proposition 2.2] and the desired bound follows. Now assume $r = p = 2$. From the proof of [31, Lemma 4.6], we deduce that H contains a unique class of involutions and they belong to the A_1^3 class of G (in the notation of [66]). This gives $|x^G| > q^{16}$ as required and by applying Lemma 2.6 we conclude that

$$\widehat{Q}(G, s, 2) < q^{16}(q^{-16} \cdot |H|)^2 < q^{-4}$$

for all $q \geqslant 2$. The result follows. ∎

LEMMA 6.14: *Let $G = E_7(q)$ and let $s \in G$ be an element of order*

$$\frac{(q^3 - 1)(q^4 - q^2 + 1)}{(2, q - 1)}.$$

Then $P(G, s, 2) > 1 - q^{-2}$ and $\gamma_u(G) = 2$.

Proof. In view of Lemma 6.5, it suffices to show that $\mathcal{M}(G, s) = \{H\}$ with

$$H = (\mathrm{L}_2(q^3) \times {}^3 D_4(q)).3.$$

Set $T = \langle s \rangle$ and $N = N_G(T)$. By the main theorem of [58], N is not maximal in G, so $N < H < G$ for some maximal rank subgroup H. By considering the order of s, it is clear that H is not a maximal parabolic subgroup of G. Moreover, further inspection of [58, Tables 5.1 and 5.2] shows that $H = (\mathrm{L}_2(q^3) \times {}^3 D_4(q)).3$ is the only option. Now G has a unique conjugacy class of maximal subgroups of this form and we will write n for the number of G-conjugates of H containing s. We need to show that $n = 1$. Note that $C_G(s) = C_H(s)$, so

$$n = \frac{|s^G \cap H|}{|s^G|} \cdot \frac{|G|}{|H|} \geqslant \frac{|s^H|}{|s^G|} \cdot \frac{|G|}{|H|} = 1$$

and thus $n = 1$ if and only if $s^G \cap H = s^H$.

Suppose $t \in H$ is G-conjugate to s, say $s = t^g$ for some $g \in G$. We need to show that s and t are H-conjugate. From the structure of H, it is easy to determine the H-classes of maximal tori of H; we see that there is a unique class of maximal tori of order $|s|$, so $T = \langle s \rangle$ and $\langle t \rangle$ are H-conjugate. Therefore, by replacing t by an appropriate H-conjugate, if necessary, we may assume that $\langle s \rangle = \langle t \rangle$. But then g normalises T and we have $N_G(T) < H$, so s and t are indeed H-conjugate and we conclude that $n = 1$ as required. ∎

LEMMA 6.15: *Let $G = E_6^\epsilon(q)$ and let $s \in G$ be an element of order*

$$(q^6 + \epsilon q^3 + 1)/(3, q - \epsilon).$$

Then $P(G, s, 2) > 1 - q^{-4}$ and $\gamma_u(G) = 2$.

Proof. By [72, Section 4(g,h)] and [45, Proposition 6.2] we have $\mathcal{M}(G, s) = \{H\}$ with $H = \mathrm{L}_3^\epsilon(q^3).3$. Now apply Lemma 6.6. ∎

Finally, we prove that $\gamma_u(G) \geqslant 3$ for the remaining two families of exceptional groups.

LEMMA 6.16: *If $G = G_2(q)'$, then $\gamma_u(G) \geqslant 3$.*

Proof. If $q = 2$, then $G \cong U_3(3)$ and with the aid of MAGMA it is easy to check that $\gamma_u(G) = 3$. For the remainder, we may assume $q \geqslant 3$.

As in Lemma 6.4, let $\mathcal{P}$ be the union of the parabolic subgroups of G. In addition, let $\mathcal{H}^\epsilon$ be the union of the maximal rank subgroups of G of the form $\mathrm{SL}_3^\epsilon(q){:}2$ for $\epsilon = \pm$. We claim that

$$G = \mathcal{P} \cup \mathcal{H}^+ \cup \mathcal{H}^-.$$

Notice that this implies that every element in G is contained in a maximal subgroup H with $b(G, G/H) \geqslant 3$, so Lemma 2.3 gives $\gamma_u(G) \geqslant 3$ as required. (In fact, if $q \geqslant 4$ is even, then a theorem of Bubboloni et al. [16] implies that $G = \mathcal{H}^+ \cup \mathcal{H}^-$.)

By Lemma 6.4, it suffices to show that every maximal torus of G is either contained in a Levi factor of a maximal parabolic subgroup, or in a maximal subgroup of the form $\mathrm{SL}_3^\epsilon(q){:}2$. There are six conjugacy classes of maximal tori in G (corresponding to the six conjugacy classes in the Weyl group of G, which is isomorphic to D_{12}):

$$C_{q-\epsilon}^2, \ C_{q^2-\epsilon q+1}, \ C_{q^2-1} \text{ (two classes)}.$$

There are two classes of maximal parabolic subgroups, both with Levi factor $\mathrm{GL}_2(q)$, so the maximal tori C_{q-1}^2 and C_{q^2-1} (both classes) are contained in Levi factors. In addition, $\mathrm{SU}_3(q)$ contains C_{q+1}^2 and C_{q^2-q+1}, and $\mathrm{SL}_3(q)$ contains C_{q^2+q+1}. The result follows. ∎

LEMMA 6.17: *If $G = F_4(q)$, then $\gamma_u(G) \geqslant 3$.*

Proof. This is similar to the proof of the previous lemma. Define $\mathcal{P}$ as before and let $\mathcal{H}$ and $\mathcal{K}$ be the union of the maximal rank subgroups of the form $B_4(q)$ and ${}^3D_4(q)$, respectively. It suffices to show that

$$G = \mathcal{P} \cup \mathcal{H} \cup \mathcal{K}.$$

The Weyl group of G has 25 conjugacy classes, so there are 25 classes of maximal tori. Similarly, $B_4(q)$ has 20 classes of maximal tori and by studying the embedding of these tori in G, we find that all but 7 classes of maximal tori of G have representatives contained in a $B_4(q)$ subgroup (see [55, pp. 95–96]). The exceptions are

$$C_{(q^3-\epsilon)(q+\epsilon)}, \ C_{q^3-\epsilon} \times C_{q-\epsilon}, \ C_{q^2+\epsilon q+1}^2, \ C_{q^4-q^2+1}.$$

However, these are precisely the maximal tori of $^3D_4(q)$, so $\mathcal{H} \cup \mathcal{K}$ contains every maximal torus in G and the result follows. (Note that if $q = 3^f$ then $G = \mathcal{H} \cup \mathcal{K}$ by [16].)   ∎

This completes the proof of Theorem 6.3. In particular, the proof of Theorem 4 is complete.

7. Two-dimensional linear groups

In this section we prove Theorem 5. Set $G = \mathrm{L}_2(q)$ with $q \geqslant 4$.

7.1. SPREAD. We start by studying the spread and uniform spread of G. Define

$$
f(q) = \begin{cases} q - 1 & \text{if } q \equiv 1 \,(\mathrm{mod}\ 4), \\ q - 4 & \text{if } q \equiv 3 \,(\mathrm{mod}\ 4), \\ q - 2 & \text{if } q \text{ is even.} \end{cases}
$$

LEMMA 7.1: Let $G = \mathrm{L}_2(q)$ with $q \geqslant 4$. Assume $q \geqslant 11$ if q is odd. Then $u(G) \geqslant f(q)$.

Proof. First assume q is odd and let $s \in G$ be an element of order $(q+1)/2$, so $\mathcal{M}(G, s) = \{H\}$ with $H = D_{q+1}$. Let $x \in H$ be an element of prime order r. If $r = 2$ then $\mathrm{fpr}(x, G/H) = i_2(H)/i_2(G)$ since G has a unique class of involutions and we get

$$
\mathrm{fpr}(x, G/H) = \begin{cases} \frac{1}{q} & \text{if } q \equiv 1 \,(\mathrm{mod}\ 4), \\ \frac{q+3}{q(q-1)} & \text{if } q \equiv 3 \,(\mathrm{mod}\ 4). \end{cases}
$$

Similarly, if r is odd then $|x^G \cap H| = 2$, $|x^G| = q(q-1)$ and thus

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

We conclude that if $x \in G$ has prime order, then

$$
\mathrm{fpr}(x, G/H) < \begin{cases} \frac{1}{q-1} & \text{if } q \equiv 1 \,(\mathrm{mod}\ 4) \\ \frac{1}{q-4} & \text{if } q \equiv 3 \,(\mathrm{mod}\ 4) \end{cases}
$$

and the result follows by Corollary 2.2. A very similar argument applies when q is even, working with an element of order $q + 1$.   ∎

Remark 7.2: As noted in Remark 5, the spread of $G = \mathrm{L}_2(q)$ is studied by Brenner and Wiegold in [10] and the bound $s(G) \geqslant f(q)$ is established in [10, Theorem 4.02]. In fact, this result states that $s(G) = f(q)$ for all $q \geqslant 11$, but we will show below that this is false when $q \equiv 3 \pmod 4$.

Fix subgroups A and B of G, where $A = D_{e(q+1)}$, B is a Borel subgroup and $e = 2$ if q is even, otherwise $e = 1$. It will be useful to record that

$$(17) \qquad\qquad G = \bigcup_{g \in G} A^g \cup \bigcup_{g \in G} B^g$$

(see [15, Corollary 4.3], for example).

THEOREM 7.3: *Let* $G = \mathrm{L}_2(q)$ *with* $q \geqslant 4$ *and* $q \not\equiv 3 \pmod 4$. *Assume that* $q \geqslant 13$ *if* q *is odd. Then* $s(G) = u(G) = f(q)$.

Proof. In view of Lemma 7.1, it suffices to show that $s(G) \leqslant f(q)$. First assume $q \equiv 1 \pmod 4$. Fix a Borel subgroup B of G and let x^B be the unique class of involutions in B. Note that $|x^B| = q$, say $x^B = \{x_1, \dots, x_q\}$. Let $A = C_G(x_1) = D_{q+1}$, which is a maximal subgroup of G. We claim that there is no element $y \in G$ such that $G = \langle x_i, y \rangle$ for all i. In view of (17), it suffices to show that $\bigcup_i \mathcal{M}(G, x_i)$ contains every G-conjugate of A and B.

First note that G has $q+1$ Borel subgroups, say $B, B_1, \dots, B_q$. By considering fixed points, one checks that each involution in G is contained in exactly two Borel subgroups. Moreover, we have

$$B \cap B_i = C_{(q-1)/2}$$

for all i, so $B \cap B_i$ contains a unique involution. Therefore, we may assume that $x_i \in B \cap B_i$ and thus $\bigcup_i \mathcal{M}(G, x_i)$ contains every conjugate of B.

Now let us consider the conjugates of A. First note that $(|A^g|, |B|) = 2$ and thus $|A^g \cap B| \leqslant 2$ for all $g \in G$ (in fact, equality holds for all $g \in G$). Now each x_i is contained in $(q-1)/2$ conjugates of A; if x_i and x_j are both contained in A^g, then $\langle x_i, x_j \rangle \leqslant A^g \cap B$ and thus $i = j$. This shows that $\bigcup_i \mathcal{M}(G, x_i)$ contains all $q(q-1)/2$ conjugates of A and the result follows.

To complete the proof, let us assume q is even. Let B be a Borel subgroup of G and fix maximal subgroups $A = D_{2(q+1)}$ and $C = D_{2(q-1)}$. Let

$$x^B = \{x_1, \dots, x_{q-1}\}$$

be the set of involutions in B. We claim that there is no $y \in G$ such that $G = \langle x_i, y \rangle$ for all i. To see this, let us first observe that each x_i is contained in a unique Borel subgroup (namely B itself), and also $q/2$ conjugates of both A and C. Moreover, $|A^g \cap B| = 2$ and $|C^g \cap B| \in \{2, q-1\}$ for all $g \in G$, so $\bigcup_i \mathcal{M}(G, x_i)$ contains $q(q-1)/2$ subgroups of the form $D_{2(q \pm 1)}$. In particular, $\bigcup_i \mathcal{M}(G, x_i)$ contains every conjugate of A and all but q conjugates of C. Let $H_1, \ldots, H_q$ be the conjugates of C that are not contained in $\bigcup_i \mathcal{M}(G, x_i)$

Seeking a contradiction, suppose there is an element $y \in G$ with $G = \langle x_i, y \rangle$ for all i. By considering (17), it follows that y must be contained in a Borel subgroup and $|y| > 1$ is a divisor of $q-1$. Without loss of generality, we may as well assume y has order $q-1$. In particular, y is contained in a unique conjugate of C, namely $N_G(\langle y \rangle)$. Since we are assuming $y \notin \bigcup_i \mathcal{M}(G, x_i)$, it follows that $y \in H_i$ for some i. As noted above, we have $|H_i \cap B| \in \{2, q-1\}$. If $H_i \cap B = \langle z \rangle$ for an involution z, then $z = x_j$ for some j and we get $H_i \in \mathcal{M}(G, x_j)$, which is a contradiction. Therefore, $|H_i \cap B| = q-1$ and thus $H_i \cap B = \langle y \rangle$ since H_i has a unique subgroup of order $q-1$. But this implies that $y \in B$, which is a contradiction since $B \in \mathcal{M}(G, x_1)$. The result follows. ∎

Now assume $q \equiv 3 \pmod 4$ and $q \geqslant 11$. By Lemma 7.1 we have

$$u(G) \geqslant f(q) = q - 4.$$

In the proof of Theorem 7.3, we worked with the set of involutions in a fixed Borel subgroup B of G. However, a different approach is needed when $q \equiv 3 \pmod 4$ since $|B| = q(q-1)/2$ is odd and it is more difficult to determine the exact spread of G. Indeed, this remains an open problem.

The next result gives a lower bound on $s(G)$ when q is a prime. In particular, we see that the difference $s(G) - u(G)$ for a non-abelian simple group G can be arbitrarily large.

PROPOSITION 7.4: *Let $G = \mathrm{L}_2(q)$, where $q \equiv 3 \pmod 4$ and $q \geqslant 11$ is a prime. Then $s(G) \geqslant (3q - 7)/2$ and $s(G) - u(G) = (q+1)/2$.*

Proof. Fix a maximal subgroup $A = D_{q+1}$ and let B be a Borel subgroup of G. Consider a subset $\{x_1, \ldots, x_m\}$ of nontrivial elements in G.

If $s \in G$ has order $(q+1)/2$, then s is contained in a unique maximal subgroup of G, namely $N_G(\langle s \rangle)$, which is a conjugate of A. Similarly, each element of order q is contained in a unique maximal subgroup (here we are using the

hypothesis that q is a prime), which is a conjugate of B. In view of (17), it follows that there is no element $y \in G$ such that $G = \langle x_i, y \rangle$ for all i if and only if $\bigcup_i \mathcal{M}(G, x_i)$ contains every conjugate of A and B. Since $(|A|, |B|) = 1$, we deduce that

$$(18) \qquad s(G) = |S| + |T| - 1,$$

where S and T are subsets of $G^{\#}$ of minimal size such that $\bigcup_{x \in S} \mathcal{M}(G, x)$ contains every conjugate of A and $\bigcup_{x \in T} \mathcal{M}(G, x)$ contains every conjugate of B. Note that there are $q(q-1)/2$ conjugates of A and $q+1$ conjugates of B.

First consider $|S|$. Let $x \in G$ be a nontrivial element. As observed in the proof of [10, Theorem 4.02], if $|x| = 2$ then x is contained in precisely $(q+3)/2$ conjugates of A. On the other hand, if $|x| > 2$ divides $q+1$, then x is contained in a unique conjugate of A. Therefore,

$$|S| \geqslant \frac{\frac{1}{2} q(q-1)}{\frac{1}{2}(q+3)} > q - 4$$

and thus $|S| \geqslant q - 3$.

Now let us consider $|T|$. As noted above, each $x \in G$ of order q is contained in a unique conjugate of B. Similarly, any nontrivial element of order dividing $(q-1)/2$ is contained in exactly two conjugates of B. This implies that $|T| \geqslant (q+1)/2$. We claim that $|T| = (q+1)/2$. To see this, let $B_1, \ldots, B_{q+1}$ be the Borel subgroups of G and note that $B_i \cap B_j = C_{(q-1)/2}$ and $B_i \cap B_j \cap B_k = 1$ for distinct i, j, k. In particular, if we write $B_i \cap B_j = \langle x_{i,j} \rangle$, then

$$T = \{x_{1,2}, x_{3,4}, \ldots, x_{q,q+1}\}$$

has the desired property. This justifies the claim and we conclude that

$$s(G) = |S| + |T| - 1 \geqslant (q-3) + \frac{1}{2}(q+1) - 1 = \frac{1}{2}(3q - 7)$$

as required.

Finally, let us consider $u(G)$. Fix a conjugacy class x^G with $x \neq 1$ and note that x is contained in a conjugate of A or B (see (17)). If x is contained in a conjugate of A, then there is no $g \in G$ such that $G = \langle s, x^g \rangle$ for all $s \in S$. Similarly, if x is in a conjugate of B, then there is no $g \in G$ such that $G = \langle t, x^g \rangle$ for all $t \in T$. Therefore,

$$u(G) = \max\{|S|, |T|\} - 1 = |S| - 1$$

and thus $s(G) - u(G) = |T| = (q+1)/2$. ∎

Remark 7.5: Let $G = \mathrm{L}_2(q)$, where $q \geqslant 11$ is a prime with $q \equiv 3 \pmod 4$. As noted in the proof of the previous proposition, in order to compute $s(G)$ we need to determine $|S|$ in (18). For $q = 11$, we can use MAGMA to show that $|S| = 9$, which gives $s(G) = 9 + 6 - 1 = 14$ and $u(G) = 8$.

Remark 7.6: The case $G = \mathrm{L}_2(7)$ requires special attention. In [10, Section 4], it is observed that $s(G) \geqslant 3$. Using MAGMA, we can identify 6 elements in G to show that $s(G) < 6$. For instance, if we take

$$G = \langle (3,6,7)(4,5,8), (1,8,2)(4,5,6) \rangle < S_8$$

then

$$\mathcal{A} = \{(2,3,8)(4,5,7), (1,8,5)(2,7,6), (2,3,4)(6,8,7),$$
$$(2,7,8)(3,5,6), (1,6,4)(3,5,7), (1,5,2)(3,8,4)\}$$

has the desired property (that is, there is no $y \in G$ such that $G = \langle x, y \rangle$ for all $x \in \mathcal{A}$). In addition, an exhaustive search shows that $s(G) \geqslant 5$, whence $s(G) = 5$. Finally, one checks that $u(G) = 3$. For example, the class $(1,7,2,3,8,5,6)^G$ is a witness to the bound $u(G) \geqslant 3$.

The next result gives a lower bound on $s(\mathrm{L}_2(q))$ which is valid for all $q \geqslant 11$ with $q \equiv 3 \pmod 4$. In particular, this shows that the claim $s(\mathrm{L}_2(q)) = q - 4$ in [10, Theorem 4.0.2] is incorrect for all such q.

PROPOSITION 7.7: *Let $G = \mathrm{L}_2(q)$, where $q \equiv 3 \pmod 4$ and $q \geqslant 11$. Then*

$$s(G) \geqslant q - 3.$$

Proof. Define A and B as before (see (17)) and set $C = D_{q-1}$. Note that G contains $\frac{1}{2}q(q-1)$ conjugates of A. Let $\{x_1, \ldots, x_{q-3}\}$ be a set of nontrivial elements of G.

First observe that each $y \in G$ of order $(q+1)/2$ is contained in a unique maximal subgroup of G, namely $N_G(\langle y \rangle)$, which is a conjugate of A. In addition, each involution is contained in $\frac{1}{2}(q+3)$ conjugates of A, whereas every other nontrivial element of G is contained in at most one conjugate of A. This implies that if at least one x_i is not an involution, then $\bigcup_i \mathcal{M}(G, x_i)$ does not contain every conjugate of A and it follows that there exists an element $y \in G$ of order $(q+1)/2$ such that $G = \langle x_i, y \rangle$ for all i. Therefore, we may assume each x_i is an involution. We claim that there is an element $y \in G$ of order $(q-1)/2$

such that $G = \langle x_i, y \rangle$ for all i. In particular, this shows that $s(G) \geqslant q - 3$, as required.

To justify the claim, first observe that G contains $q(q+1)/2$ distinct conjugates of C. If $s \in G$ has order $(q-1)/2$, then $\mathcal{M}(G, y)$ comprises a unique conjugate of C (namely, $N_G(\langle s \rangle)$) and two conjugates of B. Now each involution in G is contained in $(q+1)/2$ conjugates of C and no conjugates of B (since $|B|$ is odd). In particular, $\bigcup_i \mathcal{M}(G, x_i)$ does not contain every conjugate of C. Moreover, if $N_G(\langle y \rangle)$ is such a conjugate of C, then $G = \langle x_i, y \rangle$ for all i and the result follows. ∎

To conclude this section, we briefly consider the spread and uniform spread of $G = \mathrm{PGL}_2(q)$, where $q \geqslant 5$ is odd.

If $q = 5$, then $G \cong S_5$ and thus $s(G) = 3$ and $u(G) = 2$ by Theorem 4.3. If $q = 7$, then a computation in MAGMA yields $s(G) \geqslant u(G) = 4$. Now assume that $q \geqslant 9$. In her PhD thesis [42], Garion states that $s(G) = q - 4$ (see [42, Proposition 6.2.4]), but her argument only establishes the bound $u(G) \geqslant q - 4$. Indeed, the problem of determining the exact values of $s(G)$ and $u(G)$ is still open.

Our main result is the following.

PROPOSITION 7.8: *Let* $G = \mathrm{PGL}_2(q)$ *with* $q \geqslant 9$ *odd. Then*

$$q - 4 \leqslant u(G) \leqslant s(G) \leqslant q - 1.$$

Proof. First we show that $u(G) \geqslant q - 4$. Let $s \in G$ be an element of order $q + 1$ and note that $\mathcal{M}(G, s) = \{H\}$ with

$$H = N_G(\langle s \rangle) = D_{2(q+1)}.$$

Fix an element $x \in H$ of prime order r.

Suppose $r = 2$. Now H has three classes of involutions (a central involution, plus two classes of size $(q+1)/2$) and G contains two classes (represented by the elements t_1 and t_1' in the notation of [44, Table 4.5.1]). We calculate that

$$\mathrm{fpr}(x, G/H) = \begin{cases} \dfrac{1}{q} & \text{if } x \text{ is conjugate to } t_1, \\[2mm] \dfrac{q+3}{q(q-1)} & \text{if } x \text{ is conjugate to } t_1'. \end{cases}$$

If $r > 2$, then r divides $(q+1)/2$, $|x^G| = q(q-1)$ and $|x^G \cap H| \leqslant r - 1 \leqslant (q-1)/2$, so $\mathrm{fpr}(x, G/H) < 1/2q$. Therefore,

$$\mathrm{fpr}(x, G/H) < \frac{1}{q - 4}$$

for all $x \in G$ of prime order, whence $u(G) \geqslant q - 4$ by Corollary 2.2.

Finally, let us turn to the upper bound on $s(G)$; here we essentially repeat the argument in the proof of Theorem 7.3 with $q \equiv 1 \pmod 4$. Fix a maximal subgroup $A = D_{2(q+1)}$ and let B be a Borel subgroup of G. Note that G contains $q+1$ Borel subgroups, say $B, B_1, \ldots, B_q$. Let $\{x_1, \ldots, x_q\}$ be the unique class of involutions in B and set $\mathcal{M} = \bigcup_i \mathcal{M}(G, x_i)$. It suffices to show that $\mathcal{M}$ contains every conjugate of A and B.

Since $B \cap B_i = C_{q-1}$ contains a unique involution, we may assume that $x_i \in B_i$ for all i and thus $\mathcal{M}$ contains every Borel subgroup. Now each x_i is contained in $(q-1)/2$ conjugates of A, and there are $q(q-1)/2$ conjugates of A in total. We have $|A^g \cap B| = 2$ for all $g \in G$, so no two of the x_i are contained in the same conjugate of A. Therefore, $\mathcal{M}$ contains every conjugate of A and the result follows. ■

7.2. UNIFORM DOMINATION. By [27, Proposition 6.4], we have $\gamma_u(\mathrm{L}_2(q)) \leqslant 4$, with equality if and only if $q = 9$. Our first aim is to determine the exact value of $\gamma_u(\mathrm{L}_2(q))$ for all q. We begin by recording a preliminary lemma.

LEMMA 7.9: *Let $G = \mathrm{L}_2(q)$ where $q \geqslant 11$ is odd and consider the action of G on the set of cosets of $H = D_{q+1}$. The nontrivial subdegrees are as follows:*

(i) *$q \equiv 1 \pmod 4$: $(q+1)/2$ and $q+1$, with multiplicities $(q-3)/2$ and $(q-1)/4$, respectively.*

(ii) *$q \equiv 3 \pmod 4$: $(q+1)/4$, $(q+1)/2$ and $q+1$, with multiplicities 2, $(q-3)/2$ and $(q-3)/4$, respectively.*

In particular, $b(G, G/H) = 2$.

Proof. First observe that
$$H \cap H^g \leqslant C_2 \times C_2$$
for all $g \in G \setminus H$ (see [64, Lemma 2(b)], for example). Suppose $q \equiv 1 \pmod 4$, so $|H \cap H^g| \in \{1, 2\}$ for all $g \in G \setminus H$. If $y \in H$ has order 2 then $|y^G \cap H| = (q+1)/2$ and $|y^G| = q(q+1)/2$, so y has $(q-1)/2$ fixed points on $\Omega = G/H$. Moreover, each H-orbit of length $(q+1)/2$ contains a unique fixed point of y, so H has $(q-3)/2$ such orbits in total and we deduce that H has
$$\frac{\frac{1}{2}q(q-1) - \frac{1}{4}(q+1)(q-3) - 1}{q+1} = \frac{1}{4}(q-1)$$
regular orbits.

Now assume $q \equiv 3 \pmod 4$, so $H = C_G(x)$ for an involution $x \in G$. For $g \in G \setminus H$ we observe that $H \cap H^g = \langle x, x^g \rangle = C_2 \times C_2$ if and only if $[x, x^g] = 1$. Similarly, $H \cap H^g = 1$ if and only if there is no involution in G that commutes with both x and x^g. Now x commutes with $(q + 1)/2$ involutions (other than x itself) and thus H has

$$\frac{\frac{1}{2}(q + 1)}{\frac{1}{4}(q + 1)} = 2$$

orbits of length $(q + 1)/4$. By [3, Theorem 1.1(ii)], there are precisely

$$(q + 1)(q - 3)/4$$

elements x^g for which there is no involution commuting with both x and x^g. This implies that H has

$$\frac{\frac{1}{4}(q + 1)(q - 3)}{q + 1} = \frac{1}{4}(q - 3)$$

regular orbits. Finally, we deduce that H has

$$\frac{\frac{1}{2}q(q - 1) - \frac{1}{2}(q + 1) - \frac{1}{4}(q + 1)(q - 3) - 1}{\frac{1}{2}(q + 1)} = \frac{1}{2}(q - 3)$$

orbits of length $(q + 1)/2$. The result follows. ∎

PROPOSITION 7.10: *Let* $G = \mathrm{L}_2(q)$ *with* $q \geqslant 4$. *Then*

$$\gamma_u(G) = \begin{cases} 4 & \text{if } q = 9, \\ 3 & \text{if } q \in \{5, 7\} \text{ or } q \text{ is even,} \\ 2 & \text{if } q \geqslant 11 \text{ is odd.} \end{cases}$$

Proof. The cases with $q \leqslant 9$ can be checked directly, so let us assume $q \geqslant 11$. Note that $\gamma_u(G) \in \{2, 3\}$ by [27, Proposition 6.4].

First assume that q is odd and let $s \in G$ be an element of order $(q + 1)/2$. As noted in the proof of [27, Proposition 6.4], we have $\mathcal{M}(G, s) = \{H\}$ with $H = D_{q+1}$, and thus

$$\gamma_u(G) \leqslant b(G, G/H) = 2,$$

by Lemma 7.9.

Now assume $q \geqslant 16$ is even. We claim that each $g \in G$ is contained in a maximal subgroup H of G with $b(G, G/H) \geqslant 3$, which implies that $\gamma_u(G) \geqslant 3$ (and hence equality holds by [27, Proposition 6.4]). To see this, we consider the action of g on the natural module for G. If g acts reducibly, then g is

contained in the stabiliser of a 1-space (that is, a Borel subgroup of G) and the claim follows. On the other hand, if g acts irreducibly then it is contained in a maximal dihedral subgroup $H = D_{2(q+1)}$ and the subdegrees for the action of G on G/H are presented in [39, Table 2]. We see that there are no regular suborbits and thus $b(G, G/H) \geqslant 3$. This justifies the claim and the proof of the proposition is complete. ∎

The next result completes the proof of Theorem 5.

PROPOSITION 7.11: *Let* $G = \mathrm{L}_2(q)$ *with* $q \geqslant 11$ *odd. Then* $P_2(G) = g(q)$, *where*

$$g(q) = \begin{cases} \frac{1}{2}(1 + \frac{1}{q}) & \text{if } q \equiv 1 \ (\mathrm{mod}\ 4), \\ \frac{1}{2}(1 - \frac{q+3}{q(q-1)}) & \text{if } q \equiv 3 \ (\mathrm{mod}\ 4). \end{cases}$$

In particular, $P_2(G) \geqslant \frac{24}{55}$, *with equality if and only if* $q = 11$.

Proof. Let $s \in G$ be an element of order $(q + 1)/2$. Then, as noted above, $\mathcal{M}(G, s) = \{H\}$ with $H = N_G(\langle s \rangle) = D_{q+1}$, whence

$$P(G, s, 2) = \frac{r|H|^2}{|G|},$$

where r is the number of regular orbits of H on G/H (see Lemma 2.4). By applying Lemma 7.9, we deduce that $P(G, s, 2) = g(q)$ and thus $P_2(G) \geqslant g(q)$.

To complete the proof, we need to show that

$$P(G, t, 2) \leqslant P(G, s, 2)$$

for all $t \in G^{\#}$. If t is contained in a Borel subgroup B, then $P(G, t, 2) = 0$ since $b(G, G/B) \geqslant 3$. Therefore, by replacing t by a suitable conjugate, if necessary, we may assume that $t = s^m \in H$ for some positive integer m. Clearly, $P(G, t, 2) = 0$ if $|t| = 2$, so assume $|t| > 2$. Then the map $s^g \mapsto t^g$ is a bijection from s^G to t^G and we observe that if $\{t^{g_1}, t^{g_2}\}$ is a TDS then $\{s^{g_1}, s^{g_2}\}$ is a TDS. Therefore $P(G, t, 2) \leqslant P(G, s, 2)$ and the result follows. ∎

8. Classical groups

In the previous section, we studied the two-dimensional linear groups $\mathrm{L}_2(q)$ and we now turn our attention to finite simple classical groups in general. We will focus on the uniform domination number and our aim is to prove the results

stated in parts (ii) and (iii) of Theorem 6 (recall that part (i) is established in [27]).

The main result of this section is the following, which makes substantial progress towards a complete classification of the finite simple classical groups G with $\gamma_u(G) = 2$. As in the introduction, write

$$(19) \qquad \mathcal{C} = \{\mathrm{PSp}_{2r}(q) : r \geqslant 5 \text{ odd}, q \text{ odd}\} \cup \{\mathrm{P\Omega}_{2r}^{\pm}(q) : r \geqslant 4 \text{ even}\}.$$

THEOREM 8.1: *Let G be a finite simple classical group. Then $\gamma_u(G) = 2$ only if one of the following holds:*

   (i) *$G = \mathrm{L}_2(q)$ with $q \geqslant 11$ odd;*
   (ii) *$G = \mathrm{L}_n^\epsilon(q)$ with n odd and*

$$(n, q, \epsilon) \notin \{(3, 2, +), (3, 4, +), (3, 3, -), (3, 5, -)\};$$

   (iii) *$G \in \mathcal{C}$.*

Moreover, $\gamma_u(G) = 2$ in cases (i) and (ii). In addition, for the groups G in part (ii) we have

   (a) *$P_2(G) > \frac{1}{2}$, unless $G = \mathrm{U}_5(2)$ with $P_2(G) = \frac{605}{1728}$; and*
   (b) *$P_2(G) \to 1$ as $|G| \to \infty$.*

Remark 8.2: We have been unable to determine if $\gamma_u(G) = 2$ for the groups $G \in \mathcal{C}$ and we refer the reader to Remarks 8.15 and 8.16 for a brief discussion of the difficulties that arise in these special cases.

We present the proof of Theorem 8.1 in a sequence of lemmas. We begin by recording some useful preliminary results.

LEMMA 8.3: *Let G be a finite simple classical group and let $s \in G$ be an element that acts reducibly on the natural module V. Then one of the following holds:*

   (i) *s is contained in a proper subgroup H of G with $b(G, G/H) \geqslant 3$.*
   (ii) *$G = \mathrm{U}_{2m}(q)$, m is odd and s is a regular semisimple element that fixes an orthogonal decomposition $V = U \perp U^\perp$ into nondegenerate m-spaces and acts irreducibly on both summands.*
   (iii) *$G = \mathrm{P\Omega}_{2m}^+(q)$, m is even and s is a regular semisimple element that fixes an orthogonal decomposition $V = U \perp U^\perp$ into nondegenerate minus-type m-spaces and acts irreducibly on both summands.*

Proof. Let U be a proper nonzero subspace of V fixed by s of minimal possible dimension. In particular, note that s acts irreducibly on U. Since s also fixes the radical $U \cap U^\perp$, we deduce that U is either totally singular or nondegenerate (recall that if G is linear, then every subspace of V is totally singular). Let G_U be the stabiliser of U in G and set $H = N_G(G_U)$. Let n be the dimension of V.

If U is totally singular, then H is a maximal parabolic subgroup and it is easy to check that $|H|^2 > |G|$ (see [36], for example), whence

$$b(G, G/H) \geqslant \frac{\log |G|}{\log |G/H|} > 2$$

and (i) holds. Therefore, we may assume U is nondegenerate and s is not contained in a proper parabolic subgroup of G, so Lemma 6.4 implies that s is a regular semisimple element. If $G = \mathrm{PSp}_n(q)'$ then $|H|^2 > |G|$ and thus (i) holds. If $G = \Omega_n(q)$ then $\dim U = 1$ (since every element of G fixes a 1-space) and once again we see that $|H|^2 > |G|$.

We have now reduced to the case where U is a nondegenerate ℓ-space and G is a unitary or even-dimensional orthogonal group. Note that s fixes the orthogonal decomposition $V = U \perp U^\perp$ and $\ell \leqslant n/2$.

First assume $G = \mathrm{U}_n(q)$. Since s acts irreducibly on U, we see that ℓ is odd. If $n = 2\ell$, then (ii) holds, so we may assume that $\ell < n/2$. Let W be any nondegenerate ℓ-dimensional subspace of V. We claim that there exists a nontrivial element of G that fixes both U and W. In particular, $b(G, G/H) \geqslant 3$ and thus (i) holds. To see this, consider the sum $X = U + W$. Begin by assuming that X is degenerate and fix a nonzero vector v in the radical $X \cap X^\perp$. Then $X \subseteq \langle v \rangle^\perp$ and we can define a transvection $g \in G$ that acts trivially on the hyperplane $\langle v \rangle^\perp$. In particular, g fixes U and W. Now assume that X is nondegenerate and note that $V = X \perp X^\perp$. Suppose that $\dim X = n-1$. Then, since $\ell < n/2$, we must have $n = 2\ell+1$. The element s stabilises $U^\perp$, a subspace of dimension $\ell + 1$, which is even. Therefore, s stabilises a nonzero subspace of $U^\perp$ of dimension strictly less than ℓ, which is a contradiction. Therefore, $\dim X \leqslant n - 2$, and there is clearly an element $g \in G^{\#}$ that acts trivially on X, so g fixes both U and W. This implies that $b(G, G/H) \geqslant 3$ as required.

Finally, suppose $G = \mathrm{P}\Omega_n^\epsilon(q)$ with $n = 2m \geqslant 8$. Let $(\, ,)$ be the symmetric bilinear form on V corresponding to the quadratic form defining G. Since s acts irreducibly on U, we deduce that ℓ is even and U is minus-type. If $m = \ell$, then U and $U^\perp$ must both be minus-type spaces, so $\epsilon = +$ and case (iii) holds, so we may assume that $\ell < m$.

Let W be any nondegenerate ℓ-dimensional subspace of V of the same type as U. Again we claim that there exists a nontrivial element of G that fixes both U and W. Write $X = U + W$. If X is nondegenerate, then since $\dim X \leqslant 2m - 2$, there exists $g \in G^{\#}$ that acts trivially on X and consequently stabilises U and W.

Now assume X is degenerate. If there exist linearly independent vectors u, v in $X \cap X^{\perp}$, then $X \subseteq \langle u, v \rangle^{\perp}$ and the long root element defined as

$$x \mapsto x + (x, u)v - (x, v)u$$

(see [74, Section 3.7.3]) acts trivially on $\langle u, v \rangle^{\perp}$ and hence stabilises U and W. Now assume $X \cap X^{\perp} = \langle u \rangle$ is 1-dimensional and write $X = Y \perp \langle u \rangle$ where Y is nondegenerate. Then $V = Y \perp Y^{\perp}$ and $u \in Y^{\perp}$. Since $Y^{\perp}$ is nondegenerate, there exists $v \in Y^{\perp}$ such that $(u, v) = 1$, which implies that $\langle u, v \rangle \subseteq Y^{\perp}$ is nondegenerate. Therefore, $Z = Y \perp \langle u, v \rangle$ is a nondegenerate subspace of V containing X. Since $\ell < m$, it follows that $\dim Z \leqslant 2\ell + 1 < 2m$ and thus Z is a proper nondegenerate subspace of V containing X. If $\dim Z \leqslant 2m - 2$, then there exists $g \in G^{\#}$ that acts trivially on Z, so we may assume $\dim Z = 2m - 1$ (in which case, q must be odd). Now $\dim Y^{\perp} = 3$ and we can define an element $g \in G^{\#}$ so that it acts trivially on Y and as a regular unipotent element on $Y^{\perp}$. Moreover, we may choose g so that it fixes the singular vector $u \in Y^{\perp}$. Then g acts trivially on $X = Y \perp \langle u \rangle$ and thus g fixes U and W. We conclude that $b(G, G/H) \geqslant 3$ and (i) holds. This completes the proof. ∎

Remark 8.4: In the proof of Lemma 8.11 we will show that if G and s are as in part (ii) of Lemma 8.3, then the conclusion stated in part (i) still holds (with H the stabiliser of the given orthogonal decomposition of V).

COROLLARY 8.5: *Let G be one of the following finite simple classical groups:*

$$\mathrm{U}_{2m}(q) \ (m \ even), \ \Omega_n(q), \ \mathrm{P}\Omega_{2m}^{+}(q) \ (m \ odd).$$

Then $\gamma_u(G) \geqslant 3$.

Proof. Notice that every element $s \in G$ acts reducibly on the natural module for G and thus Lemma 8.3 implies that s is contained in a proper subgroup H with $b(G, G/H) \geqslant 3$. Now apply Lemma 2.3 to conclude. ∎

Next we recall the definition of a Singer cycle.

Definition 8.6: Let G be a finite simple classical group over $\mathbb{F}_q$ with natural module V. An element $s \in G$ is a **Singer cycle** if $\langle s \rangle$ is an irreducible subgroup (with respect to the action on V) of maximal possible order. In particular, s is a regular semisimple element and

$$|s| = \begin{cases} \frac{q^n-1}{(q-1)(n,q-1)} & \text{if } G = \mathrm{L}_n(q) \\ \frac{q^n+1}{(q+1)(n,q+1)} & \text{if } G = \mathrm{U}_n(q) \text{ and } n \text{ is odd} \\ \frac{q^{n/2}+1}{(2,q-1)} & \text{if } G = \mathrm{PSp}_n(q) \text{ or } \mathrm{P\Omega}_n^-(q) \end{cases}$$

where $n = \dim V$. Note that any element in G that acts irreducibly on V is equal to s^k for some Singer cycle $s \in G$ and integer k. Let us also note that none of the groups $\mathrm{U}_n(q)$ ($n \geqslant 4$ even), $\Omega_n(q)$ and $\mathrm{P\Omega}_n^+(q)$ contain elements that act irreducibly on V, so Singer cycles do not exist in these cases.

In the statement of the next result, we say that H is a **field extension subgroup** if it is contained in Aschbacher's $\mathcal{C}_3$ collection of maximal subgroups of G (see [53, Section 4.3]).

LEMMA 8.7: *Let G be a finite simple classical group over $\mathbb{F}_q$ with natural module V and let $s \in G$ be a Singer cycle. Let H be a field extension subgroup of G containing s. Then s is contained in a unique conjugate of H.*

Proof. First observe that $C_G(s) = C_H(s) = \langle s \rangle$, so it suffices to show that

$$s^G \cap H = s^H.$$

By considering the structure of H, we see that H contains a unique conjugacy class of maximal tori of order $|s|$ and we can complete the proof by repeating the argument in the proof of Lemma 6.14. ∎

LEMMA 8.8: *Suppose $G = \mathrm{PSp}_{2m}(q)'$, where $m \geqslant 2$ and either m or q is even. Then $\gamma_u(G) \geqslant 3$.*

Proof. First assume m is even and fix an element $s \in G^{\#}$. If s acts reducibly on the natural module for G, then Lemma 8.3 implies that $P(G, s, 2) = 0$. Now assume s acts irreducibly, in which case $s = x^k$ for some Singer cycle $x \in G$ and integer k. Now $\mathcal{M}(G, x)$ (and thus $\mathcal{M}(G, s)$) contains a field extension subgroup H of type $\mathrm{Sp}_m(q^2)$ and it is easy to check that $|H|^2 > |G|$ (note that $|H| = 2|\mathrm{PSp}_m(q^2)|$ by [53, Proposition 4.3.10]). Therefore $b(G, G/H) \geqslant 3$ and we conclude that $P(G, s, 2) = 0$, so $\gamma_u(G) \geqslant 3$.

Finally, if $m \geqslant 3$ is odd and q is even, then [27, Theorem 6.3(iii)] implies that $\gamma_u(G) \geqslant m$ and the result follows. ∎

LEMMA 8.9: *If $G = \mathrm{PSp}_6(q)$, then $\gamma_u(G) \geqslant 3$.*

Proof. In view of the previous lemma, we may assume q is odd and it suffices to show that $P(G, s, 2) = 0$ when $s \in G$ is a Singer cycle. Since $\mathcal{M}(G, s)$ contains a field extension subgroup H of type $\mathrm{Sp}_2(q^3)$, it is sufficient to show that $b(G, G/H) \geqslant 3$. Write $G = \widehat{G}/Z$, where $\widehat{G} = \mathrm{Sp}_6(q)$ and $Z = Z(\widehat{G})$. By applying [43, Lemmas 2.2 and 4.1], we see that there is an element $x \in \mathrm{GL}_6(q)$ such that $\widehat{G} \cap \widehat{G}^x = \mathrm{Sp}_2(q^3)$. In particular, if $y \in \widehat{G}$ then

$$\mathrm{Sp}_2(q^3) \cap \mathrm{Sp}_2(q^3)^y = \widehat{G} \cap \widehat{G}^x \cap \widehat{G}^{xy}$$

and thus [43, Lemma 5.7] implies that Z is a proper subgroup of $\mathrm{Sp}_2(q^3) \cap \mathrm{Sp}_2(q^3)^y$. Therefore, by passing to the quotient group $G = \widehat{G}/Z$, we deduce that the intersection of any two conjugates of H in G is nontrivial and thus $b(G, G/H) \geqslant 3$. ∎

LEMMA 8.10: *If $G = \mathrm{L}_n(q)$, where $n \geqslant 4$ is even, then $\gamma_u(G) \geqslant 3$.*

Proof. Set $n = 2m$ with $m \geqslant 2$. As in the proof of the previous lemma, it suffices to show that $P(G, s, 2) = 0$ for a Singer cycle $s \in G$. To see this, first observe that $\mathcal{M}(G, s)$ contains a field extension subgroup H of the form $\mathrm{GL}_m(q^2)$. According to [53, Proposition 4.3.6], we have

$$|H| = \frac{2(q+1)|\mathrm{PGL}_m(q^2)|}{(2m, q-1)}$$

and one checks that $|H|^2 > |G|$ when $q = 2$, so $b(G, G/H) \geqslant 3$ and the desired result follows.

Now assume $q > 2$. Set $\bar{G} = \mathrm{SL}_{2m}(K)$, where K is the algebraic closure of $\mathbb{F}_q$, and let σ be a Steinberg endomorphism of $\bar{G}$ such that $\bar{G}_\sigma = \mathrm{SL}_{2m}(q)$. Then there exists a maximal closed σ-stable subgroup $\bar{H}$ of $\bar{G}$ such that $\bar{H}_\sigma$ is of type $\mathrm{GL}_m(q^2)$. Here $\bar{H}$ is of type $\mathrm{GL}_m(K) \wr S_2$ and without loss of generality we may assume that $G = \bar{G}_\sigma/Z$ and $H = \bar{H}_\sigma/Z$ with $Z = Z(\bar{G}_\sigma)$. By [26, Corollary 3.15], we have

$$\dim(\bar{H} \cap \bar{H}^g) \geqslant m - 1$$

for all $g \in \bar{G}$ and thus [43, Proposition 8.1] implies that the intersection of any two conjugates of $\bar{H}_\sigma$ in $\bar{G}_\sigma$ is nontrivial. In fact, the proof of [43, Proposition

8.1] implies that any such intersection either contains a nontrivial unipotent element, or it has order at least $(q-1)^{m-1}$. Now

$$|Z| = (2m, q-1)$$

and by excluding the cases $(m, q) = (2, 3), (2, 5)$ we deduce that Z is a proper subgroup of every such intersection and it follows that the intersection of any two conjugates of H in G is nontrivial. It is straightforward to check directly that the same conclusion holds when $(m, q) = (2, 3)$ or $(2, 5)$. We conclude that $b(G, G/H) \geqslant 3$ and the proof of the lemma is complete. ∎

LEMMA 8.11: *If $G = U_n(q)$, where $n \geqslant 4$ is even, then $\gamma_u(G) \geqslant 3$.*

Proof. First recall that every element of G acts reducibly on the natural module. Therefore, by Lemma 8.3, we may assume that $n = 2m$ with $m \geqslant 3$ odd, and it suffices to show that $b(G, G/H) \geqslant 3$ for a maximal subgroup H of type $\mathrm{GU}_m(q) \wr S_2$. If $q = 2$ then $|H|^2 > |G|$ and the result follows, so we may assume $q > 2$. We can now repeat the argument in the proof of the previous lemma, working with the algebraic group $\bar{G} = \mathrm{SL}_{2m}(K)$ and an appropriate Steinberg endomorphism. We omit the details. ∎

To complete the proof of Theorem 6, we may assume that $G = \mathrm{L}_n^\epsilon(q)$ with n odd. We start by studying the special case $n = 3$.

LEMMA 8.12: *If $G = \mathrm{L}_3^\epsilon(q)$, then*

$$\gamma_u(G) = \begin{cases} 4 & \text{if } (\epsilon, q) = (+, 4), \\ 3 & \text{if } (\epsilon, q) \in \{(+, 2), (-, 3), (-, 5)\}, \\ 2 & \text{otherwise.} \end{cases}$$

Moreover, if $\gamma_u(G) = 2$ then

$$P_2(G) = \begin{cases} \frac{(q^2 + \epsilon q + 1)(q^2 - \epsilon q - 3)}{q^2(q^2 - 1)} & \text{if } q \equiv 0 \pmod 3 \\ \frac{3q^5 - 5q^3 + 3q + \epsilon 8}{3q^3(q^2 - 1)} & \text{if } q \equiv \epsilon \pmod 3 \\ \frac{(q^3 - \epsilon 3q^2 + q + \epsilon 2)(q^2 + \epsilon q + 1)}{q^3(q - \epsilon)^2} & \text{otherwise} \end{cases}$$

and thus $P_2(G) \geqslant \frac{13}{24}$, with equality if and only if $G = \mathrm{L}_3(3)$. In particular, $P_2(G) \to 1$ as $q \to \infty$.

Proof. The special cases with $(\epsilon, q) \in \{(+,2), (+,4), (-,3), (-,5)\}$ can be checked directly with the aid of MAGMA. For the remainder, we may assume G does not correspond to one of these cases.

Let $s \in G^{\#}$. If s is reducible then $P(G, s, 2) = 0$ by Lemma 8.3, so let us assume s is irreducible, in which case $s = x^k$ for some Singer cycle $x \in G$ and integer k. Since $C_G(s) = C_G(x) = \langle x \rangle$, it follows that $P(G, s, 2) \leqslant P(G, x, 2)$. Therefore, we may as well assume $s \in G$ is a Singer cycle, so $P_2(G) = P(G, s, 2)$. Set $a = (q^2 + \epsilon q + 1)/(3, q - \epsilon)$. By applying the main theorem of [4] and Lemma 8.7, we deduce that $\mathcal{M}(G, s) = \{H\}$, where $H = N_G(\langle s \rangle) = C_a{:}C_3$ is a field extension subgroup of type $\mathrm{GL}_1^{\epsilon}(q^3)$. By Lemma 2.4 we have $P_2(G) = r|H|^2/|G|$ and so it remains to determine the number r of regular orbits of H on G/H.

By arguing as in the proof of [24, Proposition 3.2], we see that

$$(20) \qquad r = \frac{|G : H| - a(b-1) - 1}{|H|} \quad \text{and} \quad b = \frac{2a|G : H|}{|y^G|}$$

for any element $y \in H$ of order 3. Since such an element y is regular, it follows that

$$|y^G| = \begin{cases} q(q^2 - 1)(q^3 - \epsilon) & \text{if } q \equiv 0 \ (\mathrm{mod}\ 3) \\ \frac{1}{3}q^3(q + \epsilon)(q^2 + \epsilon q + 1) & \text{if } q \equiv \epsilon \ (\mathrm{mod}\ 3) \\ q^3(q^3 - \epsilon) & \text{otherwise} \end{cases}$$

and one can check that this gives the stated expression for $P_2(G)$. ∎

Next we handle the case where $n \geqslant 5$ is a prime.

LEMMA 8.13: *If $G = \mathrm{L}_n^{\epsilon}(q)$ with $n \geqslant 5$ prime, then $\gamma_u(G) = 2$ and either $P_2(G) > \frac{1}{2}$, or $G = \mathrm{U}_5(2)$ and $P_2(G) = \frac{605}{1728}$. Moreover, $P_2(G) \to 1$ as $|G|$ tends to infinity.*

Proof. First assume $G = \mathrm{U}_5(2)$ and let $s \in G$ be a Singer cycle, so s has order 11 and $P(G, s, 2) = P_2(G)$. Then $\mathcal{M}(G, s) = \{H\}$ with $H = \mathrm{L}_2(11)$ and using MAGMA we calculate that H has 11 regular orbits on G/H. By applying Lemma 2.4, we deduce that $P_2(G) = \frac{605}{1728}$.

For the remainder, let us assume $G \neq \mathrm{U}_5(2)$. Fix a Singer cycle $s \in G$ and observe that $\mathcal{M}(G, s) = \{H\}$, where $H = N_G(\langle s \rangle) = C_a{:}C_n$ and

$$a = |s| = \frac{q^n - \epsilon}{(q - \epsilon)(n, q - \epsilon)}.$$

Let $y \in H$ be any element of order n and set

$$b = \frac{2a|G:H|}{|y^G|}.$$

Then (20) holds, where r denotes the number of regular orbits of H on G/H. Since y is a regular element of G, it follows that

$$|C_G(y)| \leqslant (q+1)^{n-1}$$

and thus $b \leqslant (1 - n^{-1})(q+1)^{n-1}$. Now,

$$P(G, s, 2) = \frac{r|H|^2}{|G|} \geqslant 1 - \frac{b|H|^2}{n|G|}$$

and we observe that

$$|H| \leqslant \left(\frac{q^n - 1}{q - 1}\right) n, \quad |G| > (2n)^{-1} q^{n^2 - 1}.$$

Therefore

$$P(G, s, 2) > 1 - 2n^2 \left(\frac{q^n - 1}{q - 1}\right)^2 (1 - n^{-1})(q+1)^{n-1} \cdot q^{1-n^2}$$

$$> 1 - 2n^2 q^{4n - 2 - n^2}$$

and the result follows. ∎

Finally, to complete the proof of Theorem 8.1 we address the general case with n composite.

LEMMA 8.14: *If $G = \mathrm{L}_n^\epsilon(q)$ with $n \geqslant 3$ composite and odd, then $\gamma_u(G) = 2$ and $P_2(G) > \frac{1}{2}$. Moreover, $P_2(G) \to 1$ as $|G|$ tends to infinity.*

Proof. Let $s \in G$ be a Singer cycle and note that $n \geqslant 9$. By [4] and Lemma 8.7, we have

$$\mathcal{M}(G, s) = \{H_k : k \in \pi(n)\},$$

where H_k is a field extension subgroup of type $\mathrm{GL}_{n/k}^\epsilon(q^k)$ and $\pi(n)$ is the set of prime divisors of n. More precisely, [53, Proposition 4.3.10] gives

$$(21) \qquad H_k = B_k.k \leqslant \left(\left(\frac{q^k - \epsilon}{q - \epsilon}\right).\mathrm{PGL}_{n/k}^\epsilon(q^k)\right).\langle\varphi\rangle,$$

where B_k is the image of $\mathrm{GL}_{n/k}^\epsilon(q^k)$ in $\mathrm{L}_n^\epsilon(q)$ and φ is a field automorphism of order k.

Let $\{x_1, \ldots, x_a\}$ be a set of representatives of the conjugacy classes in G of elements of prime order and set

$$\widehat{Q}(G, s, 2) := \sum_{i=1}^{a} |x_i^G| \left(\sum_{k \in \pi(n)} \mathrm{fpr}(x_i, G/H_k) \right)^2.$$

In order to prove the lemma, it suffices to show that $\widehat{Q}(G, s, 2) < \frac{1}{2}$ and $\widehat{Q}(G, s, 2) \to 0$ as $|G| \to \infty$. To do this, it will be convenient to observe that $|\pi(n)| < \log n$, so

$$\widehat{Q}(G, s, 2) < \alpha \log n$$

where

$$\alpha = \sum_{k \in \pi(n)} \left(\sum_{i=1}^{a} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H_k)^2 \right).$$

Let V be the natural module for G and let p be the characteristic of $\mathbb{F}_q$. Let $\bar{G} = \mathrm{PSL}_n(K)$, where K is the algebraic closure of $\mathbb{F}_q$, and let σ be a Steinberg endomorphism of $\bar{G}$ such that $(\bar{G}_\sigma)' = G$. For any element $x \in G$, write $x = \hat{x}Z$ with $\hat{x} \in \mathrm{GL}_n^\epsilon(q)$ and $Z = Z(\mathrm{GL}_n^\epsilon(q))$, and let $\nu(x)$ be the codimension of the largest eigenspace of $\hat{x}$ as an element of $\mathrm{GL}_n(K)$ (note that this is independent of the choice of $\hat{x}$). Write

$$\{x_1, \ldots, x_a\} = \{y_1, \ldots, y_b\} \cup \{z_1, \ldots, z_c\},$$

where $\nu(y_i) < n/2$ and $\nu(z_i) \geqslant n/2$ for all i.

It will be useful to write $\alpha = \alpha_1 + \alpha_2 + \alpha_3$, where the α_i are defined as follows. Firstly, if $3 \in \pi(n)$ then

$$\alpha_1 = \sum_{i=1}^{a} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H_3)^2,$$

otherwise $\alpha_1 = 0$. Similarly,

$$\alpha_2 = \sum_{k \in \pi(n), \, k \geqslant 5} \left(\sum_{i=1}^{b} |y_i^G| \cdot \mathrm{fpr}(y_i, G/H_k)^2 \right)$$

and

$$\alpha_3 = \sum_{k \in \pi(n), \, k \geqslant 5} \left(\sum_{i=1}^{c} |z_i^G| \cdot \mathrm{fpr}(z_i, G/H_k)^2 \right)$$

if $\pi(n) \neq \{3\}$, otherwise $\alpha_2 = \alpha_3 = 0$.

First consider α_3. Fix $k \in \pi(n)$ with $k \geqslant 5$ and set $H = H_k$. Let $x \in H$ be an element of prime order with $\nu(x) \geqslant n/2$. Then

$$|H| < 2kq^{\frac{1}{k}n^2-1} \leqslant 10q^{\frac{1}{5}n^2-1}, \quad |x^G| > \frac{1}{2}\Big(\frac{q}{q+1}\Big)^2 q^{\frac{1}{2}n^2-1}$$

(see [18, Corollary 3.38]) and thus

$$\sum_{i=1}^c |z_i^G| \cdot \mathrm{fpr}(z_i, G/H)^2 < 2\Big(\frac{q+1}{q}\Big)^2 q^{1-\frac{1}{2}n^2}(10q^{n^2/5-1})^2$$

$$= 200\Big(\frac{q+1}{q}\Big)^2 q^{-\frac{1}{10}n^2-1}.$$

It follows that $\alpha_3 \leqslant \delta_1$, where $\delta_1 = 0$ if $\pi(n) = \{3\}$, otherwise

$$\delta_1 = \Big(200\Big(\frac{q+1}{q}\Big)^2 q^{-\frac{1}{10}n^2-1}\Big)\log n.$$

Now let us turn to α_1 and α_2. Fix $k \in \pi(n)$ and set $H = H_k$ and $B = B_k$ as in (21). In addition, let us define $m = \frac{n}{k}$ and set $\beta = \alpha_1$ if $k = 3$, otherwise

$$\beta = \sum_{i=1}^b |y_i^G| \cdot \mathrm{fpr}(y_i, G/H)^2.$$

Our aim is to determine a bound $\beta < \gamma$ which is valid for all $k \geqslant 3$, in which case $\alpha_1 + \alpha_2 < \gamma \log n$.

Let $x \in H$ be an element of prime order r and assume $\nu(x) < n/2$ if $k \geqslant 5$. There are several cases to consider and we will closely follow the proof of [19, Proposition 3.1].

First assume $x^G \cap (H \setminus B)$ is non-empty. Here $r = k$ and $\nu(x) = n(1-k^{-1}) > n/2$ (see [19, (66)]), so we may assume $k = 3$. Now

$$|x^G| > \frac{1}{6}\Big(\frac{q}{q+1}\Big)^2 q^{\frac{2}{3}n^2}$$

and we calculate that $H \setminus B$ contains fewer than

$$2\Big(\frac{q^3-\epsilon}{q-\epsilon}\Big) \cdot \frac{|\mathrm{PGL}_{n/3}^\epsilon(q^3)|}{|\mathrm{PGL}_{n/3}^\epsilon(q)|} < 8q^{\frac{2}{9}n^2}$$

such elements. In addition, there are at most $4q^{\frac{2}{9}n^2}$ in B (there are none if n is indivisible by 9). By applying Lemma 2.6, it follows that the contribution to β from the elements with $x^G \cap (H \setminus B) \neq \emptyset$ is less than

$$6\Big(\frac{q+1}{q}\Big)^2 q^{-\frac{2}{3}n^2}(12q^{\frac{2}{9}n^2})^2 = 864\Big(\frac{q+1}{q}\Big)^2 q^{-\frac{2}{9}n^2} = \delta_2.$$

For the remainder, we may assume $x^G \cap H \subseteq B$.

Next suppose $r = p > 2$ and let λ be the partition of n corresponding to the Jordan form of x on V (this uniquely determines the $\bar{G}$-class of x). By considering the embedding of $\mathrm{GL}_{n/k}^{\epsilon}(q^k)$ in $\mathrm{GL}_n^{\epsilon}(q)$, it follows that $\lambda = (m^{ka_m}, \dots, 1^{ka_1})$ for some non-negative integers a_i (recall that this notation indicates that x has ka_i Jordan blocks of size i). Let $t \geqslant 1$ be the number of nonzero a_i in λ. Then as explained in the proof of [19, Proposition 3.1], we have

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^t q^{\dim x^G - 1}$$

and there are fewer than $2^t q^{\frac{1}{k} \dim x^G}$ elements in B that are $\bar{G}$-conjugate to x. Therefore, the contribution to β from unipotent elements when p is odd is less than

$$\sum 2^{2t+1}\left(\frac{q+1}{q}\right)^t q^{1+(\frac{2}{k}-1)\dim x^G} < \sum q^{2t+2+(\frac{2}{k}-1)\dim x^G},$$

where the sum is over a set of $\bar{G}$-class representatives x of order p with the appropriate Jordan form on V. We claim that

$$2t + 2 + \left(\frac{2}{k} - 1\right)\dim x^G \leqslant 12 - 2n.$$

If $t = 1$ then $\dim x^{\bar{G}} \geqslant \frac{1}{2}n^2$ and the desired bound holds. For $t \geqslant 2$ we have $n \geqslant \frac{1}{2}kt(t+1)$,

$$\dim x^{\bar{G}} \geqslant k^2\left(m(t^2 - t) - \frac{1}{4}t^4 + \frac{1}{6}t^3 + \frac{1}{4}t^2 - \frac{1}{6}t\right)$$

(see [18, Lemma 3.25]) and the claim quickly follows. Since there are fewer than $2^{n/k}$ partitions of n/k, we conclude that the entire contribution to β from unipotent elements when p is odd is less than

$$2^{n/3} \cdot q^{12-2n} < q^{5-n} = \delta_3.$$

Next we focus on the contribution from semisimple elements of odd order, so let us assume $r \neq p$ is odd. Let $i \geqslant 1$ be minimal such that r divides $q^i - 1$. Similarly, let $i_0 \geqslant 1$ be minimal such that r divides $q^{ki_0} - 1$ and note that

$$i_0 = \begin{cases} i/k & \text{if } k \text{ divides } i, \\ i & \text{otherwise.} \end{cases}$$

We define the integer $c = c(i, \epsilon)$ as in [18, Lemma 3.33], so

$$c = \begin{cases} 2i & \text{if } \epsilon = - \text{ and } i \text{ is odd,} \\ i/2 & \text{if } \epsilon = - \text{ and } i \equiv 2 \,(\text{mod } 4), \\ i & \text{otherwise.} \end{cases}$$

First assume $C_{\bar{G}}(x)$ is disconnected and $c = 1$. By [18, Lemma 3.34], it follows that r divides n and $\nu(x) = n(1 - r^{-1})$, so we may assume $k = 3$. In addition, the condition $x^G \cap H \subseteq B$ implies that $r \geqslant 5$, hence $n \geqslant 15$ and $q \geqslant 4$ (since $c = 1$). Now

$$|x^G| > \frac{1}{2r}\left(\frac{q}{q+1}\right)^{r-1} q^{n^2(1-\frac{1}{r})} \geqslant \frac{1}{10}\left(\frac{q}{q+1}\right)^4 q^{\frac{4}{5}n^2}$$

and $|B| < 2q^{n^2/3-1}$, so the contribution to β from these elements is less than

$$40\left(\frac{q+1}{q}\right)^4 q^{-\frac{2}{15}n^2-2}.$$

For the remainder of our analysis of semisimple elements of odd order, we may assume that either $C_{\bar{G}}(x)$ is connected or $c > 1$.

First assume that k does not divide i, so $i_0 = i$. As explained in [18, Section 3.4], the G-class of x is determined by a tuple $(a_1, \ldots, a_t)$ of non-negative integers (where $t = (r-1)/c$) and we have

$$\text{(22)} \qquad \dim x^{\bar{G}} = n^2 - (n-v)^2 - c\sum_{j=1}^{t} a_j^2$$

where

$$v = n - c\sum_{j=1}^{t} a_j.$$

In addition, if $c = 1$ we may assume that $v \geqslant a_j$ for all j. Since $i_0 = i$, it follows that each a_j is divisible by k, so $n \geqslant kdc$ where $d \geqslant 1$ is the number of nonzero a_j. As in the proof of [19, Proposition 3.1], we have

$$|x^G \cap H| < 2^d q^{\frac{1}{k}\dim x^{\bar{G}}}, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^d q^{\dim x^{\bar{G}}}$$

and it follows that the combined contribution to β from these semisimple elements is less than

$$\sum 2\left(\frac{q+1}{q}\right)^d q^{-\dim x^{\bar{G}}}(2^d q^{\frac{1}{k}\dim x^{\bar{G}}})^2 < \sum q^{3d+1-(1-\frac{2}{k})\dim x^{\bar{G}}},$$

where the sum is over a set of representatives of the relevant G-classes. Now one can check that

$$\dim x^{\bar{G}} \geqslant \begin{cases} 4nkd - 4k^2d^2 - 2dk^2 - 2k^2 & \text{if } c \geqslant 2 \\ 2nkd - k^2d^2 - dk^2 & \text{if } c = 1 \end{cases}$$

and by setting $k = 3$ and $d = 1$ we deduce that

$$3d + 1 - \left(1 - \frac{2}{k}\right)\dim x^{\bar{G}} \leqslant 12 - 2n.$$

Now assume k divides i, so $i_0 = i/k$. As before, the G-class of x is determined by a tuple $(a_1, \ldots, a_t)$ and we write d for the number of nonzero a_j, so $n \geqslant dc$ and

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^d q^{\dim x^{\bar{G}}}.$$

Note that in this case, the a_j need not be divisible by k, in general. Now, if $k = 3$ then the proof of [19, Proposition 3.1] gives

$$(23) \qquad |x^G \cap H| < 2^{3d}\left(\frac{q^3}{q^3 - 1}\right)^d q^{\frac{1}{3}\dim x^{\bar{G}}}$$

and we claim that the same bound holds for $k \geqslant 5$.

To see this, let $y \in x^G \cap H$ and write $\nu(y) = t$ and $\nu_0(y) = t_0$ with respect to the natural modules V and V_0 for G and $\mathrm{PGL}_{n/k}^\epsilon(q^k)$, respectively. Recall that we may assume $t < n/2$ since $k \geqslant 5$. Then $t_0 \leqslant t/k$ (see the proof of [61, Lemma 4.2]) and by appealing to the proof of [18, Proposition 3.36] we deduce that

$$|y^B| < 2\left(\frac{q^k}{q^k - 1}\right)^{kd} q^{kt_0(\frac{2n}{k} - t_0 - 1)} \leqslant 2\left(\frac{q^5}{q^5 - 1}\right)^{5d} q^{t(\frac{2n}{k} - \frac{t}{k} - 1)}$$

$$< 4\left(\frac{q^3}{q^3 - 1}\right)^d q^{t(\frac{2n}{k} - \frac{t}{k} - 1)}.$$

From [18, Proposition 3.40] we see that there are fewer than

$$\sum_{t_0=1}^{\lfloor t/k \rfloor} q^{kt_0} < 2q^t$$

distinct B-classes in $x^G \cap H$, whence

$$|x^G \cap H| < 8\left(\frac{q^3}{q^3 - 1}\right)^d q^{\frac{1}{k}t(2n-t)}.$$

Now $\dim x^{\bar{G}} \geqslant 2t(n-t)$ by [17, Proposition 2.9] and it is easy to check that

$$\frac{1}{5}t(2n-t) < \frac{2}{3}t(n-t).$$

This shows that (23) holds for all k.

It follows that the contribution to β from these semisimple elements is less than

$$\sum 2^{6d+1}\left(\frac{q+1}{q}\right)^d\left(\frac{q^3}{q^3-1}\right)^{2d}q^{-\frac{1}{3}\dim x^{\bar{G}}} < \sum q^{7d+1-\frac{1}{3}\dim x^{\bar{G}}},$$

where we sum over a set of G-class representatives. In view of (22), we calculate that

$$\dim x^{\bar{G}} \geqslant 2ndc - d^2c^2 - dc$$

and thus

$$7d + 1 - \frac{1}{3}\dim x^{\bar{G}} \leqslant 12 - 2n.$$

By combining the above estimates, noting that G has at most q^{n-1} semisimple conjugacy classes, we conclude that the entire contribution to β from semisimple elements $x \in G$ of odd order with $x^G \cap H \subseteq B$ is less than

$$q^{n-1} \cdot q^{12-2n} + 40\left(\frac{q+1}{q}\right)^4 q^{-\frac{2}{15}n^2-2}.$$

Notice that this is larger than 1 when $n = 9$, so this case requires special attention. Here $k = 3$, $i \in \{1, 2, 3, 6, \frac{9}{2}(3-\epsilon)\}$ and we can estimate the contribution to β by considering each possibility for i in turn. For example, suppose $\epsilon = +$ and $i = 6$, so $i_0 = 2$ and r divides $q^2 - q + 1$. Then

$$|x^G \cap H| \leqslant 3\left(\frac{|\mathrm{GL}_3(q^3)|}{|\mathrm{GL}_1(q^3)||\mathrm{GL}_1(q^6)|}\right) < 3q^{18}, \quad |x^G| = \frac{|\mathrm{GL}_9(q)|}{|\mathrm{GL}_3(q)||\mathrm{GL}_1(q^6)|} > \frac{1}{2}q^{66}$$

and there are fewer than $\frac{1}{6}q(q-1)$ such G-classes for a fixed value of r. Since $q^2 - q + 1$ has less than $\log(q^2 - q + 1)$ odd prime divisors, we deduce that the total contribution to β from semisimple elements with $i = 6$ is less than

$$\frac{1}{6}q(q-1)\log(q^2 - q + 1) \cdot 2q^{-66}(3q^{18})^2 < q^{-26}.$$

In a similar fashion, we can estimate the contribution for the other values of i. Indeed, one can check that if $n = 9$ then the total contribution to β from

semisimple elements of odd order is less than q^{-8} (this estimate is valid for $\epsilon = \pm$). Set

$$\delta_4 = \begin{cases} q^{11-n} + 40(\frac{q+1}{q})^4 q^{-\frac{2}{15}n^2 - 2} & \text{if } n \geqslant 15, \\ q^{-8} & \text{if } n = 9. \end{cases}$$

To complete the proof of the lemma, it remains to estimate the contribution to β from involutions. Let $x \in H$ be an involution and first assume $p = 2$. Here x has Jordan form $[J_2^{k\ell}, J_1^{n-2k\ell}]$ on V, for some $1 \leqslant \ell \leqslant \lfloor n/2k \rfloor$, and we get

$$(24) \qquad |x^G \cap H| < 2q^{2\ell(n-k\ell)}, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{2k\ell(n-k\ell)}.$$

Therefore, the contribution to β is less than

$$\sum_{\ell=1}^{\lfloor n/2k \rfloor} 8\left(\frac{q+1}{q}\right)q^{-2\ell(n-k\ell)} < \frac{n}{6} \cdot 8\left(\frac{q+1}{q}\right)q^{6-2n} < q^{2-n}.$$

Now assume $p \neq 2$. Here x has Jordan form $[-I_\ell, I_{n-\ell}]$ on V for some $1 \leqslant \ell \leqslant \lfloor n/2k \rfloor$ and we get the same bounds as in (24). In particular, the contribution to β is less than $q^{2-n} = \delta_5$.

By bringing together the above estimates, we deduce that

$$\beta < \delta_2 + \delta_3 + \delta_4 + \delta_5 = \gamma$$

and thus

$$\widehat{Q}(G, s, 2) < (\alpha_1 + \alpha_2 + \alpha_3) \log n < (\gamma \log n + \delta_1) \log n.$$

This implies that $\widehat{Q}(G, s, 2) < \frac{1}{2}$ for all possible values of n and q. Moreover, we deduce that $\widehat{Q}(G, s, 2) \to 0$ as n or q tends to infinity. This completes the proof of the lemma. ∎

This completes the proof of Theorem 6. We close this section by commenting on the classical groups arising in part (iii) of Theorem 8.1; these are the groups that comprise the collection $\mathcal{C}$ (see (19)).

Remark 8.15: Suppose $G = \mathrm{PSp}_{2m}(q)$, where mq is odd and $m \geqslant 5$. Let V be the natural module for G and fix an element $s \in G^{\#}$. If s acts reducibly on V, then Lemma 8.3 implies that s is contained in a proper subgroup H with $b(G, G/H) \geqslant 3$, so $P(G, s, 2) = 0$. Now assume s is irreducible, so s is a power of a Singer cycle $x \in G$. Clearly, if $g \in G$ then $\{s, s^g\}$ is a TDS only if $\{x, x^g\}$

is a TDS, so $\gamma_u(G) = 2$ if and only if $P(G, x, 2) > 0$. Therefore, we may as well assume that s is a Singer cycle.

By combining Lemma 8.7 with a theorem of Bereczky [4], we deduce that
$$\mathcal{M}(G, s) = \{H_t, K : t \in \pi(m)\},$$
where H_t is a field extension subgroup of type $\mathrm{Sp}_{2m/t}(q^t)$, K is a subgroup of type $\mathrm{GU}_m(q)$ and $\pi(m)$ is the set of prime divisors of m. The main theorem of [21] gives
$$b(G, G/H_t), b(G, G/K) \in \{2, 3, 4\},$$
but the precise base sizes in these cases have not been determined. One can check that $|K|^2 < |G|$ and $\widehat{Q}(G, K, 2) > 1$ (as defined in (10)), so our probabilistic methods do not yield $b(G, G/K) = 2$. In particular, we have $\widehat{Q}(G, s, 2) > 1$ and so a different approach is needed to determine whether or not $\gamma_u(G) = 2$. For $G = \mathrm{PSp}_{10}(3)$, which is the smallest group satisfying the conditions in part (iii) of the theorem, we can use MAGMA [9] to show that $b(G, G/K) = 2$. Moreover, we can find an element $g \in G$ by random search such that
$$H_5 \cap H_5^g = H_5 \cap K^g = K \cap K^g = K \cap H_5^g = 1,$$
which implies that $\{s, s^g\}$ is a total dominating set and thus $\gamma_u(\mathrm{PSp}_{10}(3)) = 2$ in this case. We have not been able to estimate $P_2(\mathrm{PSp}_{10}(3))$ and the general problem remains open.

Remark 8.16: Similar difficulties arise when $G = \mathrm{P\Omega}_{2m}^\epsilon(q)$ and $m \geqslant 4$ is even. First assume $\epsilon = -$. As before, we may as well assume that $s \in G$ is a Singer cycle, in which case
$$\mathcal{M}(G, s) = \{H_t : t \in \pi(m)\}$$
by [4], where H_t is a field extension subgroup of type $O_{2m/t}^-(q^t)$ and $\pi(m)$ is the set of prime divisors t of m with $2m/t \geqslant 4$. The main theorem of [21] gives $b(G, G/H_t) \leqslant 4$, but the exact base size is not known. In particular, we have $|H_2|^2 < |G|$ and $\widehat{Q}(G, H_2, 2) > 1$, so our probabilistic methods will not determine $b(G, G/H_2)$ precisely. For $m = 4$ we have $\gamma_u(G) = b(G, G/H_2)$ and we can use MAGMA when q is small. Indeed, if $m = 4$ then $\gamma_u(G) = 3$ if $q = 2$ and $\gamma_u(G) = 2$ if $q \in \{3, 5\}$. Moreover, if $q = 3$ we calculate that H_2 has exactly 10 regular orbits on G/H_2, whence
$$P_2(\mathrm{P\Omega}_8^-(3)) = \frac{2050}{7371}$$
by Lemma 2.4. A similar computation is out of reach when $q = 5$ since the index $|G : H_2|$ is too large.

Now assume $\epsilon = +$. Here every element of G acts reducibly on the natural module V, so Lemma 8.3 implies that $P(G, s, 2) = 0$, with the possible exception of the case where $s \in G$ is a regular semisimple element fixing an orthogonal decomposition $V = U \perp U^\perp$ into minus-type m-spaces, acting irreducibly on both summands. Clearly, in this case $\mathcal{M}(G, s)$ contains a maximal subgroup H of type $O_m^-(q) \wr S_2$. For $m = 4$, a computation with MAGMA shows that $b(G, G/H) = 3$ if $q = 2$ and $b(G, G/H) = 2$ if $q \in \{3, 5\}$, but the exact base size is not known in general (as before, [21] gives the bound $b(G, G/H) \leqslant 4$). In addition, if $(m, q) \neq (4, 2)$ then

$$|H|^2 < |G| \quad \text{and} \quad \widehat{Q}(G, H, 2) > 1,$$

so the probabilistic approach is inconclusive in this case. Finally, let us also observe that further work is needed to determine the complete set of maximal overgroups of s (since s is not a Singer cycle, we cannot appeal to [4]).

9. Proofs of Theorems 9 and 10

In this final section we prove Theorems 9 and 10.

Proof of Theorem 9. Let G be a finite simple group such that $\gamma_u(G) = 2$ and $G \notin \mathcal{C} \cup \mathcal{T}$. By applying Theorems 3, 4, 5 and 6, we immediately reduce to the case where G is a sporadic group (see Remark 5.10 for the precise value of $P_2(A_{13})$).

Let G be a sporadic group and recall that $G \notin \mathcal{T}$. First assume that $G \notin \{\mathrm{Fi}_{23}, \mathbb{B}, \mathbb{M}\}$. As explained in [28], we can use the GAP Character Table Library [11] to compute $\widehat{Q}(G, s, 2)$ precisely for any element $s \in G$. We obtain the following results, where we adopt the ATLAS [33] notation for conjugacy classes (we round up real numbers to 3 decimal places):

G	M_{23}	J_1	J_4	Ru	Ly	O'N	Fi'_{24}	Th
s	23A	15A	29A	29A	37A	31A	29A	27A
$\widehat{Q}(G, s, 2)$	0.030	0.364	0.001	0.168	0.001	0.337	0.001	0.060

In particular, we deduce that $P_2(G) > \frac{1}{2}$.

We will now consider the three remaining groups. First let $G = \mathrm{Fi}_{23}$ and $s \in G$. If s is not in the class 35A, then one can verify that there exists $H \in \mathcal{M}(G, s)$ such that $b(G, G/H) \geqslant 3$ and consequently $P(G, s, 2) = 0$ (the base size for every primitive action of a sporadic group is given in [30]). Now assume that s does belong to 35A. In this case $\mathcal{M}(G, s) = \{H\}$ with $H = S_{12}$. Therefore, $P_2(G) = P(G, s, 2)$, which Lemma 2.4 implies is equal to $r|H|^2/|G|$, where r is the number of regular orbits of H on G/H. A computation in GAP by Alexander Hulpke establishes $r = 1$, so

$$P_2(G) = P(G, s, 2) = \frac{|H|^2}{|G|} = \frac{7700}{137241}.$$

Now let $G = \mathbb{B}$ and let s be in 47A. Then $\mathcal{M}(G, s) = \{H\}$ where $H = 47{:}23$ (see [45, Table IV]). Since $|x^G| \geqslant 10^{10}$ for all prime order elements $x \in G$, we deduce that

$$P_2(G) \geqslant P(G, s, 2) \geqslant 1 - \frac{1104^2}{10^{10}} > 1 - 10^{-3}.$$

Finally, let $G = \mathbb{M}$ and let s be in 59A. Then $\mathcal{M}(G, s) = \{H\}$ where $H = \mathrm{L}_2(59)$ (see [45, Table IV]) and we proceed as in the previous case. Since $|H| = 102660$ and $|x^G| \geqslant 10^{19}$ for all prime order elements $x \in G$, we conclude that

$$P_2(G) \geqslant P(G, s, 2) \geqslant 1 - \frac{102660^2}{10^{19}} > 1 - 10^{-9}.$$

This completes the proof. ■

Remark 9.1: Let G be a sporadic simple group with $\gamma_u(G) = 2$ and $G \notin \mathcal{T}$. If there is an element $s \in G$ such that $\mathcal{M}(G, s) = \{H\}$ and $b(G, G/H) = 2$, then in some cases we can determine the probability $P_2(G)$ precisely.

For example, let $G = \mathrm{M}_{23}$ and $s \in G$. If $|s| \neq 23$, then s is contained in a maximal subgroup H with $b(G, G/H) \geqslant 3$. Now assume $|s| = 23$, in which case $\mathcal{M}(G, s) = \{H\}$ with $H = N_G(\langle s \rangle) = 23{:}11$ and $P_2(G) = P(G, s, 2)$. Using MAGMA, we calculate that H has 159 regular orbits on G/H, so Lemma 2.4 yields

$$P_2(G) = \frac{159|H|^2}{|G|} = \frac{13409}{13440} > 0.997.$$

Remark 9.2: In Remarks 8.15 and 8.16, we briefly discussed some of the special difficulties that arise when we try to determine if $\gamma_u(G) = 2$ for the classical

groups in $\mathcal{C}$. Here we discuss the groups in

$$\mathcal{T} = \{\mathrm{J}_3, \mathrm{He}, \mathrm{Co}_1, \mathrm{HN}\}.$$

For each $G \in \mathcal{T}$, there exists at least one class s^G such that $b(G, G/H) = 2$ for all $H \in \mathcal{M}(G, s)$. Indeed, the relevant classes are as follows:

J_3	3B, 8A, 9A, 9B, 9C, 12A, 19A, 19B
He	7C, 7D, 7E, 21A, 21B
Co_1	35A
HN	5C, 5D, 10D, 10E, 15B, 15C, 20D, 20E, 25A, 25B, 30B, 30C

However, $\widehat{Q}(G, s, 2) > 1$ in all cases, and we never have $\mathcal{M}(G, s) = \{H\}$ with $b(G, G/H) = 2$. Therefore, our methods are inconclusive and we have not been able to determine if $\gamma_u(G) = 2$ in these cases (in particular, we have been unable to apply computational methods to answer this question). However, we can verify the bound $\widehat{Q}(G, s, 3) < 1$ for a suitable element s, which implies that $\gamma_u(G) \in \{2, 3\}$ (see [27, Theorem 4.2]).

Finally, let us remark that if $G = \mathrm{Co}_1$ and s is in 35A, then

$$\mathcal{M}(G, s) = \{H, K, L_1, L_2\}$$

where $H = (A_5 \times J_2){:}2$, $K = (A_7 \times L_2(7)){:}2$ and $L_1 \cong L_2 = (A_6 \times U_3(3)){:}2$.

We now turn to the proof of Theorem 10.

Proof of Theorem 10. Let G be a finite simple group such that $\gamma_u(G) = 2$ and $G \notin \mathcal{C} \cup \mathcal{T}$. By Lemma 2.7, the claims in parts (i) and (ii) are immediate consequences of Theorems 3(iv) and 4(ii). Moreover, Theorem 9 implies that $\gamma_u^{(2)}(G) = 3$ unless $G \in \{A_{13}, U_5(2), \mathrm{Fi}_{23}\}$ or $G = L_2(q)$ with $q \geqslant 11$ and $q \equiv 3 \pmod 4$. In the first three cases, we can verify the claim in MAGMA by carrying out a random search.

Now assume that $G = L_2(q)$ for $q \geqslant 11$ and $q \equiv 3 \pmod 4$. Let $s \in G$ be an element of order $(q+1)/2$. As noted in the proof of Proposition 7.4, we have $\mathcal{M}(G, s) = \{H\}$ with $H = D_{q+1}$. By Lemma 2.8, it suffices to show that there exist $\alpha, \beta, \gamma \in G/H$ such that $\{\alpha, \beta\}$, $\{\alpha, \gamma\}$ and $\{\beta, \gamma\}$ are bases for the action of G on G/H. To prove this, we will identify G with $\mathrm{PSU}_2(q)$ and G/H with the set Ω of orthogonal pairs of nondegenerate 1-dimensional subspaces of the natural module V for $\mathrm{PSU}_2(q)$.

Fix an orthonormal basis $\{u, v\}$ for V and write $\alpha = \{\langle u \rangle, \langle v \rangle\}$. Then

$$\Omega = \{\alpha\} \cup \{\omega_\lambda : \lambda \in \mathbb{F}_{q^2}^\times \text{ and } \lambda^{q+1} \neq -1\},$$

where

$$\omega_\lambda = \{\langle u + \lambda v \rangle, \langle u - \lambda^{-q} v \rangle\}.$$

Note that $\omega_\lambda = \omega_{-\lambda^{-q}}$ and the condition $\lambda^{q+1} \neq -1$ ensures that

$$\langle u + \lambda v \rangle \neq \langle u - \lambda^{-q} v \rangle.$$

We claim that if $\lambda \in \mathbb{F}_{q^2}^\times$ and $\lambda^{q+1} \neq -1$, then $\{\alpha, \omega_\lambda\}$ is a base if and only if λ is a nonsquare in $\mathbb{F}_{q^2}$.

By Proposition 7.9(ii), H has exactly $(q-3)/4$ regular orbits on Ω. Therefore, there are exactly $(q+1)(q-3)/4$ points $\omega \in \Omega$ such that $\{\alpha, \omega\}$ is a base. Now, there are exactly $(q^2 - 1)/2 - (q+1) = (q+1)(q-3)/2$ nonsquare $\lambda \in \mathbb{F}_{q^2}^\times$ such that $\lambda^{q+1} \neq -1$. Therefore, it suffices to prove that $\{\alpha, \omega_\lambda\}$ is not a base if λ is a square. To this end, suppose that $\lambda = \kappa^2$ for some $\kappa \in \mathbb{F}_{q^2}^\times$ and fix $g = \hat{g} Z(\mathrm{SU}_2(q))$, where

$$\hat{g} = \begin{pmatrix} 0 & \kappa^{1-q} \\ -\kappa^{q-1} & 0 \end{pmatrix},$$

with respect to the ordered basis (u, v). It is straightforward to check that g fixes α and ω_λ, which proves that $\{\alpha, \omega_\lambda\}$ is not a base, as claimed.

Now write

$$\mathbb{F}_{q^2}^\times = \langle \mu \rangle, \quad \beta = \omega_\mu \quad \text{and} \quad \gamma = \omega_{-\mu}.$$

Since μ has multiplicative order $q^2 - 1$, we see that $\{\alpha, \beta\}$ and $\{\alpha, \gamma\}$ are bases. It now remains to prove that $\{\beta, \gamma\}$ is a base. The norm of $u + \mu v$ is $1 + \mu^{q+1}$, which is in $\mathbb{F}_q^\times$, so there exists $\nu \in \mathbb{F}_{q^2}^\times$ such that $\nu^{q+1} = 1 + \mu^{q+1}$. Now

$$(\nu\mu^{-1})^{q+1} = (1 + \mu^{q+1})\mu^{-(q+1)} = 1 + \mu^{-(q+1)},$$

which is the norm of $u - \mu^{-q} v$, so $\{a, b\}$ is an orthonormal basis for V, where $a = \nu^{-1}(u + \mu v)$ and $b = \nu^{-1}\mu(u - \mu^{-q} v)$. Moreover, it is straightforward to check that

$$\langle u - \mu v \rangle = \langle a + \delta b \rangle, \quad \langle u - \mu^{-q} v \rangle = \langle a - \delta^{-q} b \rangle$$

where $\delta = 2(\mu^{-q} - \mu)^{-1}$. Therefore,

$$\beta = \{\langle a \rangle, \langle b \rangle\}, \quad \gamma = \{\langle a + \delta b \rangle, \langle a - \delta^{-q} b \rangle\}$$

and thus the argument in the previous paragraph implies that $\{\beta, \gamma\}$ is a base if and only if δ is a nonsquare. Since 2 is square and μ is nonsquare it remains

to prove that $\mu^{-(q+1)} - 1$ is square. However, this follows immediately from the fact that $\mu^{-(q+1)} - 1 \in \mathbb{F}_q^\times$. Therefore, $\{\beta, \gamma\}$ is a base for G on Ω, which completes the proof that $\gamma_u^{(2)}(G) = 3$. ∎

References

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

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

[3] C. Bates, D. Bundy, S. Perkins and P. Rowley, *Commuting involution graphs in special linear groups*, Communications in Algebra **32** (2004), 4178–4196.

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

[5] G. J. Binder, *The bases of the symmetric group*, Izvestija Vysših Učebnyh Zavedeniǐ Matematika **78** (1968), 19–25.

[6] G. J. Binder, *The two-element bases of the symmetric group*, Izvestija Vysših Učebnyh Zavedeniǐ Matematika **90** (1970), 9–11.

[7] G. J. Binder, *Certain complete sets of complementary elements of the symmetric and the alternating group of the nth degree*, Matematicheskie Zametki **7** (1970), 173–180.

[8] G. J. Binder, *The inclusion of the elements of an alternating group of even degree in a two-element basis*, Izvestija Vysših Učebnyh Zavedeniǐ Matematika **135** (1973), 15–18.

[9] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, Journal of Symbolic Computation **24** (1997), 235–265.

[10] J. L. Brenner and J. Wiegold, *Two generator groups, I*, Michigan Mathematical Journal **22** (1975), 53–64.

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

[12] T. Breuer, *GAP computations concerning probabilistic generation of finite simple groups*, https://arxiv.org/abs/0710.3267.

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

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

[15] D. Bubboloni and M. S. Lucido, *Coverings of linear groups*, Communications in Algebra **30** (2002), 2143–2159.

[16] D. Bubboloni, M. S. Lucido and T. Weigel, *Generic 2-coverings of finite groups of Lie type*, Rendiconti del Seminario Matematico della Università di Padova **115** (2006), 209–252.

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

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

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

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

[21] T. C. Burness, *On base sizes for actions of finite classical groups*, Journal of the London Mathematical Society **75** (2007), 545–562.

[22] T. C. Burness, *Simple groups, generation and probabilistic methods*, in *Groups St Andrews 2017 in Birmingham*, London Mathematical Society Lecture Note Series, Vol. 455, Cambridge University Press, Cambridge, 2019, pp. 200–229.

[23] T. C. Burness, *On base sizes for almost simple primitive groups*, Journal of Algebra **516** (2018), 38–74.

[24] T. C. Burness and M. Giudici, *On the Saxl graph of a permutation group*, Mathematical Proceedings of the Cambridge Philosophical Society **168** (2020), 210–248.

[25] T. C. Burness and S. Guest, *On the uniform spread of almost simple linear groups*, Nagoya Mathematical Journal **109** (2013), 35–109.

[26] T. C. Burness, R. M. Guralnick and J. Saxl, *On base sizes for algebraic groups*, Journal of the European Mathematical Society **19** (2017), 2269–2341.

[27] T. C. Burness and S. Harper, *On the uniform domination number of a finite simple group*, Transactions of the American Mathematical Society **372** (2019), 545–583.

[28] 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.

[29] T. C. Burness, M. W. Liebeck and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proceedings of the London Mathematical Society **98** (2009), 116–162.

[30] T. C. Burness, E. A. O'Brien and R. A. Wilson, *Base sizes for sporadic groups*, Israel Journal of Mathematics **177** (2010), 307–333.

[31] T. C. Burness and A. R. Thomas, *On the involution fixity of exceptional groups of Lie type*, International Journal of Algebra and Computation **28** (2018), 411–466.

[32] R. W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Pure and Applied Mathematics (New York), John Wiley and Sons, New York, 1985.

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

[34] D. I. Deriziotis and G. O. Michler, *Character table and blocks of finite simple triality groups $^3D_4(q)$*, Transactions of the American Mathematical Society **303** (1987), 39–70.

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

[36] S. Dong, H. Pan and F. Tang, *On the weakly monomial subgroups of finite simple groups*, Journal of Algebra and its Applications **18** (2019), Article no. 1950037.

[37] X. G. Fang and C. E. Praeger, *Finite two-arc transitive graphs admitting a Suzuki simple group*, Communications in Algebra **27** (1999), 3727–3754.

[38] X. G. Fang and C. E. Praeger, *Finite two-arc transitive graphs admitting a Ree simple group*, Communications in Algebra **27** (1999), 3755–3769.

[39] I. A. Faradẑev and A. A. Ivanov, *Distance-transitive representations of groups G with $PSL_2(q) \trianglelefteq G \leqslant P\Gamma L_2(q)$*, European Journal of Combinatorics **11** (1990), 347–356.

[40] P. Fleischmann and I. Janiszczak, *The semisimple conjugacy classes of finite groups of Lie type E_6 and E_7*, Communications in Algebra **21** (1993), 93–161.

[41] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.8.7, 2017, http://www.gap-system.org.

[42] S. Garion, *Properties of the product replacement algorithm graph*, PhD. thesis, Hebrew University of Jerusalem, 2009.

[43] D. Goldstein and R. M. Guralnick, *Alternating forms and self-adjoint operators*, Journal of Algebra **308** (2007), 330–349.

[44] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Mathematical Surveys and Monographs, Vol. 40, American Mathematical Society, Providence, RI, 1998.

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

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

[47] Z. Halasi, *On the base size of the symmetric group acting on subsets*, Studia Scientiarum Mathematicarum Hungarica **49** (2012), 492–500.

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

[49] S. Harper, *The spread of almost simple classical groups*, https://arxiv.org/abs/2004.11060.

[50] J. P. James, *Partition actions of symmetric groups and regular bipartite graphs*, Bulletin of the London Mathematical Society **38** (2006), 224–232.

[51] G. A. Jones, *Ree groups and Riemann surfaces*, Journal of Algebra **165** (1994), 41–62.

[52] G. A. Jones, *Cyclic regular subgroups of primitive permutation groups*, Journal of Group Theory **5** (2002), 403–407.

[53] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series, Vol. 129, Cambridge University Press, Cambridge, 1990.

[54] R. Lawther, *Jordan block sizes of unipotent elements in exceptional algebraic groups*, Communications in Algebra **23** (1995), 4125–4156.

[55] R. Lawther, *The action of $F_4(q)$ on cosets of $B_4(q)$*, Journal of Algebra **212** (1999), 79–118.

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

[57] R. Lawther, M. W. Liebeck and G. M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific Journal of Mathematics **205** (2002), 393–464.

[58] M. W. Liebeck, J. Saxl and G. M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proceedings of the London Mathematical Society **65** (1992), 297–325.

[59] M. W. Liebeck and G. M. Seitz, *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*, Mathematical Surveys and Monographs, Vol. 180, American Mathematical Society, Providence, RI, 2012.

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

[61] M. W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, Journal of the American Mathematical Society **12** (1999), 497–520.

[62] M. A. Pellegrini, 2-*Coverings for exceptional and sporadic simple groups*, Archiv der Mathematik **101** (2013), 201–206.

[63] S. Piccard, *Sur les bases du groupe symétrique et du groupe alternant*, Mathematische Annalen **116** (1939), 752–767.

[64] R. Schmidt, *A characterization of* $\mathrm{PSL}(2, p^n)$ *by its centralizer lattice*, Journal of Algebra **21** (1972), 280–291.

[65] K. Shinoda, *The conjugacy classes of the finite Ree groups of type* (F_4), Journal of the Faculty of Sciences University of Tokyo **22** (1975), 1–15.

[66] N. Spaltenstein, *Caractères unipotents de* ${}^3D_4(\mathbb{F}_q)$, Commentarii Mathematici Helvetici **57** (1982), 676–691.

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

[68] R. Steinberg, *Generators for simple groups*, Canadian Journal of Mathematics **14** (1962), 277–283.

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

[70] A. R. Thomas, *The irreducible subgroups of exceptional algebraic groups*, Memoirs of the American Mathematical Society, to appear.

[71] H. N. Ward, *On Ree's series of simple groups*, Transactions of the American Mathematical Society **121** (1966), 62–89.

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

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

[74] R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Mathematics, Vol. 251, Springer, London, 2009.