ON THE UNIFORM SPREAD OF ALMOST SIMPLE LINEAR GROUPS

TIMOTHY C. BURNESS AND SIMON GUEST

ABSTRACT. Let G be a finite group and let k be a non-negative integer. We say that G has uniform spread k if there exists a fixed conjugacy class C in G with the property that for any k 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. Further, the exact uniform spread of G, denoted by $u(G)$, is the largest k such that G has the uniform spread k property. By a theorem of Breuer, Guralnick and Kantor, $u(G) \geq 2$ for every finite simple group G. Here we consider the uniform spread of almost simple linear groups. Our main theorem states that if $G = \langle \mathrm{PSL}_n(q), g \rangle$ is almost simple then $u(G) \geq 2$ (unless $G \cong S_6$), and we determine precisely when $u(G)$ tends to infinity as $|G|$ tends to infinity.

1. INTRODUCTION

Let G be a group and let $d(G)$ be the minimal number of generators for G. We say that G is *d-generated* if $d(G) \leq d$. It is well known that every finite simple group is 2-generated, and in recent years a wide range of related problems on the generation of simple groups has been studied. For example, in [18, 31, 36] it is proved that the probability that two randomly chosen elements of a finite simple group G generate G tends to 1 as $|G|$ tends to infinity, confirming a 1969 conjecture of Dixon [18]. In a different direction, various generalizations have been investigated by imposing restrictions on the orders of the generating pairs (see [38, 39, 40, 43], for example).

Following Steinberg [45], a finite group G is said to be 3/2-*generated* if every nontrivial element of G belongs to a generating pair. In [45], Steinberg conjectured that every finite simple group has this strong 2-generation property, and this was later proved by Guralnick and Kantor in [25], using probabilistic methods. More generally, G is said to have *spread* k if, for any k nontrivial elements $x_1, \ldots, x_k \in G$, there is some $y \in G$ such that $G = \langle x_i, y \rangle$ for all i (this notion is originally due to Brenner and Wiegold [6]). We define $s(G)$ to be the *exact spread* of G, which is the largest k such that G has the spread k property. In particular, G is 3/2-generated if and only if $s(G) \geq 1$.

The stronger notion of *uniform spread* was introduced in [25]. We say that G has uniform spread k if there exists a fixed conjugacy class C in G such that for any k nontrivial elements $x_1, \ldots, x_k \in G$, there is some $y \in C$ with $G = \langle x_i, y \rangle$ for all i. We define the *exact uniform spread* of G, denoted by $u(G)$, in the obvious way. Clearly $s(G) \geq u(G)$, and in general these numbers are distinct. For example, if $G = \mathrm{SL}_3(2)$ then $s(G) = 4$ and $u(G) = 3$.

Let G be a finite simple group. In [25, 27] it is proved that $s(G) \geq 2$ for all but at most finitely many G, and that there are infinitely many examples with $s(G) = 2$. This has been extended in [7], where it is proved that every finite simple group G satisfies the bound $u(G) \geq 2$, with equality if and only if $G = \mathrm{Sp}_{2m}(2)$ (with $m \geq 3$), A_5, A_6 or $\Omega_8^+(2)$ (see [7, Theorem 1.2]). Related results for almost simple groups are also obtained in [7]

Date: August 23, 2012.

2010 *Mathematics Subject Classification.* Primary 20D06; Secondary 20E28, 20F05, 20P05.

Corresponding author: Dr. T.C. Burness.

(recall that a group G is *almost simple* if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for some non-abelian finite simple group G_0, which is the socle of G). Of course, if G is almost simple and G/G_0 is non-cyclic then $s(G) = 0$ since $G \neq \langle x, y\rangle$ for all $x \in G_0$, $y \in G$. However, the following slightly weaker spread-two property is established in [7, Corollary 1.5]: if $x_1, x_2 \in G$ are nontrivial then there exists $y \in G$ such that $G_0 \leqslant \langle x_i, y\rangle$ for $i = 1, 2$.

In this paper we consider the spread of almost simple groups. An important motivation comes from the following conjecture concerning the spread of an arbitrary finite group (see [7, Conjecture 1.8]):

Conjecture 1. *A finite group G is $3/2$-generated if and only if G/N is cyclic for every nontrivial normal subgroup N of G.*

Clearly, the cyclic condition on quotients is necessary for $3/2$-generation. For the converse, Guralnick [22] has established a reduction to the case where G is almost simple with socle G_0, and some special cases have recently been established. Indeed, if G_0 is a sporadic group then the conjecture follows from [7, Table 9 and Lemma 6.1], while the result for alternating groups follows from [7] (for $G = A_n$ and $G_0 = A_6$) and [3] (for the case $G = S_n$). Therefore, to complete the proof of Conjecture 1 we may assume G_0 is a simple group of Lie type.

The above conjecture can also be interpreted in terms of the *generating graph* of a finite group G, which is defined as follows. Let $\Gamma(G)$ be the graph defined on the set of nontrivial elements of G so that two vertices x, y are joined by an edge if and only if $G = \langle x, y\rangle$. Then G is $3/2$-generated if and only if there is no isolated vertex in $\Gamma(G)$. Similarly, G has spread 2 if and only if the diameter of $\Gamma(G)$ is at most 2. An even stronger conjecture is proposed in [8]: if $|G| \geq 4$ then $\Gamma(G)$ contains a Hamiltonian cycle (a path that visits each vertex exactly once) if and only if G/N is cyclic for every nontrivial normal subgroup N of G (see [8, Conjecture 1.6]). For example, it is known that all sufficiently large finite simple groups have this remarkable property (see [8]).

The purpose of this paper is to establish a stronger version of Conjecture 1 in the case $G_0 = \mathrm{PSL}_n(q)$. Our main theorem is the following:

Theorem 2. *Let $G = \langle \mathrm{PSL}_n(q), g\rangle$ be an almost simple group. Then either $u(G) \geq 2$, or $G = \mathrm{PSL}_2(9).2 \cong S_6$ and $u(G) = 0$.*

In a similar spirit to [25, 7], probabilistic methods play an essential role in the proof of Theorem 2. Indeed, our main theorem is an easy corollary of Theorem 3 below on random generation. To state the result we require some additional notation. Let G be a finite group, let C be a conjugacy class of G and let $x \in G$. We write $\mathbb{P}(G = \langle x, y\rangle \mid y \in C)$ for the probability that x and a randomly chosen element of C generate G.

Theorem 3. *Let $G = \langle \mathrm{PSL}_n(q), g\rangle$ be an almost simple group. Then either there exists a G-class $C \subseteq g\mathrm{PSL}_n(q)$ such that*

$$\mathbb{P}(G = \langle x, y\rangle \mid y \in C) > 1/2$$

for all nontrivial $x \in G$, or

$$G \in \{\mathrm{PSL}_2(9).2,\ \mathrm{PSL}_3(4).2_1,\ \mathrm{PSL}_4(2).2,\ \mathrm{PSL}_4(3).2_2\} \tag{1}$$

where $\mathrm{PSL}_2(9).2 \cong S_6$, $\mathrm{PSL}_3(4).2_1$ is an extension of $\mathrm{PSL}_3(4)$ by a graph-field automorphism and $\mathrm{PSL}_4(3).2_2 \cong \langle \mathrm{PSL}_4(3), \iota\rangle$ where ι is the inverse-transpose graph automorphism.

The groups in (1) are genuine exceptions, but in each case it is easy to check directly that $u(G) \geq 2$, unless $G = \mathrm{PSL}_2(9).2$ where we have $u(G) = 0$ and $s(G) = 2$ (see Section 2.7). Note that $\mathrm{PSL}_4(2).2 \cong S_8$ and $\mathrm{PSL}_4(3).2_2 \cong \mathrm{PGO}_6^+(3)$.

It is interesting to consider the asymptotic behaviour of $s(G)$ and $u(G)$ for infinite sequences of simple groups G. In [27] it is proved that $s(A_n)$ tends to infinity if and only if the smallest prime divisor of n tends to infinity. More generally, [27, Theorem 1.1] states that if G_i is a sequence of simple groups such that $|G_i| \to \infty$, then $s(G_i) \to \infty$ if and only if there does not exist an infinite subsequence of the G_i consisting either of odd dimensional orthogonal groups over a field of fixed size, or alternating groups A_{n_i} with each n_i divisible by a fixed prime. In fact, if we exclude these exceptional cases then the proof actually shows that $u(G_i) \to \infty$ (this observation is originally due to Guralnick and Kantor [25]). Here we extend the analysis to sequences of suitable almost simple groups with socle $\mathrm{PSL}_n(q)$.

Theorem 4. *Let $G_i = \langle S_i, g_i \rangle$ be a sequence of almost simple groups, where $S_i = \mathrm{PSL}_{n_i}(q_i)$ and $|G_i|$ tends to infinity. Then $u(G_i)$ is bounded if and only if there exists an infinite subsequence of the G_i where n_i is odd, q_i is fixed and each g_i is either a graph automorphism, or a graph-field automorphism involving an odd order field automorphism.*

Our final result concerns the minimal generation of almost simple groups. Recall that every finite simple group is 2-generated. More generally, if G is almost simple with socle G_0 then a theorem of Dalla-Volta and Lucchini [16] states that

$$d(G) = \max\{2, d(G/G_0)\} \leq 3.$$

As an easy corollary of Theorem 3 we recover this result in the case $G_0 = \mathrm{PSL}_n(q)$.

Corollary 5. *Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$. Then*

$$d(G) = \max\{2, d(G/G_0)\} \leq 3.$$

Let $G = \langle \mathrm{PSL}_n(q), g \rangle$ be an almost simple group. Bounds on fixed point ratios play an essential role in the proof of Theorem 3 (from which Theorem 2 quickly follows). Recall that if $\Omega = G/H$ is a transitive G-set then the *fixed point ratio* of an element $x \in G$, which we denote by $\mathrm{fpr}(x, G/H)$, is the proportion of points in Ω fixed by x. Our approach relies on the following easy observation (see Theorem 2.3). Suppose there exists $s \in \mathrm{PSL}_n(q)$ such that

$$\sum_{H \in \mathcal{M}(gs)} \mathrm{fpr}(x, G/H) < 1/2 \tag{2}$$

for all $x \in G$ of prime order, where $\mathcal{M}(gs)$ is the set of maximal subgroups of G containing gs. Then the conclusion to Theorem 3 holds with $C = (gs)^G$. In almost all cases we will show that there exists such an element s.

There are several steps in estimating the summation in (2). Firstly, we need to choose s in such a way that we can determine the subgroups in $\mathcal{M}(gs)$; the basic idea is to choose s so that gs is contained in very few maximal subgroups, and we use a combination of tools to do this. For example, we frequently apply the main theorem of [24] (and related results in [23, Section 2]) on subgroups containing elements of large prime orders (see Section 2.5), and we use the theory of Shintani descent in the case where g is a field or graph-field automorphism (see Section 2.6). Next we require upper bounds on fixed point ratios for elements of prime order in primitive actions of G (see Section 2.4). Fortunately, such bounds have been widely studied in recent years (see [9, 10, 11, 12] and [25, Section 3], for example). Our aim is to obtain an explicit bound of the form

$$\sum_{H \in \mathcal{M}(gs)} \mathrm{fpr}(x, G/H) < F(n, q)$$

for some function F with the property that $F(n, q) < 1/2$ for all suitable values of n and q. In addition, if $F(n, q)$ tends to 0 as n or q tends to infinity then the conclusion to

Theorem 4 also follows. For some small values on n and q we frequently require a more detailed analysis; in these cases it is often convenient to verify the desired bound directly, with the aid of Magma [4] (see Section 2.7 for further details).

In a forthcoming paper we extend our techniques and analysis to the other almost simple groups of Lie type. Combined with Guralnick's reduction theorem [22], and earlier work on groups with an alternating or sporadic socle, this will complete the proof of the Breuer-Guralnick-Kantor conjecture on 3/2-generated finite groups.

Let us make some comments on the organization of this paper. In Section 2 we fix notation and we present a number of results which will be required in the proofs of the main theorems. More precisely, in Section 2.2 we describe the probabilistic methods at the heart of our proof of Theorem 3 – the main result here is Theorem 2.3. Next, in Section 2.3 we give a brief overview of the subgroup structure of almost simple groups with socle $\mathrm{PSL}_n(q)$, based on Aschbacher's main theorem [1]. Various bounds on fixed point ratios are presented in Section 2.4, and some useful results on primitive prime divisors are recalled in Section 2.5. The theory of Shintani descent plays an important role in our analysis – this is explained in Section 2.6. Finally, in Section 2.7 we discuss the role of Magma in the proofs of the main theorems.

The proofs of Theorems 2 – 4 is given in Sections 3 – 6. Here the analysis naturally splits into 4 cases, according to the various possibilities for g. In Section 3 we quickly handle the case where g is a diagonal automorphism (this is essentially given in [7]). Next, in Sections 4 and 5, we assume g is a field or graph-field automorphism, and we complete the proof in Section 6 where we deal with graph automorphisms. Finally, the short proof of Corollary 5 is presented in Section 7.

Acknowledgments. The authors would like to thank Bob Guralnick for bringing this problem to their attention, and for many helpful discussions relating to this work. The first author would also like to thank the University of Southern California and the California Institute of Technology for their generous hospitality during a research visit in Spring 2008. The first author was supported by EPSRC grant EP/I019545/1.

2. Preliminaries

2.1. **Notation and terminology.** We start by fixing some of the notation we will use throughout the paper. Let G be a finite group and let n be a positive integer. We write G^n for the direct product of n copies of G, $Z(G)$ for the centre of G and $|x|$ for the order of an element $x \in G$. The exact spread and exact uniform spread of G are denoted by $s(G)$ and $u(G)$, respectively. The cyclic group of order n is denoted by Z_n (or just n), while $\mathbb{F}_q$ is the finite field of order q. For integers a and b, (a, b) denotes their highest common factor, and $\delta_{a,b}$ is the familiar Kronecker delta (so that $\delta_{a,b} = 1$ if $a = b$, otherwise $\delta_{a,b} = 0$). We adopt the standard terminology and notation of [33] for finite classical groups and their subgroups. In particular, we write $\mathrm{GL}_n^+(q) = \mathrm{GL}_n(q)$, $\mathrm{GL}_n^-(q) = \mathrm{GU}_n(q)$ and we extend this notation to the projective groups $\mathrm{PGL}_n^\epsilon(q)$ and $\mathrm{PSL}_n^\epsilon(q)$ in the obvious way. We will often represent an element of $(\mathrm{P})\mathrm{GL}(V)$ as a matrix with respect to a fixed basis of V; it is convenient to write $[A_1, \ldots, A_t]$ to denote a block-diagonal matrix with blocks A_i. We will also write J_m for a standard unipotent Jordan block of size m.

Let $G_0 = \mathrm{PSL}_n(q)$, where $n \geq 2$ and $q = p^f$ for a prime p. By a theorem of Steinberg (see [46, Theorem 30]), every automorphism of G_0 is a product of the form $idfg$, where

- i is an *inner* automorphism (induced by conjugation in G_0);
- d is a *diagonal* automorphism (induced by conjugation in $\mathrm{PGL}_n(q) \setminus G_0$);
- f is a *field* automorphism (induced by an automorphism of $\mathbb{F}_q$); and

- g is a *graph* automorphism (induced by the order-two symmetry of the associated Dynkin diagram of type A_{n-1}, with $n \geq 3$).

As the terminology suggests, an *inner-diagonal* automorphism is the product of an inner and a diagonal automorphism. Naturally, we identify G_0 and $\mathrm{PGL}_n(q)$ with the subgroups of $\mathrm{Aut}(G_0)$ comprising the inner and inner-diagonal automorphisms of G_0, respectively. The full automorphism group has structure

$$\mathrm{Aut}(G_0) = (G_0 \rtimes Z_{(n,q-1)}) \rtimes (Z_f \times Z_a),$$

where $a = 2$ if $n \geq 3$, otherwise $a = 1$.

2.2. **Probabilistic methods.** Let G be a finite group. For $x, y \in G$ we define

$$\mathbb{P}(x,y) = 1 - \frac{|\{z \in y^G \mid G = \langle x, z\rangle\}|}{|y^G|} = \frac{|\{z \in y^G \mid G \neq \langle x, z\rangle\}|}{|y^G|};$$

the probability that x and a randomly chosen conjugate of y do *not* generate G.

Lemma 2.1. *Suppose there exists an element $y \in G$ and a positive integer k such that $\mathbb{P}(x,y) < 1/k$ for all nontrivial $x \in G$. Then $u(G) \geq k$.*

Proof. Let $\mathbb{P}(E)$ be the probability that an event E occurs, and let E^c denote the complementary event, so $\mathbb{P}(E^c) = 1 - \mathbb{P}(E)$. Suppose $x_1, \ldots, x_k \in G$ are nontrivial and let E_i be the event that $G = \langle x_i, z\rangle$, where z is a randomly chosen G-conjugate of y. Clearly, it suffices to show that $\mathbb{P}(E) > 0$, where $E = E_1 \cap \cdots \cap E_k$. Now

$$\mathbb{P}(E) = 1 - \mathbb{P}(E^c) = 1 - \mathbb{P}(E_1^c \cup \cdots \cup E_k^c) \geq 1 - \sum_{i=1}^{k} \mathbb{P}(E_i^c)$$

and $\mathbb{P}(E_i^c) = \mathbb{P}(x_i, y) < 1/k$, so $\mathbb{P}(E) > 1 - k(1/k) = 0$ as required. □

Consequently, we see that Theorem 3 implies Theorem 2 (modulo checking the four exceptions in (1)).

Clearly, we need to estimate $\mathbb{P}(x,y)$ in order to apply effectively Lemma 2.1. To do this, we will use the bound provided in Lemma 2.2 below, but first we require some additional notation. For $y \in G$ let $\mathcal{M}(y)$ denote the set of maximal subgroups of G containing y. Let $\Omega = G/H$ denote the set of (right) cosets of a subgroup H in G, and let $\mathrm{fpr}(x, G/H)$ be the *fixed point ratio* of $x \in G$ with respect to the natural transitive action of G on G/H, so $\mathrm{fpr}(x, G/H)$ is the proportion $|C_\Omega(x)|/|\Omega|$ of points in Ω that are fixed by x, where $C_\Omega(x) = \{\omega \in \Omega \mid \omega x = \omega\}$ is the set of fixed points of x on Ω. It is straightforward to show that

$$\mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|}. \tag{3}$$

Lemma 2.2. *For any $x, y \in G$ we have*

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

Proof. Suppose $z \in y^G$ and $G \neq \langle x, z\rangle$. Then $\langle x', y\rangle \leqslant H$ for some $H \in \mathcal{M}(y)$ and $x' \in x^G$. The bound now follows since $\mathrm{fpr}(x, G/H)$ is the probability that a randomly chosen G-conjugate x' of x has the property $\langle x', y\rangle \leqslant H$. □

Clearly we have

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

for all positive integers i, j. In particular, Theorem 3 follows immediately from the next result.

Theorem 2.3. *Let $G = \langle \mathrm{PSL}_n(q), g\rangle$ be an almost simple group and assume G is not one of the groups listed in* (1)*. Then there exists an element $s \in G_0$ such that*

$$\sum_{H\in\mathcal{M}(gs)} \mathrm{fpr}(x, G/H) < 1/2$$

for all $x \in G$ of prime order.

Our strategy therefore is to find a suitable element $s \in G_0$ so that we can determine the maximal subgroups in $\mathcal{M}(gs)$, or at least the subgroups in the superset $\mathcal{M}((gs)^i)$ for some suitable positive integer i. The basic idea is to choose s so that gs is contained in very few maximal subgroups of G. Moreover, if we set $\alpha(x) = \sum_{H\in\mathcal{M}(gs)} \mathrm{fpr}(x, G/H)$, then in order to prove Theorem 4 it suffices to show that $\alpha(x) \to 0$ as $|G| \to \infty$ for all relevant G, and all $x \in G$ of prime order. In general we do this by obtaining an explicit upper bound of the form $\alpha(x) < F(n, q)$ with the property that $F(n, q) \to 0$ as n or q tends to infinity.

Finally, we record a general result on the number of points in Ω fixed by an element $x \in G$.

Lemma 2.4. *Let G be a finite transitive permutation group on a set Ω with point stabilizer H. Suppose $x \in G$ and $x^G \cap H$ is the union of r distinct H-classes, with representatives $x_1, \ldots, x_r$. Then*

$$|C_\Omega(x)| = |C_G(x)| \sum_{i=1}^{r} |C_H(x_i)|^{-1} = \sum_{i=1}^{r} [C_G(x_i) : C_H(x_i)].$$

Proof. By (3) we have

$$|C_\Omega(x)| = \frac{|x^G \cap H|}{|x^G|} \cdot [G : H] = \frac{|C_G(x)|}{|H|} \sum_i |x_i^H| = |C_G(x)| \sum_i |C_H(x_i)|^{-1}.$$

The final equality holds since $|C_G(x)| = |C_G(x_i)|$ for all i. □

Corollary 2.5. *Let G be a finite group, let H be a self-normalizing subgroup of G and let $x \in H$. Let N be the number of distinct G-conjugates of H containing x. Then $N = 1$ if and only if $C_G(x) = C_H(x)$ and $x^G \cap H = x^H$.*

Proof. Suppose $x^G \cap H$ is the union of r distinct H-classes, with representatives $x_1, \ldots, x_r$. Since $N_G(H) = H$, Lemma 2.4 implies that

$$N = \frac{|x^G \cap H|}{|x^G|} \cdot [G : H] = \sum_{i=1}^{r} [C_G(x_i) : C_H(x_i)]$$

and the result follows. □

2.3. **Subgroup structure.** Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$ and natural module V over $\mathbb{F}_q$. The main theorem on the subgroup structure of finite classical groups is due to Aschbacher. In [1], nine subgroup collections are defined, labelled $\mathcal{C}_i$ for $1 \le i \le 9$, and the main theorem states that if H is a maximal subgroup of G not containing G_0 then H is contained in one of these collections. A rough description of the various $\mathcal{C}_i$ collections is given in Table 1.

We refer the reader to [33] (and [33, Table 3.5.A], in particular, for the case $G_0 = \mathrm{PSL}_n(q)$ we are interested in here) for a detailed analysis of these various subgroup collections. Throughout this paper we adopt the standard notation and terminology of [33]. In

$\mathcal{C}_1$	Stabilizers of subspaces, or pairs of subspaces, of V
$\mathcal{C}_2$	Stabilizers of decompositions $V = \bigoplus_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathcal{C}_3$	Stabilizers of prime index extension fields of $\mathbb{F}_q$
$\mathcal{C}_4$	Stabilizers of decompositions $V = V_1 \otimes V_2$
$\mathcal{C}_5$	Stabilizers of prime index subfields of $\mathbb{F}_q$
$\mathcal{C}_6$	Normalizers of symplectic-type r-groups in absolutely irreducible representations
$\mathcal{C}_7$	Stabilizers of decompositions $V = \bigotimes_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathcal{C}_8$	Stabilizers of non-degenerate forms on V
$\mathcal{C}_9$	Almost simple irreducible subgroups of G

TABLE 1. The $\mathcal{C}_i$ collections

particular, if H is a maximal subgroup of G then the *type of* H provides a rough group-theoretic description of H. For example, if $n = 6$ and H is the G-stabilizer of a direct sum decomposition $V = V_1 \oplus V_2 \oplus V_3$ with $\dim V_i = 2$ then we say that H is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_2(q) \wr S_3$.

2.4. **Fixed point ratios.** Let $G = \langle G_0, g \rangle$ be an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$, where $q = p^f$ for a prime p. Recall that in order to prove Theorem 2.3 we need to estimate the sum

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

for certain elements gs in the coset gG_0, where $x \in G$ has prime order. As previously described, Aschbacher's theorem (combined with the analysis in [33]) provides us with detailed information on the possible subgroups in $\mathcal{M}(gs)$. Given a maximal subgroup $H \in \mathcal{M}(gs)$ our attention now turns to the corresponding fixed point ratio $\mathrm{fpr}(x, G/H)$, where $x \in G$ is an arbitrary element of prime order. To prove Theorem 2.3 we require good upper bounds on $\mathrm{fpr}(x, G/H)$.

The study of fixed point ratios dates back to the early days of group theory in the nineteenth century, and in recent years our understanding of fixed point ratios for almost simple primitive groups has advanced greatly. For example, if $n \geq 5$ then Liebeck and Saxl prove that $\mathrm{fpr}(x, G/H) \leq 4/3q$ for all $x \in G$ of prime order (this is a special case of [35, Theorem 1]), and there are examples (for arbitrary n and q) where this upper bound is essentially sharp. For instance, if H is the stabilizer of a 1-dimensional subspace of V, then $\mathrm{fpr}(x, G/H)$ is roughly $1/q$ when x is a transvection. However, we can establish much better bounds when H is a so-called *non-subspace* subgroup of G, which essentially means that H acts irreducibly on V (see [9, Definition 1] for the precise definition).

Theorem 2.6. *Let G be a primitive permutation group with socle $G_0 = \mathrm{PSL}_n(q)$ and point stabilizer H, where $n \geq 3$ and H is a non-subspace subgroup of G. Assume $(n, q) \neq (4, 2), (3, 2)$. Then*

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

for all $x \in G$ of prime order, where $\epsilon = 1/n$ if H is of type $\mathrm{Sp}_n(q)$, otherwise $\epsilon = 0$.

Proof. This is a special case of [9, Theorem 1]. □

For the remaining subspace subgroups we will use Theorem 2.7 below. Here the notation P_k denotes a maximal parabolic subgroup of G corresponding to the G-stabilizer of a k-dimensional subspace of V. In addition, $P_{k,n-k}$ denotes the G-stabilizer of a pair of subspaces $U \subseteq W$ of V, where $\dim U = k$ and $\dim W = n - k$ (such a subgroup is maximal in G whenever $G \not\leqslant \mathrm{P\Gamma L}_n(q)$).

Type of H	Conditions	$g(n,q)$
$\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$	n odd	q^{-2}
$\mathrm{GL}_{n/2}(q^2)$	n even	$2q^{8-2n}$
$\mathrm{Sp}_n(q)$	n even	$2q^{2-n}$
$O_n^\epsilon(q)$	q odd	$2q^{1-n}$

TABLE 2. Some fixed point ratio bounds, for $n \geq 5$

Theorem 2.7. *Let G be a primitive permutation group with socle $G_0 = \mathrm{PSL}_n(q)$ and point stabilizer H, where $n \geq 3$. Let H be a subgroup of type P_k, $P_{k,n-k}$ or $\mathrm{GL}_k(q) \times \mathrm{GL}_{n-k}(q)$, where $k \leq n/2$, and let $x \in G$ be an element of prime order. Then*

$$\mathrm{fpr}(x, G/H) < \begin{cases} \min\{1/2, q^{-1} + q^{1-n}\} & \text{if } k = 1 \\ 2q^{-k} & \text{otherwise.} \end{cases}$$

Proof. This follows from [25, Proposition 3.1, Lemma 3.12]. □

The next result provides sharper, or more explicit, bounds in some specific cases.

Proposition 2.8. *Let G be a primitive permutation group with socle $G_0 = \mathrm{PSL}_n(q)$ and point stabilizer H, where $n \geq 5$ and H is one of the subgroups listed in Table 2. Then $\mathrm{fpr}(x, G/H) < g(n,q)$ for all $x \in G$ of prime order, where $g(n,q)$ is given in the final column of Table 2.*

Proof. Let $x \in G$ be an element of prime order r. If $x \in H \cap \mathrm{PGL}(V)$ then x is either semisimple (if $r \neq p$) or unipotent (if $r = p$), otherwise x is either a field automorphism (in which case r divides $\log_p q = f$), or $r = 2$ and x is either a graph-field automorphism (this requires f to be even) or a graph automorphism. For $x \in H \cap \mathrm{PGL}(V)$ we define

$$\nu(x) = \min\{\dim[\overline{V}, \lambda\hat{x}] \mid \lambda \in K^*\}, \tag{4}$$

where $\hat{x}$ is a pre-image of x in $\mathrm{GL}(V)$, $\overline{V} = V \otimes K$ with $K = \overline{\mathbb{F}}_q$ and $[\overline{V}, \lambda\hat{x}]$ is the subspace $\langle v - v\lambda\hat{x} \mid v \in \overline{V}\rangle$. In particular, $\nu(x)$ is simply the codimension of the largest eigenspace of $\hat{x}$ on $\overline{V}$. Various bounds on $|x^G|$ in terms of $\nu(x)$ are presented in [10, Section 3]. We will use the notation $[A_1, \ldots, A_t]$ to denote a block-diagonal matrix with blocks A_i, and we write J_m for a standard unipotent Jordan block of size m.

First assume H is a non-subspace subgroup, so H is of type $\mathrm{GL}_{n/2}(q^2)$, $\mathrm{Sp}_n(q)$, or $O_n^\epsilon(q)$. Here the desired result quickly follows from Theorem 2.6. For example, suppose H is of type $\mathrm{Sp}_n(q)$. For now, let us assume $n \geq 8$. If $x \in H \setminus \mathrm{PGL}(V)$ then $|x^G| > \frac{1}{2}q^{(n^2-n-4)/2}$ by [10, Corollary 3.49], and the bound in Theorem 2.6 is sufficient. Now assume $x \in H \cap \mathrm{PGL}(V)$. If $\nu(x) \geq 2$ then $|x^G| > \frac{1}{2}q^{4n-8}$ by [10, Corollary 3.38] and once again the result follows from Theorem 2.6. Finally, if $\nu(x) = 1$ then $x = [J_2, I_{n-2}]$ is a transvection and using (3) we calculate that $\mathrm{fpr}(x, G/H) < 2q^{2-n}$ since

$$|x^G \cap H| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-2}(q)|q^{2n-1}} = q^n - 1$$

and

$$|x^G| = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-2}(q)||\mathrm{GL}_1(q)|q^{2n-3}} = \frac{(q^{n-1}-1)(q^n-1)}{q-1}.$$

If $n = 6$ then we can analyse the various possibilities for x in more detail, following the proof of [10, Proposition 8.1]. We leave the details to the reader. In the same way we can deal with the other non-subspace subgroups in Table 2.

For the remainder let us assume n is odd and H is of type $\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$. Let $x \in H$ be an element of prime order r. There are several cases to consider, distinguished by the various possibilities for r.

First assume $x \in H \cap \mathrm{PGL}(V)$. Suppose $r = 2$ and $p > 2$. If $\nu(x) = 1$ then

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

$$|x^G| = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_1(q)||\mathrm{GL}_{n-1}(q)|} = \frac{q^{n-1}(q^n-1)}{q-1}$$

and the result follows. Similarly, if $\nu(x) = s \geq 2$ then the bounds

$$|x^G \cap H| \leq \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{GL}_s(q)||\mathrm{GL}_{n-s-1}(q)|} + \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{GL}_{s-1}(q)||\mathrm{GL}_{n-s}(q)|} < 2q^{\gamma}(q^{-2(n-s)} + q^{-2s})$$

and $|x^G| > \frac{1}{4}q^{\gamma}$, where $\gamma = 2ns - 2s^2$, are good enough.

Next suppose $r = p$. Let a_i denote the number of Jordan blocks of size i in the Jordan form of $\hat{x}$ on $\overline{V}$. Then $a_i = 0$ for all $i > p$, and $a_1 \geq 1$ (since $r = p$ and $x \in H$). Let t denote the number of non-zero a_i terms, and note that $t \geq 2$. If $a_i = 0$ for all $i > 2$, say $x = [J_2^s, J_1^{n-2s}]$ for some $s \geq 1$, then it is easy to see that

$$\mathrm{fpr}(x, G/H) \leq (q^{n-2s}-1)/(q^n-1)$$

and the result follows. In the remaining cases (with $r = p$) we may assume $p > 2$. By applying [10, Lemma 3.18] we deduce that

$$|x^G \cap H| < 2^{t-1}q^{\gamma - 2n + 2\sum_i a_i}$$

and $|x^G| > \frac{1}{2}q^{\gamma}$, where $\gamma = n^2 - 2\sum_{i<j} ia_ia_j - \sum_i ia_i^2$, whence

$$\mathrm{fpr}(x, G/H) < 2^t q^{-2n+2\sum_i a_i}.$$

If $t = 2$ then we may assume $a_i > 0$ for some $i > 2$, hence $\sum_i a_i \leq n-2$ and thus $\mathrm{fpr}(x, G/H) < 2^2q^{-4} < q^{-2}$ as required. On the other hand, if $t \geq 3$ then $\sum_i a_i \leq n - t(t-1)/2$ and this yields

$$\mathrm{fpr}(x, G/H) < 2^t q^{-2n+2(n-t(t-1)/2)} = 2^t q^{-t(t-1)} < q^{2t-t^2} \leq q^{-3}.$$

Now assume $r \neq p$ and $r > 2$. Let $i \geq 1$ be minimal such that r divides $q^i - 1$. Then $C_G(x)$ is of type

$$\mathrm{GL}_l(q) \times \prod_{j=1}^{d} \mathrm{GL}_{a_j}(q^i)$$

for some $d \geq 1$, where $n = l + i\sum_j a_j$ and $a_j \geq 1$ for all j. Set $\gamma = n^2 - l^2 - i\sum_j a_j^2$. First assume $i \geq 2$, so $l \geq 1$ (since $x \in H$). Then $|x^G \cap H| < 2^d q^{\gamma - 2(n-l)}$ and $|x^G| > \frac{1}{2}q^{\gamma}$, so

$$\mathrm{fpr}(x, G/H) < 2^{d+1}q^{-2(n-l)} \leq q^{1-3d} \leq q^{-2}$$

since $n - l \geq 2d$ and $d \geq 1$. Now assume $i = 1$ (so $q \geq 4$). If $d = 1$ then we may argue as in the case $r = 2$ with $p > 2$, so let us assume $d \geq 2$. Without loss, we may assume $l \geq a_1$. Then $|x^G| > \frac{1}{2}q^{\gamma - 1}$ and

$$|x^G \cap H| \leq (d+1) \cdot \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{GL}_{l-1}(q)| \prod_j |\mathrm{GL}_{a_j}(q^i)|} < 2^d(d+1)q^{\gamma - 2(n-l)}.$$

Therefore

$$\mathrm{fpr}(x, G/H) < 2^{d+1}(d+1)q^{1-2(n-l)} < q^{d+1+1-2d} = q^{2-d}$$

and we reduce to the case $d \leq 3$. If $(i, d) = (1, 3)$ then $q \geq 11$ (since $r \geq 5$) and the above bounds give $\mathrm{fpr}(x, G/H) < 64q^{-5} < q^{-3}$. Finally, suppose $(i, d) = (1, 2)$. If $n - l > 2$ then

$n-l \geq 3$ and thus $\mathrm{fpr}(x, G/H) < 24q^{-5} < q^{-2}$ since $q \geq 4$. Otherwise, if $n-l=2$ then $|x^G \cap H| < 4q^{4n-10} + 4q^{2n-4}$, $|x^G| > \frac{1}{2}q^{4n-6}$ and the result follows.

Finally, suppose $x \in H \setminus \mathrm{PGL}(V)$. First assume x is an involutory graph automorphism, so $|x^G| > \frac{1}{2}q^{(n^2+n-4)/2}$ (see [10, Table 3.11]). Now x induces a graph automorphism on the factor of H of type $\mathrm{GL}_{n-1}(q)$, so by considering the centralizer types listed in [10, Table 3.10] we deduce that if $p=2$ then

$$|x^G \cap H| \leq \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{Sp}_{n-1}(q)|} + \frac{|\mathrm{GL}_{n-1}(q)|}{|C_{\mathrm{Sp}_{n-1}(q)}(t)|} < q^{\frac{1}{2}(n^2-3n+2)} + q^{\frac{1}{2}n(n-1)},$$

where $t \in \mathrm{Sp}_{n-1}(q)$ is a transvection, while

$$|x^G \cap H| \leq \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{Sp}_{n-1}(q)|} + \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{SO}^+_{n-1}(q)|} + \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{SO}^-_{n-1}(q)|} < q^{\frac{1}{2}(n^2-3n+2)} + 2q^{\frac{1}{2}n(n-1)}$$

if $p > 2$. These bounds are sufficient unless $n=5$ and $q \leq 3$; here the desired result is quickly obtained through direct calculation.

If x is an involutory field or graph-field automorphism then $q = q_0^2$ and the bounds

$$|x^G \cap H| \leq \frac{|\mathrm{GL}_1(q)|}{|\mathrm{GL}_1(q_0)|} \cdot \frac{|\mathrm{GL}_{n-1}(q)|}{|\mathrm{GL}_{n-1}(q_0)|} < 4q^{\frac{1}{2}(n^2-2n+2)}, \;\; |x^G| > \frac{1}{2}(n, q-1)^{-1} q^{\frac{1}{2}(n^2-1)}$$

are sufficient. Finally, if x is a field automorphism of odd prime order r then $q = q_0^r$ and

$$|x^G \cap H| < 4q^{(1+(n-1)^2)\left(1-\frac{1}{r}\right)}, \;\; |x^G| > \frac{1}{2}q^{(n^2-1)\left(1-\frac{1}{r}\right)-1},$$

hence

$$\mathrm{fpr}(x, G/H) < 8q^{(3-2n)\left(1-\frac{1}{r}\right)+1} \leq 8q^{3-\frac{4}{3}n} \leq q^{4-\frac{4}{3}n}.$$

The result follows. □

Corollary 2.9. *Suppose $n \geq 3$, H is a non-subspace subgroup and $(n,q) \neq (4,2), (3,2)$. Also assume $n \geq 6$ if H is of type $\mathrm{Sp}_n(q)$. Then $\mathrm{fpr}(x, G/H) < f(n,q)$ for all $x \in G$ of prime order, where*

$$f(n,q) = \left(\frac{(q^{n-1}-1)(q^n-1)}{q-1}\right)^{-\frac{1}{2}+\frac{1}{n}}. \tag{5}$$

Proof. If H is not of type $\mathrm{Sp}_n(q)$ then this follows immediately from Theorem 2.6 since

$$|x^G| \geq \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-2}(q)||\mathrm{GL}_1(q)|q^{2n-3}} = \frac{(q^{n-1}-1)(q^n-1)}{q-1}$$

for all $x \in G$ of prime order (minimal if x is a transvection). Now assume H is of type $\mathrm{Sp}_n(q)$. If $x \in H \cap \mathrm{PGL}(V)$ and $\nu(x) = 1$ then $\mathrm{fpr}(x, G/H) = (q-1)/(q^{n-1}-1)$ (see the proof of Proposition 2.8), which is less than $f(n,q)$. If $n \geq 8$ and $x \in H$ is not a transvection, then $|x^G| > \frac{1}{2}q^{4n-8}$ (see [10, Corollaries 3.38 and 3.49]) and the bound in Theorem 2.6 is good enough. Finally, the case $n=6$ can be dealt with directly, by considering each possibility for x in turn. The reader can check the details. □

More accurate bounds when $n=3$ or 4 are given in Lemmas 2.10 and 2.11 below.

Lemma 2.10. *Suppose $n=3$ and $x \in G$ has prime order.*

(i) *If H is of type $O_3(q)$, $\mathrm{GL}_1(q) \wr S_3$, $\mathrm{GL}_1(q^3)$ or $\mathrm{GL}_3(q_1)$, where $q = q_1^r$ for an odd prime r, then $\mathrm{fpr}(x, G/H) \leq (q^2+q+1)^{-1}$.*

(ii) *If H is of type $\mathrm{GL}_3^\epsilon(q^{1/2})$ then $\mathrm{fpr}(x, G/H) \leq (3, q-1)q^{-1/2}(q+1)^{-1}$.*

Proof. This is a straightforward calculation. For example, suppose H is of type $O_3(q)$, in which case q is odd. Set $d = (3, q-1)$ and let $x \in H$ be an element of prime order r. Suppose $x \in H \cap \mathrm{PGL}(V)$. If $r = p$ then x is conjugate to $[J_3]$, so $|x^G \cap H| \leq q^2 - 1$, $|x^G| \geq \frac{1}{d}q(q^2-1)(q^3-1)$ and the result follows. Similarly, if $r = 2$ then x is conjugate to $[-I_2, I_1]$ and we calculate that $\mathrm{fpr}(x, G/H) \leq (q^2+q+1)^{-1}$ since

$$|x^G \cap H| \leq i_2(\mathrm{SO}_3(q)) = \frac{|\mathrm{SO}_3(q)|}{2|\mathrm{SO}_2^+(q)|} + \frac{|\mathrm{SO}_3(q)|}{2|\mathrm{SO}_2^-(q)|} = q^2, \;\; |x^G| = q^2(q^2+q+1),$$

where $i_2(\mathrm{SO}_3(q))$ denotes the number of involutions in $\mathrm{SO}_3(q)$. Next suppose $r \neq p$ and r is odd. Let $i \geq 1$ be minimal such that r divides $q^i - 1$, so $i = 1$ or 2. If $i = 2$ then $|x^G \cap H| = q(q-1)$ and $|x^G| = q^3(q^3-1)$, otherwise $|x^G \cap H| = q(q+1)$ and $|x^G| \geq \frac{1}{d}q^3(q+1)(q^2+q+1)$. In both cases the desired bound holds. Finally, suppose $x \in H \setminus \mathrm{PGL}(V)$. If r is odd then $q = q_0^r$ and x is a field automorphism; here the bounds $|x^G \cap H| \leq [\mathrm{SO}_3(q) : \mathrm{SO}_3(q_0)]$ and $|x^G| \geq \frac{1}{d}[\mathrm{PGL}_3(q) : \mathrm{PGL}_3(q_0)]$ are sufficient. Now assume $r = 2$. If x is a field or graph-field automorphism, then $q = q_0^2$ and

$$|x^G \cap H| \leq \frac{|\mathrm{SO}_3(q)|}{|\mathrm{SO}_3(q^{1/2})|} = q^{1/2}(q+1), \;\; |x^G| \geq \frac{1}{d}\frac{|\mathrm{PGL}_3(q)|}{|\mathrm{PGU}_3(q^{1/2})|} = \frac{1}{d}q^{3/2}(q+1)(q^{3/2}-1),$$

otherwise x is a graph automorphism and we have

$$|x^G \cap H| \leq i_2(\mathrm{SO}_3(q)) + 1 = q^2 + 1, \;\; |x^G| \geq \frac{1}{d}q^2(q^3-1).$$

It is easy to check that these bounds are sufficient.

The other cases are very similar and we leave the details to the reader. Note that if H is of type $\mathrm{GL}_3(q^{1/2})$ and $x \in H$ is an involutory graph-field automorphism, or if H is of type $\mathrm{GU}_3(q^{1/2})$ and $x \in H$ is an involutory field automorphism, then

$$|x^G \cap H| \leq \frac{|\mathrm{PGL}_3^\epsilon(q^{1/2})|}{|\mathrm{SO}_3(q^{1/2})|} = q(q^{3/2}-\epsilon), \;\; |x^G| \geq \frac{1}{d}\frac{|\mathrm{PGL}_3(q)|}{|\mathrm{PGL}_3^\epsilon(q^{1/2})|} = \frac{1}{d}q^{3/2}(q+1)(q^{3/2}-\epsilon),$$

whence $\mathrm{fpr}(x, G/H) \leq dq^{-1/2}(q+1)^{-1}$ as claimed. □

Similarly, we compute the following bounds when $n = 4$. We omit the proof.

Lemma 2.11. *Suppose $n = 4$. Let H_1, H_2 and H_3 be maximal subgroups of G of type $\mathrm{GL}_2(q^2)$, $\mathrm{Sp}_4(q)$ and $O_4^-(q)$, respectively. Then $\mathrm{fpr}(x, G/H_i) \leq f_i(q)$ for all $x \in G$ of prime order, where*

$$f_1(q) = \frac{d_1(q^3+2q+1)}{q^2(q^3-1)}, \; f_2(q) = \frac{q^2}{d_2(q^3-1)}, \; f_3(q) = \frac{4d_2}{q^3-1}$$

with $d_1 = (4, q-1)$ and $d_2 = (2, q-1)$.

2.5. **Primitive prime divisors.** Let $q = p^a$ be a prime power and let r be a prime dividing $q^e - 1$. We say that r is a *primitive prime divisor* (ppd for short) of $q^e - 1$ if r does not divide $q^i - 1$ for all $1 \leq i < e$. A well known theorem of Zsigmondy [48] states that if $e \geq 3$ then either $q^e - 1$ has a primitive prime divisor, or $(q, e) = (2, 6)$. Primitive prime divisors also exist when $e = 2$, provided q is not a Mersenne prime. Note that if r is a primitive prime divisor of $q^e - 1$ then $r \equiv 1 \pmod{e}$.

Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$ and let r be a primitive prime divisor of $q^e - 1$, where $n/2 < e \leq n$. In [24], the subgroups of $\mathrm{PGL}_n(q)$ containing an element of order r are determined. As described in [24, Examples 2.1–2.9], it turns out that such a subgroup belongs to one of nine specific subgroup collections. In [23], Guralnick and Malle prove the following useful corollary.

Theorem 2.12. *Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$ and natural module V, where $n \geq 3$. Let r either be a primitive prime divisor of $q^e - 1$, where $e > n/2$ and $r > 2e + 1$, or a product of two (possibly equal) primitive prime divisors of $q^e - 1$. Suppose H is a maximal subgroup of G such that $H \cap \mathrm{PGL}(V)$ acts irreducibly on V and contains an element of order r. Then one of the following holds:*

(i) *H is of type $\mathrm{GU}_n(q^{1/2})$, $\mathrm{Sp}_n(q)$ or $O^\epsilon_n(q)$;*
(ii) *H is of type $\mathrm{GL}_{n/k}(q^k)$, where k is a prime dividing (n, e);*
(iii) *H is of type $\mathrm{GL}_n(q_0)$, where $q = q_0^k$ for some prime k.*

Proof. This follows immediately from [23, Theorem 2.2]. □

Recall that our basic strategy for proving Theorem 2.3 is to find an element $s \in G_0$ such that gs is contained in very few maximal subgroups of $G = \langle G_0, g\rangle$. If we can choose s so that some power of gs has order r, where r is a primitive prime divisor of $q^e - 1$ with $e > n/2$, then we can use the aforementioned results in [23, 24] to restrict significantly the possible subgroups in $\mathcal{M}(gs)$.

2.6. **Shintani descent.** Let G_0 be a simple group of Lie type over $\mathbb{F}_q$ and set $G = \langle G_0, g\rangle$ for some $g \in \mathrm{Aut}(G_0)$. In order to study the uniform spread of G we need to consider conjugacy classes in the coset gG_0; as previously stated, our aim is to identify a class $(gs)^G$ such that gs is contained in very few maximal subgroups of G. In the cases where g is a field or graph-field automorphism, a key tool to do this is the theory of *Shintani descent*, which we outline below (following Kawanaka [32, Section 2]).

First, let us set up the notation we will use for the remainder of this section. Let X be a connected linear algebraic group over an algebraically closed field and let $\sigma : X \to X$ be a *Frobenius morphism*, so σ is a bijective endomorphism of algebraic groups with finite fixed point subgroup $X_\sigma = \{x \in X \mid x^\sigma = x\}$. Let e be a positive integer and set $G = X_{\sigma^e}$ and $H = X_\sigma \leqslant G$. Note that G is σ-stable, so the restriction $\sigma : G \to G$ is an automorphism. Let $A = \langle \sigma'\rangle$ be a cyclic group of order e and let $\phi : A \to \mathrm{Aut}(G)$ be the homomorphism such that $\phi(\sigma') = \sigma$. In the following we will abuse notation by writing σ for σ'. Let $AG = A \ltimes G$ be the corresponding semidirect product with multiplication

$$(\sigma^i, s)(\sigma^j, t) = (\sigma^{i+j}, s^{\sigma^j} t).$$

Let σs be an element in the coset σG in AG. Then $(\sigma s)^2 = \sigma^2 s^\sigma s$ and using the fact that A has order e we quickly deduce that

$$(\sigma s)^e = s^{\sigma^{e-1}} s^{\sigma^{e-2}} \cdots s^\sigma s \in G. \tag{6}$$

By the Lang-Steinberg Theorem (see [21, Theorem 2.1.1]), there exists $a \in X$ such that

$$s = a^{-\sigma} a. \tag{7}$$

Using the expression for $(\sigma s)^e$ in (6), it is easy to check that $a(\sigma s)^e a^{-1}$ is fixed by σ, so $a(\sigma s)^e a^{-1} \in X_\sigma = H$. This observation allows us to define a map f from the set of AG-classes in the coset σG to the set of H-classes in H by

$$f : (\sigma s)^{AG} \mapsto (a(\sigma s)^e a^{-1})^H,$$

which we call the *Shintani map* of G corresponding to σ. We will frequently abuse notation by writing $f(\sigma s)$ for an arbitrary representative of the H-class of $a(\sigma s)^e a^{-1}$. In addition, to avoid any possible ambiguity we will sometimes write f_G, rather than f, for the above map.

We must check that f is well-defined. First, note that the element $a \in X$ given in (7) is not unique in general. However, if $b \in X$ also satisfies $s = b^{-\sigma} b$ then $ab^{-1} \in X_\sigma = H$ and thus the elements $a(\sigma s)^e a^{-1}$ and $b(\sigma s)^e b^{-1}$ are H-conjugate; so f is independent

of the choice of a in (7). We also need to show that f is independent of the choice of AG-class representative. To see this, suppose $\sigma t \in \sigma G$ is AG-conjugate to σs, say $\sigma t = (\sigma^i w)^{-1}\sigma s(\sigma^i w)$ for some $w \in G$ and integer $i \geq 0$. Now

$$\sigma t = (\sigma t)^i(\sigma^i w)^{-1}\sigma s(\sigma^i w)(\sigma t)^{-i} \tag{8}$$

and $(\sigma^i w)(\sigma t)^{-i} \in G$, so σs and σt are in fact G-conjugate. (Consequently, f is a map from the set of G-classes in the coset σG to the set of H-classes in H.) Therefore, there exists $z \in G$ such that $\sigma t = z^{-1}\sigma s z$, hence $\sigma t = \sigma z^{-\sigma} s z$ and $t = z^{-\sigma} s z$. Since $s = a^{-\sigma}a$ we have $t = (az)^{-\sigma} az$ and thus $f(\sigma t) = az(\sigma t)^e z^{-1}a^{-1}$. But $(\sigma t)^e = z^{-1}(\sigma s)^e z$ by assumption, hence $f(\sigma t) = a(\sigma t)^e a^{-1} = f(\sigma s)$ and f is well-defined.

The next lemma is a key result (see [32, Lemma 2.2]).

Lemma 2.13. *With the notation above, the following hold:*

(i) *We have*

$$C_G(\sigma s) = a^{-1}C_H(f(\sigma s))a = C_{a^{-1}Ha}((\sigma s)^e).$$

In particular, $|C_G(\sigma s)| = |C_H(f(\sigma s))|$ *for all* $s \in G$.

(ii) *The Shintani map* f *is a bijection.*

Proof. First consider (i). If $g \in C_G(\sigma s)$ then $sg = g^\sigma s$ and clearly we have $aga^{-1} \in C_X(f(\sigma s))$. Further, since $a^\sigma = as^{-1}$ (see (7)), we see that $aga^{-1} \in X_\sigma$ and thus $aga^{-1} \in C_H(f(\sigma s))$. Conversely, suppose $h \in C_H(f(\sigma s))$. Then $a^{-1}ha$ centralizes $(\sigma s)^e$ and using (6) we deduce that $(\sigma s)^e = a^{-\sigma^e}a$. Therefore

$$(a^{-1}ha)^{\sigma^e} = a^{-\sigma^e}ha^{\sigma^e} = (\sigma s)^e a^{-1}ha(\sigma s)^{-e} = a^{-1}ha$$

and thus $a^{-1}ha \in X_{\sigma^e} = G$. Further, it is straightforward to check that $a^{-1}ha$ centralizes σs, whence $a^{-1}ha \in C_G(\sigma s)$. This proves (i).

Now let us turn to (ii). First we claim that

$$|(\sigma s)^{AG}| = |f(\sigma s)^H| \cdot [G : H]. \tag{9}$$

This follows easily from (i) since we have already observed that $(\sigma s)^{AG} = (\sigma s)^G$ (see (8)).

Let $y \in H$. By the Lang-Steinberg Theorem (applied to X and σ^e) there exists $b \in X$ such that $y = bb^{-\sigma^e}$. Since σ fixes y it follows that σ^e fixes $b^{-\sigma}b$, whence $b^{-\sigma}b \in G$. By definition, f maps the AG-class of $\sigma b^{-\sigma}b$ to the H-class of $b(\sigma b^{-\sigma}b)^e b^{-1}$, and using the expression in (6) we calculate that

$$b(\sigma b^{-\sigma}b)^e b^{-1} = bb^{-\sigma^e}bb^{-1} = y.$$

This proves that the Shintani map f is surjective.

Finally, let $\{c_1, \ldots, c_t\}$ be the set of H-classes in H. Since f is surjective, there exist AG-classes C_i in σG such that $f(C_i) = c_i$ for all i. By (9) we have $|C_i| = |c_i| \cdot [G : H]$, so

$$\sum_{i=1}^{t} |C_i| = [G : H] \sum_{i=1}^{t} |c_i| = |G| = |\sigma G|$$

and thus $\{C_1, \ldots, C_t\}$ is the complete set of AG-classes in σG. We conclude that f is a bijection. □

Theorem 2.14. *With the notation above, let* Y *be a closed connected* σ*-stable subgroup of* X *and let* $K = Y_{\sigma^e}$ *and* $L = Y_\sigma$. *Let* $\Omega = G/K$ *and* $\Delta = H/L$. *Then*

$$|C_\Omega(\sigma s)| = |C_\Delta(f(\sigma s))|$$

for all $s \in G$.

Proof. Since K is σ-stable, we may form the semidirect product AK. In addition, we obtain a well-defined action of AG on Ω via $(Kg)^\sigma = Kg^\sigma$. Also note that since Y is σ-stable and connected, the Shintani map $f = f_G$ on G naturally induces a Shintani map f_K from the set of AK-classes in the coset σK to the set of L-classes in L.

First assume $|C_\Omega(\sigma s)| = 0$. If $(\sigma s)^G \cap \sigma K$ is non-empty then $g^{-\sigma} sg \in K$ for some $g \in G$ and thus $Kg^{-1} \in C_\Omega(\sigma s)$, a contradiction. Therefore $(\sigma s)^G \cap \sigma K$ is empty. We claim that $f_G(\sigma s)^H \cap L$ is also empty. To see this, suppose there exists $h \in H$ such that $f_G(\sigma s)^h \in L$. By the Shintani correspondence given by f_K, there exists $k \in K$ such that $f_K(\sigma k) = f_G(\sigma s)^h$, where $f_K(\sigma k) = a(\sigma k)^e a^{-1}$ for some $a \in Y$ with $a^{-\sigma} a = k$. Since a is also in X, we may assume that $f_G(\sigma k) = a(\sigma k)^e a^{-1}$, so $f_G(\sigma k) = f_G(\sigma s)^h$ and thus the Shintani correspondence given by f_G implies that σk and σs are G-conjugate. This is a contradiction since $(\sigma s)^G \cap \sigma K$ is empty. This justifies the claim and we conclude that $|C_\Delta(f(\sigma s))| = 0$, as required.

Now suppose $|C_\Omega(\sigma s)| \geq 1$, say $Kg \in C_\Omega(\sigma s)$. Then $g^\sigma s g^{-1} \in K$ and

$$(\sigma s)^{g^{-1}} = \sigma g^\sigma s g^{-1} \in (\sigma s)^G \cap \sigma K$$

is non-empty. Replacing σs by a suitable G-conjugate if necessary, we may assume that $\sigma s \in \sigma K$; that is $s \in K$. Let $\sigma s_1, \ldots, \sigma s_r$ represent the distinct AK-classes in $(\sigma s)^G \cap \sigma K$. By considering the Shintani map f_K, and by applying Lemma 2.13(i), we deduce that

$$|C_K(\sigma s_i)| = |C_L(f_K(\sigma s_i))| = |C_L(f_G(\sigma s_i))|$$

for all i. (Here we may choose $f_G(\sigma s_i) = f_K(\sigma s_i) \in L$ to represent each of the relevant H-classes, so we can write f for both f_G and f_K, when convenient.)

Evidently, AG acts transitively on Ω with point stabilizer AK, and we note that the σs_i represent the distinct AK-classes in $(\sigma s)^{AG} \cap AK$ since $(\sigma s)^{AG} = (\sigma s)^G$ and $(\sigma s_i)^{AK} = (\sigma s_i)^K$ for all i. Therefore Lemma 2.4 yields

$$|C_\Omega(\sigma s)| = \sum_{i=1}^{r} [C_{AG}(\sigma s_i) : C_{AK}(\sigma s_i)] = \sum_{i=1}^{r} [C_G(\sigma s_i) : C_K(\sigma s_i)].$$

By Lemma 2.13(i), the Shintani maps f_G and f_K preserves centralizer cardinalities so

$$|C_\Omega(\sigma s)| = \sum_{i=1}^{r} [C_H(f(\sigma s_i)) : C_L(f(\sigma s_i))]. \tag{10}$$

Finally, we observe that $f(\sigma s)^H \cap L$ is the union of the distinct L-classes $f(\sigma s_i)^L$. To see this, suppose that $l \in L$ is H-conjugate to $f(\sigma s) = f_G(\sigma s) = f_K(\sigma s) \in L$. Since f_K is surjective, there exists $t \in K$ such that $l = f_K(\sigma t)$. We may assume that $f_G(\sigma t) = f_K(\sigma t)$ and $f_G(\sigma s) = f_K(\sigma s)$, and since $f_G(\sigma s)$ and $f_G(\sigma t)$ are H-conjugate it follows that σs and σt must be G-conjugate elements in σK. Thus σt must be K-conjugate to some σs_i and therefore $l = f_K(\sigma t)$ must be L-conjugate to $f_K(\sigma s_i)$, which proves our claim. Now a further application of Lemma 2.4 yields

$$|C_\Delta(f(\sigma s))| = \sum_{i=1}^{r} [C_H(f(\sigma s_i)) : C_L(f(\sigma s_i))]$$

and thus $|C_\Omega(\sigma s)| = |C_\Delta(f(\sigma s))|$ by (10). □

Corollary 2.15. *Let $X = A_{n-1}$ and let Y be a σ-stable subgroup of X, where Y is either a parabolic subgroup, or a Levi subgroup of type $A_{i-1}A_{n-1-i}T_1$ with $1 \leq i < n/2$. Assume $f(\sigma s) \in L$ for some $s \in G$. Then the number of H-conjugates of L containing $f(\sigma s)$ is equal to the number of G-conjugates of K that are normalized by σs.*

Proof. First observe that $N_X(Y) = Y$ and $N_G(K) = K$. Now σs normalizes a G-conjugate K^g if and only if

$$(g^{-1}Kg)^{\sigma s} = g^{-1}Kg \iff g^\sigma s g^{-1} \in N_G(K) = K \iff Kg^\sigma s = Kg,$$

which is true if and only if σs fixes the coset $Kg \in \Omega$. Moreover, since $N_G(K) = K$ we have $K^{g_1} = K^{g_2}$ if and only if $Kg_1 = Kg_2$ and so $|C_\Omega(\sigma s)|$ is the number of G-conjugates of K that are normalized by σs. Similarly, $|C_\Delta(f(\sigma s))|$ is the number of H-conjugates of L containing $f(\sigma s)$, and the result follows by Theorem 2.14. □

Corollary 2.15 will be an important tool in our later analysis. To explain how it applies, let σ be a Frobenius morphism of $X = \mathrm{PSL}_n(K)$ such that $X_{\sigma^e} = \mathrm{PGL}_n(q)$ has socle $G_0 = \mathrm{PSL}_n(q)$, where K is the algebraic closure of $\mathbb{F}_q$. Now σ induces an automorphism of G_0 (a field, or a graph-field automorphism, for example) and we may consider the almost simple group $G = \langle G_0, \sigma\rangle$. Fix an element $x \in X_\sigma$ and let $\sigma s \in \sigma X_{\sigma^e}$ be a representative of the corresponding X_{σ^e}-class under the Shintani map f (see Lemma 2.13). By modifying x if necessary, we may assume that $\sigma s \in \sigma G_0$. As before, let $\mathcal{M}(\sigma s)$ denote the set of maximal subgroups of G containing σs.

We can often use Corollary 2.15 to determine the reducible subgroups in $\mathcal{M}(\sigma s)$. For example, if σ is a field automorphism of G_0 then the corollary tells us that there is a bijection between the set of maximal parabolic subgroups of $X_\sigma = \mathrm{PGL}_n(q_0)$ containing x (we choose x so that these subgroups are easy to identify) and the set of maximal parabolic subgroups of G containing σs. Moreover, this bijection respects the type of the parabolic subgroups involved. For example, if x belongs to unique maximal parabolic subgroups of $\mathrm{PGL}_n(q_0)$ of type P_1, P_2, P_{n-1} and P_n, then σs is contained in exactly 4 maximal parabolic subgroups of G, which again are of type P_1, P_2, P_{n-1} and P_n.

The final proposition of this section provides some useful information on the non-parabolic subgroups in $\mathcal{M}(\sigma s)$.

Proposition 2.16. *With the notation above, let $H \in \mathcal{M}(\sigma s)$ be a non-parabolic subgroup.*

(i) *There are at most $|C_{X_\sigma}(f(\sigma s))|$ subgroups of type H in $\mathcal{M}(\sigma s)$.*

(ii) *Suppose e is prime, σ is a field automorphism and $H \in \mathcal{M}(\sigma s)$ is a subfield subgroup of type $\mathrm{GL}_n(q_0)$, where $q = q_0^e$. Further, assume that $f(\sigma s) \in X_\sigma$ is regular semisimple and either irreducible over $\mathbb{F}_{q_0}$, or block-diagonal of the form $[A, B]$, where A and B are irreducible blocks (over $\mathbb{F}_{q_0}$) of distinct dimensions. Then there are respectively at most e or e^2 subgroups of type $\mathrm{GL}_n(q_0)$ in $\mathcal{M}(\sigma s)$.*

Proof. Let $G_1 = \langle X_{\sigma^e}, \sigma\rangle = \langle \mathrm{PGL}_n(q), \sigma\rangle$ and observe that all maximal subgroups of type H in G are G_1-conjugate (see [33, Proposition 4.0.2(i)]). In particular, if N is the number of subgroups of type H in $\mathcal{M}(\sigma s)$ then

$$N = \frac{|(\sigma s)^{G_1} \cap H|}{|(\sigma s)^{G_1}|} \cdot [G_1 : N_{G_1}(H)] = \frac{|(\sigma s)^{G_1} \cap H||C_{G_1}(\sigma s)|}{|N_{G_1}(H)|}.$$

To prove (i), first observe that $|(\sigma s)^{G_1} \cap H| \leq |H|/e$ since $(\sigma s)^{G_1}$ is contained in the coset $(\sigma s)\mathrm{PGL}_n(q) = \sigma\mathrm{PGL}_n(q)$, while the $(\sigma s)^i(\mathrm{PGL}_n(q) \cap H)$ (with $1 \leq i \leq e$) are distinct cosets in H. Now $|C_{G_1}(\sigma s)| = e|C_{X_\sigma}(f(\sigma s))|$ by Lemma 2.13, and the result follows.

Now let H be a maximal subfield subgroup of G of type $\mathrm{GL}_n(q_0)$ containing σs, where $q = q_0^e$. To prove (ii), set $H_1 = N_{G_1}(H)$ and note that $|(\sigma s)^G \cap H| \leq |(\sigma s)^{G_1} \cap H_1|$. To estimate this upper bound, observe that some G_1-conjugate of H_1 is equal to $\langle\sigma\rangle \times X_\sigma$, so without loss of generality we may assume that $H_1 = \langle\sigma\rangle \times X_\sigma$.

Let $\mathcal{E} = \{\lambda_1^e, \lambda_2^e, \ldots, \lambda_n^e\}$ be the set of eigenvalues of $f(\sigma s)$, and suppose $\sigma t \in H_1$ is an element such that $(\sigma t)^e = t^e$ and $f(\sigma s)$ have the same eigenvalues, where $t \in X_\sigma$. Then t has eigenvalues $\{\mu_1, \ldots, \mu_n\}$, where $\mu_i^e = \lambda_i^e$ for all $1 \leq i \leq n$. In particular, there are e

choices for each μ_i (in the algebraic closure K), so there are at most e^n distinct X_σ-classes in $(\sigma s)^{G_1} \cap H_1$. We claim that each of these X_σ-classes has size $|f(\sigma s)^{X_\sigma}|$.

To see this, let $\sigma t \in (\sigma s)^{G_1} \cap H_1$. As above, let $\{\mu_1, \ldots, \mu_n\}$ be the set of eigenvalues of t, where $\mu_i^e = \lambda_i^e$ for all i. First assume $f(\sigma s)$ is irreducible over $\mathbb{F}_{q_0}$. Then $f(\sigma t)$ is also irreducible over $\mathbb{F}_{q_0}$, and so is $(\sigma t)^e = t^e \in X_\sigma$. Further, each eigenvalue λ_i^e of $f(\sigma s)$ is contained in $\mathbb{F}_{q_0^n}$ and in no smaller field extension of $\mathbb{F}_{q_0}$. Similarly, since $t \in X_\sigma$, the μ_i are also in $\mathbb{F}_{q_0^n}$ and no smaller field extension, so t is irreducible over $\mathbb{F}_{q_0}$. Therefore

$$|C_{X_\sigma}(\sigma t)| = (q_0^n - 1)/(q_0 - 1) = |C_{X_\sigma}(f(\sigma s))|.$$

Moreover, since $t \in \mathrm{GL}_n(q_0)$ is irreducible over $\mathbb{F}_{q_0}$, the eigenvalues of t must be of the form $\{\mu_1, \mu_1^{q_0}, \ldots, \mu_1^{q_0^{n-1}}\}$ and so in fact there are at most e distinct X_σ-classes in $(\sigma s)^{G_1} \cap H_1$.

Now assume that $f(\sigma s)$ is block-diagonal of the form $[A, B]$, where A is irreducible over $\mathbb{F}_{q_0}$ of dimension $n-k$ and B is irreducible of dimension k (where $n-k \neq k$). By relabeling the eigenvalues of $f(\sigma s)$ if necessary, we may assume that $\lambda_1^e, \ldots, \lambda_{n-k}^e$ are contained in $\mathbb{F}_{q_0^{n-k}}$ (and no smaller field extension of $\mathbb{F}_{q_0}$), while the remainder are contained in $\mathbb{F}_{q_0^k}$ (and no smaller field extension). Now the λ_i^e are also the eigenvalues of $(\sigma t)^e = t^e$, and it follows that t is either irreducible, or t is also block-diagonal of the form $[C, D]$ where C and D are irreducible over $\mathbb{F}_{q_0}$ of dimensions $n-k$ and k, respectively. However, t is not irreducible since it has eigenvalues with distinct multiplicative orders. Therefore t is of the form $[C, D]$, hence $|C_{X_\sigma}(\sigma t)| = |C_{X_\sigma}(f(\sigma s))|$. Moreover, since the eigenvalues of t are of the form

$$\{\mu_1, \mu_1^{q_0}, \ldots, \mu_1^{q_0^{n-k-1}}, \mu_{n-k+1}, \ldots, \mu_{n-k+1}^{q_0^{k-1}}\},$$

it follows that there are at most e^2 distinct X_σ-classes in $(\sigma s)^{G_1} \cap H_1$. This proves the claim.

Consequently, if $f(\sigma s)$ is irreducible then

$$|(\sigma s)^{G_1} \cap H_1| \leq e|f(\sigma s)^{X_\sigma}| = e[X_\sigma : C_{X_\sigma}(f(\sigma s))]$$

and thus

$$N \leq \frac{e|X_\sigma||C_{G_1}(\sigma s)|}{|H_1||C_{X_\sigma}(f(\sigma s))|} = \frac{e^2|X_\sigma|}{|H_1|} = e$$

since $|C_{G_1}(\sigma s)| = e|C_{X_{\sigma^e}}(\sigma s)| = e|C_{X_\sigma}(f(\sigma s))|$ (see Lemma 2.13). The result follows. Similarly, if $f(\sigma s)$ is of the form $[A, B]$ then we replace e by e^2, and once again the result follows. □

2.7. **Computational methods.** For small values of n and q our general techniques are less effective and it is convenient to use a computer package such as Magma [4] to obtain the desired results in these situations. Here our main result is the following:

Proposition 2.17. *The conclusion to Theorem 2.3 holds for all (n, q) with $n \leq 10$ and $q \leq f(n)$, where $f(n)$ is defined as follows:*

n	2	3	4	5	6	7	8	9	10
$f(n)$	128	16	9	4	4	2	2	2	2

The next result handles the exceptional cases in the statement of Theorem 3. Here $\mathrm{PSL}_2(9).2 \cong S_6$, $\mathrm{PSL}_3(4).2_1$ is an extension of $\mathrm{PSL}_3(4)$ by a graph-field automorphism, and $\mathrm{PSL}_4(3).2_2 \cong \langle \mathrm{PSL}_4 3, \iota \rangle$ where ι is the inverse-transpose graph automorphism.

Proposition 2.18. *Let G be one of the following groups*

$$\mathrm{PSL}_2(9).2,\ \mathrm{PSL}_3(4).2_1,\ \mathrm{PSL}_4(2).2,\ \mathrm{PSL}_4(3).2_2.$$

Then either $u(G) \geq 2$, or $G = \mathrm{PSL}_2(9).2$ and $(s(G), u(G)) = (2, 0)$.

Remark 2.19. For the relevant groups G in Proposition 2.18, one can check that the G-classes C with the uniform spread 2 property are the following (here we adopt the standard $\mathbb{ATLAS}$ [15] notation for the conjugacy classes in G):

G	C
$\mathrm{PSL}_3(4).2_1$	$6A, 8A, 8B, 8C$
$\mathrm{PSL}_4(2).2$	$8A$
$\mathrm{PSL}_4(3).2_2$	$6P, 8G, 10B, 10C, 12D, 12E, 12F, 18A, 18B$

To establish Propositions 2.17 and 2.18 we adopt methods similar to those used in [7]; the main difference being that we use MAGMA rather than GAP. Let us briefly outline our basic approach.

Let $G = \langle G_0, g\rangle$ and fix an element $s \in G_0$. Recall that we are interested in computing

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

where $x \in G$ has prime order and $\mathcal{M}(gs)$ is the set of maximal subgroups in G containing gs. First we use MAGMA to construct G_0 as a permutation group on $(q^n-1)/(q-1)$ points (this is the representation of G_0 on the set of cosets of a maximal parabolic subgroup P_1; it is the standard representation of $\mathrm{PSL}_n(q)$ in MAGMA). We then use the MAGMA commands AutomorphismGroup (which is based on the algorithm of Cannon and Holt [13]) and PermutationGroup to obtain $\mathrm{Aut}(G_0)$ as a permutation group of reasonable degree. This is effective in most of the cases we consider in Proposition 2.17. However, if G_0 is large, say $G_0 = \mathrm{PSL}_{10}(2)$ or $\mathrm{PSL}_6(4)$ for example, then it is much more efficient to construct $\mathrm{Aut}(G_0)$ directly, using the natural permutation representation of $\mathrm{P\Gamma L}_n(q) = \langle \mathrm{PGL}_n(q), \phi\rangle$ on $(q^n-1)/(q-1)$ points (this is the subgroup of $\mathrm{Aut}(G_0)$ generated by the inner, diagonal and field automorphisms of G_0). To do this, we first construct the direct product $A = \mathrm{P\Gamma L}_n(q) \times \mathrm{P\Gamma L}_n(q)$ and the subgroup $B = \{(\phi x, \phi x^{-T}) \mid x \in \mathrm{PGL}_n(q)\}$ of A. Note that $B \cong \mathrm{P\Gamma L}_n(q)$ and the inverse-transpose automorphism ι acts on B by swapping ϕx and ϕx^{-T}. This gives $\mathrm{Aut}(G_0) \cong \langle B, \iota\rangle$ as a permutation group of degree $2(q^n-1)/(q-1)$.

Next we identify G as a suitable subgroup of $\mathrm{Aut}(G_0)$ (with the aid of the command LowIndexSubgroups), and we compute representatives of the conjugacy classes of both elements and maximal subgroups of G via the commands ConjugacyClasses and MaximalSubgroups, respectively (the latter denotes the MAGMA implementation of an algorithm of Cannon and Holt [14]).

Let $\mathcal{C}$ be a set of representatives of the G-classes of maximal subgroups of G and let $H \in \mathcal{C}$. It is straightforward to calculate the fixed point ratio

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

for all $x \in G$. Indeed, we first compute a set of representatives for the H-classes of H, and then we add up the lengths of the classes that are represented by G-conjugates of x (these are determined using the IsConjugate command). This gives $|x^G \cap H|$ and $\mathrm{fpr}(x, G/H)$ quickly follows.

For each $H \in \mathcal{C}$ let N_H be the number of distinct G-conjugates of H containing gs. Then

$$N_H = \mathrm{fpr}(gs, G/H) \cdot [G : H]$$

and we can compute

$$\alpha(x) := \sum_{H\in\mathcal{M}(gs)} \mathrm{fpr}(x, G/H) = \sum_{H\in\mathcal{C}} N_H \cdot \mathrm{fpr}(x, G/H)$$

for all $x \in G$ of prime order. If we can find an element $gs \in gG_0$ such that the maximum value of $\alpha(x)$ is less than $1/2$ (as we run through a set of G-class representatives of prime order) then $u(G) \geq 2$.

For the vast majority of the groups we consider in Proposition 2.17, there exists a suitable element gs with $\alpha(x) < 1/2$ for all $x \in G$ of prime order. Indeed, the only exceptions are the groups appearing in the statement of Proposition 2.18. For these groups, we attempt to show that $u(G) \geq 2$ directly (which is expensive). Our strategy is to choose a good candidate $gs \in G$ (based on the elements we use in the proof of Theorem 2.3 in Sections 3–6) and then we check that for all nontrivial $x_1, x_2 \in G$, there exists $y \in (gs)^G$ such that

$$G = \langle x_1, y\rangle = \langle x_2, y\rangle. \tag{11}$$

Of course, here we may assume x_1 and x_2 have prime order. Further, it is easy to see that it suffices to check that (11) holds when x_2 belongs to a set of representatives of the G-classes containing elements of prime order.

3. Diagonal automorphisms

Let $G_0 = \mathrm{PSL}_n(q)$, where $n \geq 2$ and $q = p^f$ for a prime p. Recall from Section 2.1 that every automorphism of G_0 is a product of the form $idfg$, where i is *inner*, d is *diagonal* and f and g are *field* and *graph* automorphisms, respectively. More precisely,

$$\mathrm{Aut}(G_0) = (G_0 \rtimes Z_{(n,q-1)}) \rtimes (Z_f \times Z_a),$$

where $a = 2$ if $n \geq 3$, otherwise $a = 1$. Consequently, in order to prove Theorems 2 – 4 we may assume $G = \langle G_0, g\rangle$, where $g \in \mathrm{Aut}(G_0)$ is one of the following:

(i) $g \in \mathrm{PGL}_n(q)$ is a diagonal automorphism;
(ii) $g = \sigma x$, where σ is a nontrivial field automorphism and $x \in \mathrm{PGL}_n(q)$;
(iii) $g = \iota\sigma x$, where ι is the inverse-transpose graph automorphism, σ is a nontrivial field automorphism and $x \in \mathrm{PGL}_n(q)$;
(iv) $g = \iota x$, where ι is the inverse-transpose graph automorphism and $x \in \mathrm{PGL}_n(q)$.

Theorem 3.1. *Theorems 2, 3 and 4 hold in case (i).*

Proof. The proof of the main theorem of [7] provides an explicit semisimple element $s \in G_0$ such that

$$\mathbb{P}(G_0 = \langle x, y\rangle \mid y \in s^{G_0}) > 2/3$$

for all nontrivial $x \in G_0$. Moreover, since $G \leqslant \mathrm{PGL}_n(q)$ we observe that there exists $s_1 \in G$ such that $G = \langle G_0, s_1\rangle$ and $s_1^m = s$ for some integer m. The proof of the above bound in [7] now goes through unchanged (see [7, Proposition 5.23], for example) and we conclude that

$$\mathbb{P}(G = \langle x, y\rangle \mid y \in s_1^G) > 2/3$$

for all nontrivial $x \in G$. Therefore Theorem 3 holds and Theorem 2 follows in the usual way (note that $u(G) \geq 3$ in this case).

Now let us turn to Theorem 4. In [25] it is proved that if G_i is a sequence of simple groups isomorphic to $\mathrm{PSL}_{n_i}(q_i)$, then $u(G_i) \to \infty$ if $|G_i| \to \infty$ (see also [27, Propositions 3.6 and 3.9]). As in [7], an explicit semisimple element $s \in G_0 = \mathrm{PSL}_n(q)$ is given in [25] and it is shown that $\mathbb{P}(G_0 = \langle x, y\rangle \mid y \in s^{G_0})$ is bounded below by a function of n and q, which tends to 1 as n or q tend to infinity. In particular, if $\mathrm{PSL}_{n_i}(q_i) < G_i \leqslant \mathrm{PGL}_{n_i}(q_i)$ then we can choose $s_1 \in G_i$ as in the previous paragraph so that the argument in [25] also yields $u(G_i) \to \infty$. □

We will deal with cases (ii)–(iv) in the next three sections.

4. Field automorphisms

In this section we consider the case $G = \langle G_0, g\rangle$, where $g = \sigma x$ with σ a field automorphism of G_0 of order $e > 1$ and $x \in \mathrm{PGL}_n(q)$. Here $q = q_0^e$ for some p-power q_0, and by fixing a suitable basis for the natural G_0-module V we may assume that σ is *standard* in the sense that $\sigma : (a_{ij}) \mapsto (a_{ij}^{q_0})$. In addition we may write $x = \delta t$, where $t \in G_0$ and δ is a diagonal matrix of the form $\delta = [\lambda, I_{n-1}]$ (modulo scalars) for some $\lambda \in \mathbb{F}_q^*$. Therefore $G = \langle G_0, g\rangle = \langle G_0, \sigma\delta\rangle$, so without any loss of generality we may assume that $g = \sigma\delta$.

The main result of this section is the following (recall that $\mathcal{M}(gs)$ is the set of maximal subgroups of G containing gs):

Theorem 4.1. *Let $G_0 = \mathrm{PSL}_n(q)$ and $G = \langle G_0, g\rangle$, where $g = \sigma x$ with σ a nontrivial field automorphism of G_0 and $x \in \mathrm{PGL}_n(q)$. Assume $G \neq \mathrm{PSL}_2(9).2$. Then there exists $s \in G_0$ such that*

$$\sum_{H \in \mathcal{M}(gs)} \mathrm{fpr}(z, G/H) < 1/2$$

for all $z \in G$ of prime order. In particular $u(G) \geq 2$, and $u(G) \to \infty$ as $|G| \to \infty$.

Our approach is based on the theory of Shintani descent (see Section 2.6). Let $X = \mathrm{PSL}_n(K)$ be the ambient simple algebraic group over the algebraic closure K of $\mathbb{F}_q$. We may view σ as a Frobenius morphism of X with fixed point subgroups $X_\sigma = \mathrm{PGL}_n(q_0)$ and $X_{\sigma^e} = \mathrm{PGL}_n(q)$. By Lemma 2.13, the corresponding Shintani map f provides a bijection between the set of $\mathrm{PGL}_n(q)$-classes in the coset $\sigma\mathrm{PGL}_n(q)$ and the set of $\mathrm{PGL}_n(q_0)$-classes in $\mathrm{PGL}_n(q_0)$. As before, for $s \in G_0$ we abuse notation by writing $f(\sigma s)$ for a representative of the $\mathrm{PGL}_n(q_0)$-class corresponding to the $\mathrm{PGL}_n(q)$-class of σs, so $f(\sigma s)$ is X-conjugate to $(\sigma s)^e$. In view of (6), we note that if $s \in G_0$ then $f(gs) = f(\sigma\delta s)$ has determinant λ^α, where $\alpha = (q-1)/(q_0-1)$.

Lemma 4.2. *Suppose $y \in \mathrm{PGL}_n(q_0)$ has determinant λ^α. Then there exists $s \in G_0$ such that $f(gs)$ is $\mathrm{PGL}_n(q_0)$-conjugate to y.*

Proof. Since the Shintani map f is a bijection, the $\mathrm{PGL}_n(q_0)$-class of y corresponds to the $\mathrm{PGL}_n(q)$-class of σt for some $t \in \mathrm{PGL}_n(q)$. Let μ be the determinant of t and fix a generator ω for $\mathbb{F}_q^*$. Since $f(\sigma t)$ and y are $\mathrm{PGL}_n(q_0)$-conjugate, it follows that $\mu^\alpha = \lambda^\alpha$ and thus $\mu = \omega^{(q_0-1)j}\lambda$ for some integer $0 \leq j < \alpha$. Let $x \in \mathrm{PGL}_n(q)$ be an element with determinant ω^j. Then $(\sigma t)^x = \sigma x^{-\sigma} t x$ and $x^{-\sigma} t x$ has determinant λ. Therefore $x^{-\sigma} t x \in \delta G_0$, so there exists $s \in G_0$ such that $\sigma x^{-\sigma} t x = \sigma\delta s = gs \in G$ corresponds to y under the Shintani correspondence. □

We also need the following number-theoretical result. In the statement, for a positive integer n we write n_2 for the largest power of 2 dividing n. In addition, recall that (a, b) denotes the greatest common divisor of the positive integers a and b.

Lemma 4.3. *Let $q \geq 2$ be an integer. For all integers $n, m \geq 1$ we have*

$$(q^n - 1, q^m - 1) = q^{(n,m)} - 1;$$

$$(q^n - 1, q^m + 1) = \begin{cases} q^{(n,m)} + 1 & \text{if } 2m_2 \leq n_2 \\ (2, q-1) & \text{otherwise;} \end{cases}$$

$$(q^n + 1, q^m + 1) = \begin{cases} q^{(n,m)} + 1 & \text{if } m_2 = n_2 \\ (2, q-1) & \text{otherwise.} \end{cases}$$

Proof. This is a straightforward calculation. □

Proposition 4.4. *Theorem 4.1 holds when $n \geq 5$.*

Proof. Set $y = [J_2, A] \in \mathrm{PGL}_n(q_0)$, where J_2 denotes a standard unipotent Jordan block of size 2 and $A \in \mathrm{GL}_{n-2}(q_0)$ is a semisimple irreducible element with determinant λ^α, where $\alpha = (q-1)/(q_0-1)$ as before. More precisely, we take A to be a suitable power of a Singer cycle in $\mathrm{GL}_{n-2}(q_0)$ of order $q_0^{n-2}-1$, so A has order $(q_0^{n-2}-1)|\lambda^\alpha|/(q_0-1)$, where $|\lambda^\alpha|$ denotes the multiplicative order of λ^α in the cyclic group $\mathbb{F}_{q_0}^*$. Note that if $(n, q_0) \neq (8,2)$ then the order of some suitable power of y is a primitive prime divisor of $q_0^{n-2}-1$ (see Section 2.5). In addition, y has determinant λ^α, so by Lemma 4.2 there exists $s \in G_0$ such that the corresponding Shintani map sends the $\mathrm{PGL}_n(q)$-class of gs to the $\mathrm{PGL}_n(q_0)$-class of y. In particular, y and $(gs)^e$ are X-conjugate. We can write

$$\mathcal{E} = \{1, \omega^k, \omega^{q_0 k}, \omega^{q_0^2 k}, \ldots, \omega^{q_0^{n-3} k}\} \tag{12}$$

for the set of eigenvalues of $(gs)^e$, where ω is a generator of $\mathbb{F}^*_{q_0^{n-2}}$ and $k = (q_0-1)/|\lambda^\alpha|$.

Our first task is to determine the maximal subgroups of G containing gs; as before, we write $\mathcal{M} = \mathcal{M}(gs)$ to denote this set of subgroups. (In part (i) of the following lemma we use P_i to denote the G-stabilizer of an i-dimensional subspace of the natural G_0-module.)

Lemma 4.5. *Suppose $H \in \mathcal{M}$. Then one of the following holds:*

(i) *H is a maximal parabolic subgroup of type P_1, P_2, P_{n-2} or P_{n-1}, and there is exactly one subgroup of each type in $\mathcal{M}$.*

(ii) *H is an imprimitive $\mathcal{C}_2$-subgroup and one of the following holds:*
   (a) *H is of type $\mathrm{GL}_2(q) \wr S_{n/2}$ and $e \geq (n-2)/2$. There is a unique subgroup of this type in $\mathcal{M}$.*
   (b) *H is of type $\mathrm{GL}_1(q) \wr S_n$, where q is even, e is odd and $e \geq n-2$. There are at most $q_0/2$ subgroups of this type in $\mathcal{M}$.*

(iii) *H is a subfield subgroup of type $\mathrm{GL}_n(q_1)$, where $q = q_1^r$ with r a prime divisor of e. For each prime r there are at most $q_0(q_0^{n-2}-1)$ corresponding subfield subgroups in $\mathcal{M}$.*

Proof. By Corollary 2.15, there is a bijective correspondence between the reducible subgroups in $\mathcal{M}$ and the reducible subgroups of $\mathrm{PGL}_n(q_0)$ containing y. Therefore, the maximal parabolic subgroups P_1, P_2, P_{n-2} and P_{n-1} are the only possibilities. Moreover, there is exactly one subgroup in $\mathcal{M}$ of each type since y clearly fixes a unique i-dimensional subspace of the natural $\mathrm{PGL}_n(q_0)$-module for each $i \in \{1, 2, n-2, n-1\}$.

For the remainder, let us assume $H \in \mathcal{M}$ is irreducible. Recall from Section 2.3 that a maximal irreducible subgroup of G belongs to one of eight subgroup collections, labelled $\mathcal{C}_i$ (where $2 \leq i \leq 9$). From the Shintani set-up, $(gs)^e$ is X-conjugate to y, so a suitable power of $(gs)^e$, say $z = (gs)^{m'e}$, is a long root element (i.e. a transvection $[J_2, I_{n-2}]$). This useful observation allows us to restrict significantly the possibilities for H.

Suppose H is a field extension subgroup of type $\mathrm{GL}_{n/k}(q^k)$ for some prime k (recall that these subgroups comprise Aschbacher's $\mathcal{C}_3$ collection). By the proof of [37, Lemma 4.2], we have $\nu(x) \geq k$ for all $x \in H \cap \mathrm{PGL}(V)$ of prime order (see (4)), so $z \notin H$ since $\nu(z) = 1$. Similarly, by applying [37, Lemma 3.7] we deduce that there are no $\mathcal{C}_4$ or $\mathcal{C}_7$ subgroups in $\mathcal{M}$, while $\mathcal{C}_6$-subgroups are ruled out by [10, Lemma 6.3].

Next let us turn our attention to the imprimitive $\mathcal{C}_2$-subgroups in $\mathcal{M}$. If $(n, q_0) \neq (8,2)$ then a suitable power of y, say y^m, has order r where r is a primitive prime divisor of $q_0^{n-2}-1$. Set $x = (gs)^{me}$, so x has order r, and note that $r \geq n-1$ since $r \equiv 1 \pmod{n-2}$. On the other hand, if $(n, q_0) = (8,2)$ then y^{18} has order 7 and we set $x = (gs)^{18e}$. Suppose $H \in \mathcal{M}$ is of type $\mathrm{GL}_{n/t}(q) \wr S_t$ with $t \geq 2$ an integer dividing n, so H is the G-stabilizer of a decomposition of V of the form

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_t, \tag{13}$$

where $\dim V_i = n/t$ for all i.

First we claim that x fixes each of the subspaces in the above decomposition (13). To see this, suppose x induces a nontrivial permutation $\pi \in S_t$ on the V_i. Since x has prime order $r \geq n-1$, it follows that $n = t$ and $r \in \{n-1, n\}$. Further, since z is a transvection it induces a nontrivial permutation $\rho \in S_t$ on the 1-spaces (in fact, we must have $p = 2$ with ρ a transposition). Now ρ and π commute (since x and z are both powers of gs), but this is a contradiction since $C_{S_t}(\pi) = \langle \pi \rangle$. This justifies the claim.

Next we reduce to the case $\dim V_i \leq 2$. To do this, first observe that x and $(gs)^e$ commute, so $(gs)^e$ fixes each of the eigenspaces of x (over the algebraic closure K). Further, x is semisimple with $n-1$ distinct eigenvalues (1 occurs with multiplicity two), so $(gs)^e$ fixes all of the subspaces in the decomposition (13) on which x acts nontrivially (also recall that x fixes each V_i by the previous claim). Seeking a contradiction, let us assume $\dim V_i \geq 3$. Here x acts nontrivially on each V_i, so $(gs)^e$ fixes each V_i. Next observe that if $\xi \in \mathbb{F}_q$ is an eigenvalue of $(gs)^e$, then $gs = \sigma\delta s$ sends a corresponding ξ-eigenvector to a ξ^{q_0}-eigenvector of $(gs)^e$. Indeed, if $v \in V_i$ is a ξ-eigenvector for $(gs)^e$ then

$$(v \cdot gs) \cdot (gs)^e = (v \cdot (gs)^e) \cdot gs = (\xi v) \cdot gs = \xi^{q_0}(v \cdot gs).$$

In particular, gs maps 1-eigenvectors to 1-eigenvectors. Without loss of generality, we may assume that V_1 is a subspace containing a 1-eigenvector. Since the geometric multiplicity of 1 as an eigenvalue of $(gs)^e$ on V is 1, it follows that the algebraic multiplicity of 1 as an eigenvalue of $(gs)^e$ on V_1 is 2. Therefore gs fixes V_1, but this contradicts our earlier observation that the only parabolic subgroups containing gs are of type P_1, P_2, P_{n-1} and P_n (obtained via Corollary 2.15). For the remainder we may assume $\dim V_i \leq 2$.

First assume $\dim V_i = 1$. Here H is of type $\mathrm{GL}_1(q) \wr S_n$ and we note that q is even since H contains the transvection $z = (gs)^{m'e}$. Recall that $(gs)^e$ fixes each V_i in (13) on which x acts nontrivially, so all the eigenvalues of $(gs)^e$ are in $\mathbb{F}_q$ (hence $e \geq n-2$ since the eigenvalues of $(gs)^e$ are contained in $\mathbb{F}_{{q_0}^{n-2}}$, and in no proper subfield (see (12))). In particular, the V_i are simply the eigenspaces of $(gs)^e$ corresponding to the $n-2$ eigenvalues $\xi \in \mathbb{F}_q$ with $\xi \neq 1$, together with the 2-dimensional fixed space of x, say $C_V(x) = V_1 \oplus V_2$. Now z (and therefore $(gs)^e$ and also gs) interchanges V_1 and V_2, and so e must be odd.

We claim that there are precisely $q_0/2$ distinct possibilities for the 1-spaces $\{V_1, V_2\}$ in the 2-dimensional fixed space of x, so gs can belong to at most $q_0/2$ distinct $\mathcal{C}_2$-subgroups of type $\mathrm{GL}_1(q) \wr S_n$. Fix an $\mathbb{F}_q$-basis $\{u, v\}$ for $C_V(x)$ and suppose $V_1 = \langle au + bv \rangle$ and $V_2 = \langle cu + dv \rangle$ for some $a, b, c, d \in \mathbb{F}_q$. Since $(gs)^2$ fixes V_1 and V_2 we may assume that $a, b, c, d \in \mathbb{F}_{q_0}$ (note that e is odd and $\langle \xi(au + bv) \rangle = \langle au + bv \rangle, \langle \xi(cu + dv) \rangle = \langle cu + dv \rangle$ for all $\xi \in \mathbb{F}_q^*$). Evidently, there are $q_0 + 1$ possibilities for V_1; either $V_1 = \langle u + \xi v \rangle$ for some $\xi \in \mathbb{F}_{q_0}$, or $V_1 = \langle v \rangle$. Now q_0 is even and $(gs)^e$ interchanges V_1 and V_2, so there are $q_0/2$ possibilities for the pair $\{V_1, V_2\}$, as claimed.

To complete the analysis of $\mathcal{C}_2$ subgroups, let us assume $\dim V_i = 2$. By Corollary 2.15, gs belongs to a unique maximal parabolic subgroup of G of type P_2, so there is a unique 2-dimensional subspace of V fixed by gs. Recall that $(gs)^e$ fixes each V_i on which x acts nontrivially. Clearly, either x acts nontrivially on each V_i, or one of the V_i coincides with $C_V(x)$. It follows that each eigenvalue of $(gs)^e$ belongs to $\mathbb{F}_{q^2}$ (and thus $e \geq (n-2)/2$). Now, if every nontrivial eigenvalue of x belongs to $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ then the V_i are 2-spaces fixed by $(gs)^e$. In particular, the decomposition is unique and thus gs belongs to a unique $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_2(q) \wr S_{n/2}$. Finally, let us assume that all the eigenvalues of $(gs)^e$ are in $\mathbb{F}_q$. By Galois theory, gs acts transitively on the set of roots of the minimal polynomial of $(gs)^e$ that are not equal to 1, which immediately implies that gs acts transitively on the $n-2$ nontrivial eigenvalues of $(gs)^e$. In particular, gs induces an $(n-2)$-cycle on the corresponding eigenspaces $\{\langle v_i \rangle \mid 1 \leq i \leq n-2\}$, so there is a unique gs-invariant partition of $\langle v_1 \rangle \oplus \cdots \oplus \langle v_{n-2} \rangle$ into 2-spaces. The remaining 2-space is $C_V(x)$, so gs fixes a

unique decomposition of type (13) and once again we conclude that gs belongs to a unique $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_2(q) \wr S_{n/2}$.

We have now dealt with the subgroups in the $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6$ and $\mathcal{C}_7$ collections. Clearly there are no $\mathcal{C}_8$-subgroups of type $O_n^\epsilon(q)$ (with q odd) in $\mathcal{M}$ since these subgroups do not contain transvections. To eliminate any subgroups in the $\mathcal{C}_9$ collection we can either appeal to [26, Theorem 7.1] (if $n \geq 6$), or we can use the main theorem of [30]. In this way, we deduce that any additional $H \in \mathcal{M}$ is one of the following:

(i) H is a $\mathcal{C}_5$-subgroup of type $\mathrm{GL}_n(q_1)$, with $q = q_1^r$ for some prime r.
(ii) H is a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_n(q)$, with n even.
(iii) H is a $\mathcal{C}_8$-subgroup of type $\mathrm{GU}_n(q^{1/2})$.

We claim that there are no subgroups in $\mathcal{M}$ of type (ii) or (iii). To see this, first suppose $H \in \mathcal{M}$ is a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_n(q)$. Recall that the set of eigenvalues of $(gs)^e$ is given in (12), where $\mathbb{F}^*_{q_0^{n-2}} = \langle \omega \rangle$ and $k = (q_0 - 1)/|\lambda^\alpha|$. The presence of the J_2 block in y implies that $(gs)^e$ is in $\mathrm{PSp}_n(q)$, so we must have $\xi^{-1} \in \mathcal{E}$ for all $\xi \in \mathcal{E}$. However, $\omega^{-k} \notin \mathcal{E}$. Indeed, if there exists $1 \leq i \leq n-3$ such that $\omega^{-k} = \omega^{q_0^i k}$ then $q_0^i k \equiv -k \pmod{q_0^{n-2}-1}$ and thus $q_0^{n-2} - 1$ divides $(q_0^i + 1)k$. This is a contradiction since $k \leq q_0 - 1$. We conclude that there are no subgroups of type $\mathrm{Sp}_n(q)$ in $\mathcal{M}$.

Now suppose $H \in \mathcal{M}$ is a $\mathcal{C}_8$ subgroup of type $\mathrm{GU}_n(q^{1/2})$. Then q is an even power of p and $\xi^{-q^{1/2}} \in \mathcal{E}$ for all $\xi \in \mathcal{E}$. In particular, there exists a non-negative integer $i \leq n-3$ such that $\omega^{-q_0^f k} = \omega^{q_0^i k}$, where $f = e/2$, so $q_0^{n-2} - 1$ divides $k(q_0^f + q_0^i)$. Since $k \leq q_0 - 1$, we have $q_0^f \geq q_0^{n-3}$ and thus $f \geq n-3 \geq i$. But $(q_0^{n-2} - 1, k(q_0^f + q_0^i)) \leq k(q_0^{n-2} - 1, q_0^{f-i} + 1)$ and by Lemma 4.3 this is at most $k(2, q_0 - 1)$ unless $2(f-i)_2 \leq (n-2)_2$, in which case it is at most $k(q_0^{(f-i,n-2)} + 1) \leq k(q_0^{(n-2)/2} + 1) < q_0^{n-2} - 1$. This contradicts the fact that $q_0^{n-2} - 1$ divides $k(q_0^f + q_0^i)$, so there are no subgroups of type $\mathrm{GU}_n(q^{1/2})$ in $\mathcal{M}$.

Finally, suppose $H \in \mathcal{M}$ is a subfield subgroup of type $\mathrm{GL}_n(q_1)$, where $q = q_1^r$ with r prime. Since $y \in \mathrm{PGL}_n(q_1) \cap \mathrm{PGL}_n(q_0)$ we quickly deduce that $\mathbb{F}_{q_0} \cap \mathbb{F}_{q_1} = \mathbb{F}_{q_0}$, so $q_1 = q_0^m$ for some $m \geq 1$. Therefore $e = mr$ (recall that $q = q_0^e$) and thus the number of possibilities for r is equal to the number of distinct prime divisors of e (which is less than $\log(e) + 1$). By Proposition 2.16(i), there are at most $|C_{\mathrm{PGL}_n(q_0)}(y)| = q_0(q_0^{n-2} - 1)$ subfield subgroups of type $\mathrm{GL}_n(q_1)$ in $\mathcal{M}$. □

We are now in a position to proceed with the proof of Proposition 4.4. Let $z \in G$ be an element of prime order and set

$$\alpha(z) = \sum_{H \in \mathcal{M}} \mathrm{fpr}(z, G/H). \tag{14}$$

For the parabolic subgroups in $\mathcal{M}$, Theorem 2.7 gives $\mathrm{fpr}(z, G/H) < q^{-1} + q^{1-n}$ if H is of type P_1 or P_{n-1}, and $\mathrm{fpr}(z, G/H) < 2q^{-2}$ if H is of type P_2 or P_{n-2}. Therefore, the contribution to $\alpha(z)$ from the reducible subgroups in $\mathcal{M}$ is less than

$$2q^{-1} + 2q^{1-n} + 4q^{-2}.$$

For the remaining subgroups $H \in \mathcal{M}$, Corollary 2.9 states that

$$\mathrm{fpr}(z, G/H) < \left(\frac{(q^{n-1} - 1)(q^n - 1)}{q - 1} \right)^{-\frac{1}{2} + \frac{1}{n}} = f(n, q). \tag{15}$$

In view of Lemma 4.5, using the fact that there are less than $\log(e) + 1$ distinct prime divisors of e, we conclude that

$$\alpha(z) < 2q^{-1} + 2q^{1-n} + 4q^{-2} + \left(\frac{1}{2} q_0 + 1 + (\log(e) + 1) q_0 (q_0^{n-2} - 1) \right) \cdot f(n, q). \tag{16}$$

If $e \geq 3$ then this bound implies that $\alpha(z) < 1/2$ unless $(n, q_0, e) = (5, 2, 3)$. Here we may omit the term $\log(e)$, and this gives $\alpha(z) < 1/2$ as required. Similarly, if $e = 2$ and $q_0 \geq 3$ then the above bound (again, with $\log(e)$ omitted) is sufficient unless $(n, q_0) = (5, 3)$.

Suppose $(n, q_0, e) = (5, 3, 2)$. As above, we calculate that the contribution to $\alpha(z)$ from non-subfield subgroups is less than 0.285. Therefore, we need to show that the remaining contribution, which we will denote by $\beta(z)$, is at most 0.215. Let $H \in \mathcal{M}(gs)$ be a subfield subgroup of type $\mathrm{GL}_5(3)$. Since $\beta(z) \leq 3(3^3 - 1) \cdot \mathrm{fpr}(z, G/H)$, it suffices to show that $\mathrm{fpr}(z, G/H) \leq 0.0027$ for all $z \in H$ of prime order. This is a straightforward calculation. For example, suppose $z \in H$ is semisimple. If $\nu(z) \geq 2$ (see (4)) then $|z^G| > \frac{1}{2}3^{12}$ by [10, Corollary 3.38] and the desired bound follows from Theorem 2.6. On the other hand, if $\nu(z) = 1$ then

$$\mathrm{fpr}(z, G/H) = \frac{|z^H|}{|z^G|} = \frac{|\mathrm{GL}_5(3)|}{|\mathrm{GL}_4(3)||\mathrm{GL}_1(3)|} \cdot \frac{|\mathrm{GL}_4(9)||\mathrm{GL}_1(9)|}{|\mathrm{GL}_5(9)|} = \frac{1}{4941}.$$

The other cases are very similar.

Next suppose $q = 4$. If $n = 5$ or 6 then Proposition 2.17 applies, so we will assume $n \geq 7$. Let $k < n/2$ be maximal such that $n - k$ is odd and $(n, n - k) = 1$. We claim that $k \geq n/4$. If n is even then take k to be a prime in the range $n/4 < k < n/2$ (such a prime exists by Bertrand's Postulate), so $n - k$ is odd and $(n, n - k) = 1$. Now suppose n is odd (we may as well assume n is reasonably large, say $n > 100$). Let k' be a prime in the range $n/8 < k' < n/4$ and set $k = 2k'$. Then $n - k$ is odd and we may choose k' so that it does not divide n (indeed, if k' divides n then $n = 5k'$ or $7k'$, but there are at least 3 possibilities for k' since we are assuming $n > 100$; see [42], for example). Therefore $(n, n - k) = 1$ as required.

Let $y = [A, B] \in \mathrm{GL}_n(2)$, where $A \in \mathrm{GL}_k(2)$ and $B \in \mathrm{GL}_{n-k}(2)$ are Singer cycles, so $|A| = 2^k - 1$ and $|B| = 2^{n-k} - 1$. Let d be the largest divisor of $2^{n-k} - 1$ that is relatively prime to $2^i - 1$ for all $1 \leq i < n - k$. Note that every prime divisor of d is a primitive prime divisor of $2^{n-k} - 1$, and is therefore congruent to 1 modulo $n - k$. Since $n - k \geq 5$ is odd, [23, Lemma 2.1] implies that $d > 2(n - k) + 1$. In addition, since $k < n - k$ it follows that d and $2^k - 1$ are coprime, and that some power of y has order d. Moreover, since $n - k$ is odd it follows that a primitive prime divisor of $2^{n-k} - 1$ is also a primitive prime divisor of $4^{n-k} - 1$. Now, if d is a prime then a power of y has order a primitive prime divisor r of $4^{n-k} - 1$ with $r > 2(n - k) + 1$. On the other hand, if d is composite then some power of y has order a product of two (not necessarily distinct) primitive prime divisors of $4^{n-k} - 1$. Consequently, Theorem 2.12 applies and we obtain a short list of possible subgroups $H \in \mathcal{M}$, where $\mathcal{M}$ is the set of maximal subgroups of G that contain gs (using the Shintani correspondence we choose $s \in G_0$ so that $(gs)^2$ is X-conjugate to y):

(i) H is a parabolic subgroup of type P_k or P_{n-k}; there is exactly one subgroup of each type in $\mathcal{M}$.

(ii) H is a $\mathcal{C}_8$-subgroup of type $\mathrm{GU}_n(2)$ or $\mathrm{Sp}_n(4)$.

(iii) H is a subfield subgroup of type $\mathrm{GL}_n(2)$; by Proposition 2.16, there are at most $|C_{\mathrm{PGL}_n(2)}(y)| = (2^{n-k} - 1)(2^k - 1)$ subgroups of this type in $\mathcal{M}$.

In fact, it is easy to see that there are no $\mathcal{C}_8$-subgroups in $\mathcal{M}$. Indeed, if H is of type $\mathrm{GU}_n(2)$ then $|H|$ is not divisible by a primitive prime divisor of $2^{n-k} - 1$. Similarly, we can eliminate subgroups of type $\mathrm{Sp}_n(4)$ since y is irreducible on an odd dimensional subspace of V. We deduce that if $z \in G$ has prime order then

$$\alpha(z) < 4^{1-k} + (2^{n-k} - 1)(2^k - 1)f(n, 4) \leq 4^{1-n/4} + 2^n f(n, 4) < 1/2$$

for all $n \geq 8$, where $f(n, 4)$ is defined as in (15). Finally, if $n = 7$ then $k = 3$ and the first inequality yields $\alpha(z) < 1/2$ as required.

To complete the proof of Proposition 4.4 it remains to show that $u(G) \to \infty$ as $|G| \to \infty$. If $q > 49$ then the bound in (16) implies that $\alpha(z) < q^{-1/4}$ for all $n \geq 5$, so we may assume q (and therefore e) is bounded and n tends to infinity.

Assume n is large and let k be an integer such that $n/4 < k < n/2$, $n-k$ is odd and $(n,k) = (n-k,e) = 1$ (note that k exists since e is bounded). Set $y = [A,B] \in \mathrm{PGL}_n(q_0)$, where $A \in \mathrm{GL}_k(q_0)$ and $B \in \mathrm{GL}_{n-k}(q_0)$ are irreducible (take suitable powers of Singer cycles so that $\det(y) = \lambda^\alpha$). Choose $s \in G_0$ such that $(gs)^e$ is X-conjugate to y.

There is a suitable power of $(gs)^e$, say $x = (gs)^{me}$, such that x has order r, where r is a primitive prime divisor of $q_0^{n-k} - 1$. Moreover, since $(n-k,e) = 1$ it follows that r is a primitive prime divisor of $q^{n-k} - 1$. Now [23, Lemma 2.1] implies that either $r > 2(n-k)+1$, or some other power of $(gs)^e$ has order r', with r' a product of two (not necessarily distinct) primitive prime divisors of $q^{n-k}-1$. In particular, by combining Theorem 2.12 and Corollary 2.15, we see that the only possibilities for $H \in \mathcal{M}$ are the following:

(i) A maximal parabolic subgroup of type P_k or P_{n-k}; there is exactly one subgroup of each type in $\mathcal{M}$.

(ii) A $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_n(q)$, $O_n^\epsilon(q)$ or $\mathrm{GU}_n(q^{1/2})$.

(iii) A subfield subgroup of type $\mathrm{GL}_n(q_1)$, where $q = q_1^a$ for some prime divisor a of e.

Since r is a primitive prime divisor of $q^{n-k}-1$, and we have chosen k so that $n-k$ is odd, it follows that x does not belong to a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_n(q)$ or $O_n^\epsilon(q)$, so there are no such subgroups in $\mathcal{M}$. Next we observe that there are no $\mathcal{C}_8$-subgroups of type $\mathrm{GU}_n(q^{1/2})$ in $\mathcal{M}$. Since r is a primitive prime divisor of $q^{n-k}-1$, it follows that r does not divide $|\mathrm{PGU}_n(q^{1/2})|$. Indeed, suppose r divides $q^{j/2} - (-1)^j$ for some $2 \leq j \leq n$. If j is even then r divides $q^{j/2}-1$, which is absurd since r is a primitive prime divisor of $q^{n-k}-1$. On the other hand, if j is odd then Lemma 4.3 implies that r divides $(q^{j/2}+1, q^{n-k}-1) = (2, q-1)$, which once again is a contradiction.

Finally, note that for each prime divisor a of e there are at most $|C_{\mathrm{PGL}_n(q_0)}(y)| = (q_0^{n-k}-1)(q_0^k-1)/(q_0-1) < q^{n/e}$ subfield subgroups of type $\mathrm{GL}_n(q_1)$ (where $q = q_1^a$) in $\mathcal{M}$ (see Proposition 2.16(i)). Therefore, by applying Theorem 2.7, we conclude that if n is sufficiently large and $z \in G$ has prime order, then

$$\alpha(z) < 2q^{-k} + 2q^{k-n} + (\log(e)+1)q^{n/e} \cdot f(n,q).$$

Now $f(n,q) < q^{3-n-2/n}$ and q is bounded, hence $\alpha(z) \to 0$ as $n \to \infty$ and the result follows. □

To complete the proof of Theorem 4.1, it remains to deal with the small dimensional groups with $n \leq 4$.

Proposition 4.6. *Theorem 4.1 holds when $n = 4$.*

Proof. In view of Proposition 2.17, we may assume $q \geq 16$. Take $y = [A,\mu] \in \mathrm{PGL}_4(q_0)$, where $A \in \mathrm{GL}_3(q_0)$ is irreducible of order $q_0^3 - 1$ and $\mu = \lambda^\alpha/\det(A)$. By Lemma 4.2 there exists $s \in G_0$ such that $(gs)^e$ is X-conjugate to y. Note that a suitable power of $(gs)^e$, say $x = (gs)^{me}$, has order r, where r is a primitive prime divisor of $q_0^3 - 1$.

Let $\mathcal{M}$ be the set of maximal subgroups of G containing gs, and let $H \in \mathcal{M}$. We claim that one of the following holds:

(i) H is a parabolic subgroup of type P_1 or P_3; there is a unique subgroup of each type in $\mathcal{M}$.

(ii) $e \equiv 0 \pmod 3$ and H is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_4$; there is a unique such subgroup in $\mathcal{M}$.

(iii) H is a subfield subgroup of type $\mathrm{GL}_4(q_1)$, where $q = q_1^a$ for some prime divisor a of e; for each q_1 there are at most $|C_{\mathrm{PGL}_4(q_0)}(y)| = q_0^3 - 1$ such subgroups in $\mathcal{M}$.

By Corollary 2.15, the only reducible subgroups in $\mathcal{M}$ are parabolic of type P_1 or P_3; there are unique such subgroups because y fixes a unique i-dimensional subspace of the natural $\mathrm{PGL}_4(q_0)$-module, for $i = 1, 3$. Part (iii) on subfield subgroups follows in the usual way from Proposition 2.16(i).

Next suppose $H \in \mathcal{M}$ is a $\mathcal{C}_2$-subgroup. If $(3, e) = 1$ then r is a primitive prime divisor of $q^3 - 1$ and thus $\mathcal{C}_2$-subgroups are ruled out by the main theorem of [24]. Now assume e is a multiple of 3, so the eigenvalues of $(gs)^e$ are contained in $\mathbb{F}_q$. Note that $r \equiv 1 \pmod 3$ and thus $r \geq 7$. In particular, if $(gs)^e$ stabilizes a decomposition $V = V_1 \oplus V_2 \oplus V_3 \oplus V_4$ then x must fix each V_i, so the V_i are simply the eigenspaces of x and we conclude that there is a unique $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_4$ in $\mathcal{M}$.

Now assume gs stabilizes a decomposition $V = V_1 \oplus V_2$ with $\dim V_i = 2$. By the same reasoning, x must fix V_1 and V_2. Without loss of generality, let us assume that the restriction of x to V_1 has eigenvalues 1 and ξ, while x restricted to V_2 has eigenvalues ξ^{q_0} and $\xi^{q_0^2}$. As observed in the proof of Lemma 4.5, since gs commutes with x it sends 1-eigenvectors of x to 1-eigenvectors of $(gs)^e$ and thus gs fixes V_1. This is a contradiction because we have already observed that gs does not fix a 2-dimensional subspace of V. Therefore, there are no $\mathcal{C}_2$-subgroups of type $\mathrm{GL}_2(q) \wr S_2$ in $\mathcal{M}$.

The $\mathcal{C}_4, \mathcal{C}_6$ and $\mathcal{C}_7$ families are empty, and the same is true for the $\mathcal{C}_9$ family since $q \neq p$ (see [5, Table 7.9]). We can quickly eliminate $\mathcal{C}_3$-subgroups of type $\mathrm{GL}_2(q^2)$ because the eigenvalues of $(gs)^e$ do not consist of two pairs, with elements in each pair having the same multiplicative order (as elements of $\mathbb{F}_{q^3}^*$). Therefore it remains to deal with the subgroups in $\mathcal{C}_8$.

Suppose $H \in \mathcal{M}$ is a $\mathcal{C}_8$-subgroup H of type $\mathrm{GU}_4(q^{1/2})$, so $q = q_0^e$ is an even power of p and we may write $q^{1/2} = q_0^f$. Let $\mathcal{E} = \{\mu, \omega, \omega^{q_0}, \omega^{q_0^2}\}$ be the set of eigenvalues of $(gs)^e$, where $\mathbb{F}_{q_0^3}^* = \langle \omega \rangle$, and let T be a maximal torus of H containing $(gs)^e$. The conjugacy classes of maximal tori of $\mathrm{GU}_4(q_0^f)$ are parametrized by the conjugacy classes in S_4, which is the Weyl group of the corresponding root system of type A_3. For example the class of transpositions in S_4 corresponds to a class of maximal tori with structure $Z_i \times Z_j \times Z_j$, where $i = q_0^{2f} - 1$ and $j = q_0^f + 1$. The eigenvalues of elements in such a torus are of the form $\{a, a^{q_0^f}, b, c\}$, where a has multiplicative order dividing $q_0^{2f} - 1$ and b and c have multiplicative order dividing $q_0^f + 1$. In particular, the two eigenvalues corresponding to the $q_0^{2f} - 1$ factor have the same multiplicative order. Now three of the four eigenvalues of $(gs)^e$ have multiplicative order $q_0^3 - 1$ and so these must correspond to cyclic factors of T of order $q_0^{4f} - 1$ or $q_0^{2f} - 1$. Therefore the only possible tori are of the form $q_0^{4f} - 1$ or $(q_0^{2f} - 1) \times (q_0^{2f} - 1)$, but the eigenvalues of any element in such a torus either all have the same multiplicative order, or they occur in pairs having the same order. This contradiction rules out $\mathcal{C}_8$-subgroups of type $\mathrm{GU}_4(q^{1/2})$ in $\mathcal{M}$.

Next assume $H \in \mathcal{M}$ is a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_4(q)$. Now $(gs)^{e(q_0-1)}$ has eigenvalues $\{1, \xi, \xi^{q_0}, \xi^{q_0^2}\}$ for some $\xi \in \mathbb{F}_{q_0^3}$ of multiplicative order $q_0^2 + q_0 + 1$, but this is a contradiction since the nontrivial eigenvalues of semisimple elements in $H \cap G_0$ occur in pairs with the same multiplicative order. The same argument also rules out $\mathcal{C}_8$-subgroups of type $O_4^\epsilon(q)$.

Putting all this together, and applying Corollary 2.9 and Theorem 2.7, we deduce that if $z \in G$ has prime order then

$$\alpha(z) < 2q^{-1} + 2q^{-3} + \big(1 + (1 + \log(e))(q_0^3 - 1)\big) \cdot f(4, q)$$

with $f(4,q)$ defined in (15). If $e \geq 3$ then this bound implies that $\alpha(z) < 1/2$ (recall that we are assuming $q \geq 16$). Now, if $e = 2$ then by Proposition 2.16(ii) we may replace the term $(1+(1+\log(e))(q_0^3-1))$ in the above bound by $e^2 = 4$, and subsequently we deduce that $\alpha(z) < 0.187$ for all $q_0 \geq 4$. Finally, the reader can check that the above bounds imply that $\alpha(z) < q^{-1/4}$ for all $q > 27$, hence $u(G) \to \infty$ as $q \to \infty$. □

Proposition 4.7. *Theorem 4.1 holds when $n = 3$.*

Proof. If $q \leq 16$ then the result follows from Proposition 2.17, so let us assume $q \geq 25$. In fact, if $q \leq 49$ then the desired result can be verified using MAGMA, so we will assume $q > 49$. Set $y = [A,\mu] \in \mathrm{PGL}_3(q_0)$, where $A \in \mathrm{GL}_2(q_0)$ is irreducible of order q_0^2-1 and $\mu = \lambda^\alpha/\det(A)$, and fix $s \in G_0$ such that $(gs)^e$ is X-conjugate to y. As before, let $\mathcal{M}$ be the set of maximal subgroups of G containing gs. We claim that if $H \in \mathcal{M}$ then one of the following holds:

(i) H is a parabolic subgroup of type P_1 or P_2; $\mathcal{M}$ contains a unique subgroup of each type.

(ii) e is even and H is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_3$; there is a unique such subgroup in $\mathcal{M}$ if $q_0 \neq 2$, and there are at most 3 when $q_0 = 2$.

(iii) H is a subfield subgroup of type $\mathrm{GL}_3(q_1)$, where $q = q_1^a$ for some prime divisor a of e; for each q_1 there are at most $|C_{\mathrm{PGL}_3(q_0)}(y)| = q_0^2-1$ such subgroups in $\mathcal{M}$.

(iv) H is a $\mathcal{C}_8$-subgroup of type $\mathrm{GU}_3(q^{1/2})$ or $O_3(q)$. In both cases there are at most q_0^2-1 such subgroups in $\mathcal{M}$.

The argument here is very similar to the one given in the proof of the previous proposition, so we will only give details for $\mathcal{C}_2$ and $\mathcal{C}_9$ subgroups (note that in parts (iii) and (iv) we use Proposition 2.16(i) to bound the number of subgroups of the given type in $\mathcal{M}$).

Suppose $H \in \mathcal{M}$ is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_3$, say H preserves the decomposition $V = V_1 \oplus V_2 \oplus V_3$. If e is odd then $A \in \mathrm{GL}_2(q)$ is irreducible, so $(gs)^e$ must swap two of the V_i. Therefore $|(gs)^e|$ divides $2(q-1)$, but this is a contradiction since Lemma 4.3 implies that $(q_0^2-1, 2(q_0^e-1)) \leq 2q_0-2 < q_0^2-1$. Now assume e is even. If $q_0 = 2$ then Proposition 2.16(i) implies that there are at most $|C_{\mathrm{PGL}_3(q_0)}(y)| = 3$ subgroups of type $\mathrm{GL}_1(q) \wr S_3$ in $\mathcal{M}$, so let us assume $q_0 > 2$. Since e is even, the eigenvalues of $(gs)^e$ are in $\mathbb{F}_q$. Now $|(gs)^e| = q_0^2-1 > 3$ so either $(gs)^{2e}$ or $(gs)^{3e}$ fixes each V_i, hence the V_i are simply the (distinct) $\mathbb{F}_q$-eigenspaces of this element. It follows that there is a unique such subgroup in $\mathcal{M}$.

Finally, suppose $H \in \mathcal{M}$ is a $\mathcal{C}_9$-subgroup. Since $q \neq p$, the only possibility is $q = p^2$ (so $q_0 = p$ and $e = 2$), with $p \equiv 2,3 \pmod 5$ ($p \neq 3$), and H has socle A_6 (see [5, Table 7.4]). We are assuming $q > 49$, so the congruence condition implies that $q_0 \geq 13$. By considering the eigenvalues of $(gs)^2$ we deduce that $|(gs)^2| \geq 2q_0+2 \geq 28$, but no element in $\mathrm{Aut}(A_6)$ has order greater than 10, so there are no $\mathcal{C}_9$-subgroups in $\mathcal{M}$.

Let $z \in G$ be an element of prime order. By applying Theorem 2.7 and Lemma 2.10 we deduce that

$$\alpha(z) < 2q^{-1} + 2q^{-2} + \frac{(\log(e)+1)(q_0^2-1)+3d-3}{q^2+q+1} + \frac{2(3,q-1)(q_0^2-1)(d-1)}{q^{1/2}(q+1)},$$

where $d = (2,e)$. In particular, if $e \geq 3$ then $\alpha(z) < 1/2$ for all $q > 49$. Now assume $e = 2$. By applying Proposition 2.16(ii) we have

$$\alpha(z) < 2q^{-1} + 2q^{-2} + \frac{q+2}{q^2+q+1} + \frac{(3,q-1)(q+3)}{q^{1/2}(q+1)},$$

which is sufficient for all $q > 49$. In addition, we observe that $\alpha(z) < q^{-1/4}$ for all $q > 121$, whence $\alpha(z) \to 0$ as $q \to \infty$. □

Proposition 4.8. *Theorem 4.1 holds when $n = 2$.*

Proof. Here we may assume $q \geq 169$ (see Proposition 2.17). Let $y \in \mathrm{PGL}_2(q_0)$ be an irreducible element with determinant λ^α, and note that $|y| \geq (q_0+1)/(2, q_0-1)$. By Lemma 4.2, there exists $s \in G_0$ such that $(gs)^e$ and y are X-conjugate. As usual, let $\mathcal{M}$ be the set of maximal subgroups of G containing gs. We claim that if $H \in \mathcal{M}$ then one of the following holds:

(i) H is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_2$; either e is even, $q_0 \neq 3$ and there is a unique such subgroup in $\mathcal{M}$, or $q_0 = 3$ and there are at most 4.

(ii) H is a $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_1(q^2)$, and there is at most one subgroup of this type in $\mathcal{M}$.

(iii) H is a subfield subgroup of type $\mathrm{GL}_2(q_1)$, where $q = q_1^a$ for some prime divisor a of e. There are at most $q_0 + 1$ such subgroups in $\mathcal{M}$.

To see this, first observe that there are no reducible subgroups in $\mathcal{M}$ since y is irreducible, while the $\mathcal{C}_4$, $\mathcal{C}_6$, $\mathcal{C}_7$ and $\mathcal{C}_8$ families are empty. If H is a $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_1(q^2)$ then $\mathrm{fpr}(y, G/H) = 2/(q(q-1))$ and $[G : H] = q(q-1)/2$, so y (and thus gs) is contained in a unique $\mathcal{C}_3$-subgroup. As usual, the claim for subfield subgroups follows from Proposition 2.16(i) since $|C_{\mathrm{PGL}_2(q_0)}(y)| = q_0 + 1$.

Suppose $H \in \mathcal{M}$ is a $\mathcal{C}_9$-subgroup. Here the only possibility is $q = p^2$ (so $q_0 = p$ and $e = 2$), with $p \equiv \pm 3 \pmod{10}$ and H has socle A_5. As previously stated, we may assume $q_0 \geq 13$ and thus $|(gs)^e| \geq 7$. However, no element in S_5 has order greater than 6, so there are no such subgroups in $\mathcal{M}$.

Finally, suppose H is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_2$, say H preserves the decomposition $V = V_1 \oplus V_2$. If $q_0 = 3$ then Proposition 2.16(i) implies that there are at most $|C_{\mathrm{PGL}_2(q_0)}(y)| = 4$ subgroups of this type in $\mathcal{M}$, so let us assume $q_0 \neq 3$. If e is even then $(gs)^{2e}$ fixes each V_i, so V_1 and V_2 are the eigenspaces of $(gs)^{2e}$ (note that the eigenvalues are distinct since $q_0 \neq 3$) and thus $\mathcal{M}$ contains a unique subgroup of this type. Now assume e is odd. Here $(gs)^e$ must swap V_1 and V_2, so $|(gs)^e|$ divides $2(q-1)$. This is a contradiction if q_0 is even since $|(gs)^e| = q_0 + 1$. Now assume q_0 is odd, so $|(gs)^e| \geq (q_0+1)/2$. The previous divisibility condition implies that q_0 is a Mersenne prime. Therefore $2(q-1) \equiv 4 \pmod 8$ and thus the same divisibility criterion implies that $q_0 = 7$. Here a maximal $\mathcal{C}_2$-subgroup of $\mathrm{PGL}_2(q)$ is a dihedral group of order $2(7^e - 1)$. In particular, since $7^e - 1$ is indivisible by 4 (recall that e is odd), and the exponent of the dihedral group is $7^e - 1$, it follows that $(gs)^e$ is not contained in H.

Let $z \in G$ be an element of prime order and suppose $H \in \mathcal{M}$. According to [35, Theorem 1], either $\mathrm{fpr}(z, G/H) \leq 2/(q+1)$, or H is of type $\mathrm{GL}_2(q^{1/2})$ and

$$\mathrm{fpr}(z, G/H) \leq \frac{2 + q^{1/2}(q^{1/2}+1)}{q^{1/2}(q+1)}.$$

Therefore

$$\alpha(z) \leq \frac{2(q_0+1)(\log(e) + 2 - d) + 10}{q+1} + (d-1)(q_0+1) \cdot \left(\frac{2 + q^{1/2}(q^{1/2}+1)}{q^{1/2}(q+1)} \right)$$

for all $z \in G$ of prime order, where $d = (2, e)$. In particular, if $e \geq 3$ and $q \geq 169$ then $\alpha(z) < 1/2$ as required. Finally, if $e = 2$ (and $q \geq 169$ so $q_0 \neq 3$) then by applying Proposition 2.16(ii) we deduce that

$$\alpha(z) \leq \frac{4}{q+1} + 2 \left(\frac{2 + q^{1/2}(q^{1/2}+1)}{q^{1/2}(q+1)} \right) < 1/2.$$

In addition, the above bounds imply that $\alpha(z) < q^{-1/7}$ for all $q \geq 169$, whence $u(G) \to \infty$ as $q \to \infty$. □

This completes the proof of Theorem 4.1.

5. Graph-field automorphisms

Here $n \geq 3$ and $G = \langle G_0, g\rangle$ with $g = \iota\sigma x$, where ι is the inverse-transpose graph automorphism of G_0, σ is a standard field automorphism (of order $e > 1$) and $x \in \mathrm{PGL}_n(q)$. In particular, $q = q_0^e$ and we note that $\iota\sigma = \sigma\iota$. As before, we may replace x by $\delta = [\lambda, I_{n-1}]$ for some $\lambda \in \mathbb{F}_q^*$. The idea is to modify the approach used in the previous section, based on Shintani descent.

Let K be the algebraic closure of $\mathbb{F}_q$ and set $X = \mathrm{PSL}_n(K)$. We may view $\iota\sigma$ as a Frobenius morphism of X. As stated in Lemma 2.13, the associated Shintani map provides a bijective correspondence between the set of $X_{(\iota\sigma)^e}$-classes in the coset $\iota\sigma X_{(\iota\sigma)^e}$ and the set of $X_{\iota\sigma}$-classes in $X_{\iota\sigma} = \mathrm{PGU}_n(q_0)$. If e is even then $X_{(\iota\sigma)^e} = X_{\sigma^e} = \mathrm{PGL}_n(q)$ and we can proceed as in the previous section. However, if e is odd then we cannot realize $\mathrm{PGL}_n(q)$ as the set of fixed points in X of some power of $\iota\sigma$. Indeed, $X_{(\iota\sigma)^{2m+1}} = X_{\iota\sigma^{2m+1}} = \mathrm{PGU}_n(q_0^{2m+1})$ for all m. Therefore, a modified approach is required to handle this case.

The main result of this section is the following:

Theorem 5.1. *Let $G_0 = \mathrm{PSL}_n(q)$ and $G = \langle G_0, g\rangle$, where $n \geq 3$ and $g = \iota\sigma x$ is the product of the inverse-transpose graph automorphism ι, a standard field automorphism σ of order $e > 1$ and $x \in \mathrm{PGL}_n(q)$. If we assume $G \neq \mathrm{PSL}_3(4).2_1$ then there exists $s \in G_0$ such that*

$$\sum_{H \in \mathcal{M}(gs)} \mathrm{fpr}(z, G/H) < 1/2 \tag{17}$$

for all $z \in G$ of prime order. In particular, $u(G) \geq 2$ for all G. Moreover, $u(G)$ is bounded as $|G| \to \infty$ if and only if q is bounded and ne is odd.

Remark 5.2. The excluded case $G = \mathrm{PSL}_3(4).2_1$ is a genuine exception to the bound in (17), but it is easy to check that $u(G) \geq 2$ (see Proposition 2.18).

As previously remarked, the analysis here depends on the parity of e (where e is the order of the field automorphism σ involved in g).

5.1. σ has even order.

Let f be the Shintani map from the set of $\mathrm{PGL}_n(q)$-classes in the coset $\iota\sigma\mathrm{PGL}_n(q)$ to the set of $\mathrm{PGU}_n(q_0)$-classes in $\mathrm{PGU}_n(q_0)$. We start with an analogue of Lemma 4.2.

Lemma 5.3. *With the notation above, let $\alpha = -(q-1)/(q_0+1)$ and suppose $y \in \mathrm{PGU}_n(q_0)$ has determinant λ^α. Then there exists $s \in G_0$ such that $f(gs)$ is $\mathrm{PGU}_n(q_0)$-conjugate to y.*

Proof. Since f is a bijection, the $\mathrm{PGU}_n(q_0)$-class of y corresponds to the $\mathrm{PGL}_n(q)$-class of $\iota\sigma t$ for some $t \in \mathrm{PGL}_n(q)$. Let μ be the determinant of t and fix a generator ω for $\mathbb{F}_q^*$. Now

$$(\iota\sigma t)^e = t^{(\iota\sigma)^{e-1}} t^{(\iota\sigma)^{e-2}} \cdots t^{\iota\sigma} t$$

and $\det t^{(\iota\sigma)^j} = \mu^{(-q_0)^j}$, so $f(\iota\sigma t)$ has determinant μ^α. Since $f(\iota\sigma t)$ and y are $\mathrm{PGU}_n(q_0)$-conjugate, it follows that $\mu^\alpha = \lambda^\alpha$ and thus $\mu = \omega^{(q_0+1)j}\lambda$ for some integer $0 \leq j < \alpha$. Let $x \in \mathrm{PGL}_n(q)$ be an element with determinant ω^{-j}. Then $(\iota\sigma t)^x = \iota\sigma x^{-\iota\sigma} t x$ and $x^{-\iota\sigma} t x$ has determinant λ. Therefore $x^{-\iota\sigma} t x \in \delta G_0$, so there exists $s \in G_0$ such that $\iota\sigma x^{-\iota\sigma} t x = \iota\sigma\delta s = gs \in G$ corresponds to y under the Shintani correspondence. □

Proposition 5.4. *Theorem 5.1 holds when e is even and $n \geq 5$.*

Proof. This is very similar to the proof of Proposition 4.4. Set $y = [A, B] \in \mathrm{PGU}_n(q_0)$, where $A \in \mathrm{GU}_{n-2}(q_0)$ is a regular semisimple element of order $(q_0^{n-2} - (-1)^n)|\lambda^\alpha|/(q_0+1)$ and determinant λ^α (here $\alpha = -(q-1)/(q_0+1)$, as in Lemma 5.3), and $B \in \mathrm{GU}_2(q_0)$ is a unitary transvection. Note that if n is odd then A is irreducible over $\mathbb{F}_{q_0^2}$, while A splits into two irreducible blocks of dimension $n/2-1$ when n is even. Since A (and therefore y) has determinant λ^α, a combination of Lemmas 2.13 and 5.3 implies that there exists $s \in G_0$ such that $(gs)^e$ and y are X-conjugate. If $(n, q) = (6, 4)$ then Proposition 2.17 applies, so we may assume $(n, q) \neq (6, 4)$.

To determine the subgroups in $\mathcal{M} = \mathcal{M}(gs)$ we proceed as in the proof of Lemma 4.5. First observe that a suitable power of $(gs)^e$ is a transvection; this immediately eliminates the subgroups in the $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_6$, $\mathcal{C}_7$ and $\mathcal{C}_9$ collections, and we can also rule out $\mathcal{C}_8$-subgroups of type $O_n^\epsilon(q)$ for the same reason.

Next let us turn to the $\mathcal{C}_1$-subgroups in $\mathcal{M}$. First note that y is contained in a unique maximal parabolic subgroup of $\mathrm{PGU}_n(q_0)$ of type P_1, and also a unique subgroup of type $\mathrm{GU}_2(q_0) \perp \mathrm{GU}_{n-2}(q_0)$ (the stabilizer of a non-degenerate 2-space). In addition, if n is even then y is contained in exactly two subgroups of type $P_{n/2-1}$, and two of type $P_{n/2}$. By applying Corollary 2.15 we deduce that the $\mathcal{C}_1$-subgroups in $\mathcal{M}$ are as follows: one each of type $P_{1,n-1}$ and $\mathrm{GL}_2(q) \times \mathrm{GL}_{n-2}(q)$, in addition to two each of type $P_{n/2-1,n/2+1}$ and $P_{n/2}$ when n is even. (Recall that $P_{i,j}$ denotes the G-stabilizer of a pair of subspaces $U \subseteq W$ of V, where $\dim U = i$, $\dim W = j$ and $i + j = n$; such subgroups are maximal in G whenever $G \not\leqslant \mathrm{P\Gamma L}_n(q)$.)

Let us explain in more detail how Corollary 2.15 applies in this situation. Let Y be a parabolic subgroup of type $P_{1,n-1}$ of the algebraic group $X = \mathrm{PSL}_n(\overline{\mathbb{F}}_q)$. Recall that e is even so we have $(\iota\sigma)^e = \sigma^e$. Now Corollary 2.15 implies that the number of $X_{\sigma^e} = \mathrm{PGL}_n(q)$-conjugates of Y_{σ^e} (a type $P_{1,n-1}$ parabolic subgroup of $\mathrm{PGL}_n(q)$) normalized by $\iota\sigma s$ is equal to the number of $X_{\iota\sigma} = \mathrm{PGU}_n(q_0)$-conjugates of $Y_{\iota\sigma}$ (a type P_1 parabolic subgroup of $\mathrm{PGU}_n(q_0)$) containing $f(\iota\sigma s)$. We have already observed that $f(\iota\sigma s)$ is contained in a unique P_1 parabolic subgroup of $\mathrm{PGU}_n(q_0)$, so there is only one subgroup of type $P_{1,n-1}$ in $\mathcal{M}$. Similarly, suppose that Y is a Levi subgroup of X of type $A_1A_{n-3}T_1$. Then Y_{σ^e} is a type $\mathrm{GL}_2(q) \times \mathrm{GL}_{n-2}(q)$ subgroup of $X_{\sigma^e} = \mathrm{PGL}_n(q)$ and $Y_{\iota\sigma}$ is a type $\mathrm{GU}_2(q_0) \times \mathrm{GU}_{n-2}(q_0)$ subgroup of $X_{\iota\sigma} = \mathrm{PGU}_n(q_0)$. Since $f(\iota\sigma s) \in \mathrm{PGU}_n(q_0)$ is contained in only one such subgroup, Corollary 2.15 implies that there is only one subgroup of $\mathrm{PGL}_n(q)$ of type $\mathrm{GL}_2(q) \times \mathrm{GL}_{n-2}(q)$ normalized by $\iota\sigma s$. The other cases are similar.

Now assume $H \in \mathcal{M}$ is a $\mathcal{C}_2$-subgroup. By arguing as in the proof of Lemma 4.5, we deduce that one of the following holds:

(i) H is of type $\mathrm{GL}_2(q) \wr S_{n/2}$ and $e \geq (n-2)/2$; there is at most one subgroup of this type in $\mathcal{M}$;
(ii) H is of type $\mathrm{GL}_1(q) \wr S_n$, q is even, and $e \geq n-2$; there are at most $q_0/2$ subgroups of this type in $\mathcal{M}$.

Next suppose that H is a $\mathcal{C}_5$-subgroup of type $\mathrm{GL}_n(q_1)$, where $q = q_1^r$ for a prime r (as before, we note that r divides e). If $e \geq 3$ then Proposition 2.16(i) implies that for each relevant prime r there are at most $|C_{\mathrm{PGU}_n(q_0)}(y)| \leq q_0(q_0^{n-2}+1)$ distinct $\mathcal{C}_5$-subgroups in $\mathcal{M}$. Now assume $e = 2$, so $r = 2$ and n is even. We claim that there are no $\mathcal{C}_5$-subgroups in $\mathcal{M}$. To see this, first note that the set of eigenvalues of $(gs)^e$ is of the form

$$\mathcal{E} = \{1, \omega^k, \omega^{-q_0 k}, \omega^{q_0^2 k}, \ldots, \omega^{(-q_0)^{n-3}k}\},$$

where $\mathbb{F}^*_{q_0^{n-2}} = \langle \omega \rangle$ and $k = (q_0+1)/|\lambda^\alpha|$ (with $\alpha = -(q-1)/(q_0+1)$ as before). Now, if $(gs)^e$ is contained in a $\mathcal{C}_5$-subgroup of type $\mathrm{GL}_n(q_0)$ then $\omega^{q_0 k}$ is an eigenvalue of $(gs)^e$, so $\omega^{q_0 k} = \omega^{(-q_0)^j k}$ for some $0 \leq j \leq n-3$, and thus $q_0^{n-2}-1$ divides $k(q_0-(-q_0)^j)$. However, if $j \leq n-4$ then $|k(q_0-(-q_0)^j)| < q_0^{n-2}-1$, which is a contradiction. Similarly, if $j = n-3$ and $|\lambda^\alpha| \neq 1$ then $k \leq (q_0+1)/2$ and $|k(q_0-(-q_0)^j)| < q_0^{n-2}-1$, whereas if $|\lambda^\alpha| = 1$ then $k(q_0-(-q_0)^j) = (q_0+1)(q_0+q_0^{n-3})$ is clearly indivisible by $q_0^{n-2}-1$ (recall that we may assume $(n,q) \neq (6,4)$). This justifies the claim.

To complete the analysis of the subgroups in $\mathcal{M}$, we may assume H is a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_n(q)$ or $\mathrm{GU}_n(q^{1/2})$. By Proposition 2.16(i), there are at most $|C_{\mathrm{PGU}_n(q_0)}(y)| \leq q_0(q_0^{n-2}+1)$ subgroups of type $\mathrm{GU}_n(q^{1/2})$ in $\mathcal{M}$, but we claim that there are none of type $\mathrm{Sp}_n(q)$. To see this, suppose n is even and let $\mathcal{E}$ be the set of eigenvalues of $(gs)^e$ as above. Now $(gs)^e \in \mathrm{PGSp}_n(q)$ and thus $(gs)^{2e} \in \mathrm{PSp}_n(q)$, so ω^{-2k} is an eigenvalue of $(gs)^{2e}$. Therefore $\omega^{-2k} = \omega^{2k(-q_0)^j}$ for some $0 \leq j \leq n-3$, so $q_0^{n-2}-1$ divides $2k(-q_0)^j + 2k$ and thus $(q_0^{n-2}-1, 2k(q_0^j+(-1)^j)) = q_0^{n-2}-1$. However,

$$(q_0^{n-2}-1, 2k(q_0^j+(-1)^j)) \leq 2k(q_0^{n-2}-1, q_0^j+(-1)^j) \leq 2(q_0+1)(q_0^{n-2}-1, q_0^j+(-1)^j)$$

and Lemma 4.3 implies that this upper bound is less than $q_0^{n-2}-1$, which is a contradiction. For example, if j is even then Lemma 4.3 yields

$$2(q_0+1)(q_0^{n-2}-1, q_0^j+(-1)^j) = 2(q_0+1)(q_0^{n-2}-1, q_0^j+1) \leq 2(q_0+1)(q_0^{(n-2,j)}+1)$$

and we have $2(q_0+1)(q_0^{(n-2,j)}+1) < q_0^{n-2}-1$ since $(n-2,j) \leq (n-2)/2$. We conclude that there are no $\mathcal{C}_8$-subgroups of type $\mathrm{Sp}_n(q)$ in $\mathcal{M}$.

Let $z \in G$ be an element of prime order and define $\alpha(z)$ as in (14). By applying Theorem 2.7, we deduce that the contribution to $\alpha(z)$ from the subgroups in $\mathcal{C}_1$ is less than

$$q^{-1} + q^{1-n} + 2q^{-2} + ((n,2)-1)(4q^{1-n/2} + 4q^{-n/2}),$$

while Corollary 2.9 indicates that the remaining contribution is less than

$$\left((n,2) - 1 + \frac{1}{2}q_0((q,2)-1) + q_0(q_0^{n-2}+1)\left(1+(1-\delta_{2,e})(\log(e)+1)\right)\right) \cdot f(n,q),$$

where $f(n,q)$ is given in (15). For $n \geq 5$, it is straightforward to check that these bounds imply that $\alpha(z) < 1/2$ unless

$$(n,q) \in \{(8,4),(7,4),(6,4),(5,9),(5,4)\}.$$

In addition, we note that the above bounds immediately imply that $\alpha(z) \to 0$ as $q \to \infty$ (for any $n \geq 5$), whence $u(G) \to \infty$ as $q \to \infty$.

The cases $(n,q) = (5,4),(6,4)$ are dealt with in Proposition 2.17. To deal with the remaining cases, it is helpful to note that if H is a maximal subgroup of type $\mathrm{GU}_n(q_0)$ then $\mathrm{fpr}(z, G/H) \leq \beta(n,q)$ for all $z \in G$ of prime order, where $\beta(n,q)$ is defined as follows:

(n,q)	$(8,4)$	$(7,4)$	$(5,9)$
$\beta(n,q)$	$1/32639$	$1/8128$	$1/9801$

Armed with these bounds, the desired result quickly follows. For example, suppose $(n,q) = (5,9)$. As above, the $\mathcal{C}_1$ contribution is less than $9^{-1}+9^{-4}+2\cdot 9^{-2}$; the only other subgroups in $\mathcal{M}$ are of type $\mathrm{GU}_5(3)$, and thus

$$\alpha(z) < 9^{-1} + 9^{-4} + 2 \cdot 9^{-2} + 3(3^3+1)/9801 < 1/2.$$

Similarly, we get $\alpha(z) < 1/2$ when $(n,q) = (8,4)$ or $(7,4)$.

To complete the proof of Proposition 5.4, it remains to show that $u(G) \to \infty$ when q is bounded and n tends to infinity. As in the proof of Proposition 4.4, let k be an integer such that $n/4 < k < n/2$, $n-k$ is odd and $(n,k) = (n-k,e) = 1$. We may assume n is

large. Set $y = [A, B] \in \mathrm{PGU}_n(q_0)$, where $A \in \mathrm{GU}_{n-k}(q_0)$ is irreducible of order a multiple of $q_0^{n-k}+1$, and $B \in \mathrm{GU}_k(q_0)$ has order a multiple of $q_0^k-(-1)^k$ (B is irreducible when k is odd, otherwise B splits into two irreducible blocks). Note that $|C_{\mathrm{PGU}_n(q_0)}(y)| < 2q_0^{n-1}$. Since $(n-k,e)=1$, some power of y has order r, where r is either a primitive prime divisor of $q^{n-k}-1$ with $r > 2(n-k)+1$, or r is a product of primitive prime divisors of $q^{n-k}-1$. Therefore, since $n-k$ is odd, by applying Theorem 2.12 and Corollary 2.15 we deduce that the possibilities for $H \in \mathcal{M}$ are as follows (we use Proposition 2.16 to bound the number of irreducible subgroups in $\mathcal{M}$ of a given type):

(i) H is of type $\mathrm{GL}_k(q) \times \mathrm{GL}_{n-k}(q)$; there is a unique such subgroup in $\mathcal{M}$.
(ii) H is of type $P_{k/2,n-k/2}$ and n is odd; there are at most two such subgroups in $\mathcal{M}$.
(iii) H is of type $\mathrm{GL}_n(q_1)$, where $q = q_1^a$ for some prime divisor a of e; for a given a, there are less than $2q_0^{n-1}$ such subgroups in $\mathcal{M}$.
(iv) H is of type $\mathrm{GU}_n(q^{1/2})$; there are less than $2q_0^{n-1}$ such subgroups in $\mathcal{M}$.

(Note that there are no subgroups of type $\mathrm{Sp}_n(q)$ or $O_n^\epsilon(q)$ in $\mathcal{M}$ since y acts irreducibly on a subspace of V of odd dimension $n-k > n/2$.)

Let $z \in G$ be an element of prime order. In the usual way we calculate that

$$\alpha(z) < 2q^{-n/4} + 4q^{-n/8} + 2(\log(e)+2)q_0^{n-1} \cdot f(n,q),$$

hence $\alpha(z) \to 0$ as $n \to \infty$, as required. □

Proposition 5.5. *Theorem 5.1 holds when e is even and $n = 4$.*

Proof. If $q \leq 9$ then Proposition 2.17 applies, so we may assume $q \geq 16$. Set $y = [A, B] \in \mathrm{PGU}_4(q_0)$, where $A \in \mathrm{GU}_3(q_0)$ is irreducible of order q_0^3+1 and $B \in \mathrm{GU}_1(q_0)$. As usual, let $\mathcal{M}$ denote the set of maximal subgroups of G containing gs, and note that there is a unique reducible subgroup in $\mathcal{M}$ (of type $\mathrm{GL}_1(q) \times \mathrm{GL}_3(q)$). Also, since $q \neq p$, we note that G has no maximal $\mathcal{C}_9$-subgroups (see [5, Table 7.9]).

First assume e is divisible by 3. Since e is even, it follows that $e \geq 6$ and thus $q \geq 64$. It is easy to see that there are no $\mathcal{C}_4$, $\mathcal{C}_6$ or $\mathcal{C}_7$-subgroups in $\mathcal{M}$. In addition, we can eliminate $\mathcal{C}_3$-subgroups, and also $\mathcal{C}_8$-subgroups of type $\mathrm{Sp}_4(q)$ or $O_4^\epsilon(q)$, because exactly three of the eigenvalues of y have the same multiplicative order. For the remaining $\mathcal{C}_2$, $\mathcal{C}_5$ and $\mathcal{C}_8$-subgroups of G, Proposition 2.16(i) implies that there are at most $|C_{\mathrm{PGU}_4(q_0)}(y)| = q_0^3+1$ subgroups of a given type in $\mathcal{M}$. Therefore, by applying Theorem 2.7, we deduce that

$$\alpha(z) < q^{-1} + q^{-3} + (4+\log(e))(q_0^3+1) \cdot f(4,q) < 1/2 \tag{18}$$

for all q, and we also observe that $\alpha(z) \to 0$ as $q \to \infty$.

For the remainder of the proof we will assume e is indivisible by 3. Now $|(gs)^e|$ is divisible by $(q_0^3+1)/(q_0+1)$, so every primitive prime divisor of q_0^6-1 divides $|(gs)^e|$. Moreover, since e is indivisible by 3, such a prime is a primitive prime divisor of q^3-1. In particular, if $q_0 \notin \{2,3,5\}$ then [23, Lemma 2.1] implies that some power of $(gs)^e$ has order r, where r is either a primitive prime divisor of q^3-1 with $r > 7$, or r is a product of primitive prime divisors of q^3-1. Therefore, in these cases we can use Theorem 2.12 to determine the subgroups in $\mathcal{M}$.

Suppose $q_0 \notin \{2,3,5\}$. Since y acts irreducibly on a 3-dimensional subspace of V it follows that there are no $\mathcal{C}_8$-subgroups of type $\mathrm{Sp}_4(q)$ or $O_4^\epsilon(q)$ in $\mathcal{M}$. Therefore

$$\alpha(z) < q^{-1} + q^{-3} + (\log(e)+2)(q_0^3+1) \cdot f(4,q)$$

and one can check that this bound is sufficient if $e \geq 4$. Now assume $e = 2$. Here the proof of Proposition 2.16(ii) reveals that there are at most $e^2 = 4$ subgroups of type $\mathrm{GU}_4(q_0)$

in $\mathcal{M}$, and we note that there are no $\mathcal{C}_5$-subgroups since $\mathrm{PGL}_4(q_0)$ does not contain any elements of order $|(gs)^2|$. Therefore

$$\alpha(z) < q^{-1} + q^{-3} + 4 \cdot f(4,q) < 1/2. \tag{19}$$

To complete the proof we may assume $q_0 \in \{2,3,5\}$ and e is indivisible by 3. If $e \geq 4$ then it is easy to check that (18) applies, so we reduce to the case $q = 25$. Here a power of $(gs)^2$ has order 7 (a primitive prime divisor of $25^3 - 1$) and by inspecting [24] we deduce that every irreducible subgroup $H \in \mathcal{M}$ is of type $\mathrm{GU}_4(3)$. Therefore (19) holds and the result follows. □

Proposition 5.6. *Theorem 5.1 holds when e is even and $n = 3$.*

Proof. This is similar to the proof of the previous proposition. In view of Proposition 2.17, we may assume $q \geq 25$. Let $y \in \mathrm{PGU}_3(q_0)$ be an irreducible element of order a multiple of $(q_0^3+1)/(q_0+1)$ and define $\mathcal{M}$ as before. Note that there are no reducible subgroups in $\mathcal{M}$.

If e is a multiple of 3 then by arguing as in the proof of Proposition 5.5, using Lemma 2.10 and Proposition 2.16(i), noting that $|C_{\mathrm{PGU}_3(q_0)}(y)| = q_0^2 - q_0 + 1$, we have

$$\alpha(z) < (q_0^2 - q_0 + 1)\left(\frac{(3,q-1)}{q^{1/2}(q+1)} + \frac{\log(e)+3}{q^2+q+1}\right) < 1/2 \tag{20}$$

and the result follows. For the remainder, let us assume e is indivisible by 3.

Suppose $q_0 \notin \{2,3,5\}$. Then as in the proof of Proposition 5.5, some power of $(gs)^e$ has order r, where r is either a primitive prime divisor of $q^3 - 1$ with $r > 7$, or r is a product of primitive prime divisors of $q^3 - 1$. In particular, if $H \in \mathcal{M}$ then Theorem 2.12 implies that H is of type $\mathrm{GL}_1(q^3)$, $\mathrm{GU}_3(q^{1/2})$ or $\mathrm{GL}_3(q_1)$. Moreover, if $H \in \mathcal{M}$ is of type $\mathrm{GL}_1(q^3)$ then $H \leqslant C_G((gs)^e)$, so there is a unique such subgroup in $\mathcal{M}$ (because $(gs)^e$ is contained in a unique maximal torus of $C_G((gs)^e)$). Now, if $e \geq 4$ then Lemma 2.10 implies that

$$\alpha(z) < (q_0^2 - q_0 + 1)\left(\frac{2(3,q-1)}{q^{1/2}(q+1)} + \frac{\log(e)}{q^2+q+1}\right) + \frac{1}{q^2+q+1} < 1/2.$$

Similarly, if $e = 2$ then the proof of Proposition 2.16(ii) implies that $\mathcal{M}$ contains at most 2 subgroups of type $\mathrm{GU}_3(q^{1/2})$ and thus

$$\alpha(z) \leq \frac{2(3,q-1)}{q^{1/2}(q+1)} + \frac{1}{q^2+q+1} < 1/2 \tag{21}$$

for all $q \geq 25$ (note that there are no subfield subgroups in $\mathcal{M}$ when $e = 2$).

Finally, suppose $q_0 \in \{2,3,5\}$ and e is indivisible by 3. If $e \geq 4$ then (20) applies, so we reduce to the case $q = 25$. Here we obtain the same list of subgroups in $\mathcal{M}$ as in the previous paragraph, using [24] and [5, Table 7.4], so (21) holds and the result follows. □

5.2. σ **has odd order.** As before, let $K = \overline{\mathbb{F}}_q$, $X = \mathrm{PSL}_n(K)$ and recall that we may assume that $g = \iota\sigma\delta$, where $\delta = [\lambda, I_{n-1}]$. We claim that g has order $2e$, which implies that g is $\mathrm{PGL}_n(q)$-conjugate to $\iota\sigma$ (see [20, 7.2]). To see this, first note that the order of g is certainly a multiple of $2e$. Now an easy calculation shows that

$$(\iota\sigma\delta)^2 = \sigma^2\delta^{-\sigma}\delta = \sigma^2[\lambda^{1-q_0}, I_{n-1}].$$

In particular, if we set $\mu = [\lambda^{1-q_0}, I_{n-1}]$ then

$$(\iota\sigma\delta)^{2e} = (\sigma^2\mu)^e = \mu^{\sigma^{2e-2}}\mu^{\sigma^{2e-4}}\cdots\mu^{\sigma^2}\mu.$$

However, since e is odd and $\mu^{\sigma^e} = \mu$, this is equal to

$$\mu^{\sigma^{e-1}}\mu^{\sigma^{e-2}}\cdots\mu^{\sigma}\mu = [\lambda^{(1-q_0)(q_0^{e-1}+q_0^{e-2}+\cdots+1)}, I_{n-1}] = 1.$$

This justifies the claim. Therefore we may assume that $g = \iota\sigma$.

Let γ be the standard involutory graph automorphism of X induced from the order-two symmetry of the corresponding Dynkin diagram of type A_{n-1}. Set $Y = C_X(\gamma)$ and note that $Y = \mathrm{PSO}_n(K)$ or $\mathrm{PSp}_n(K)$ when n is odd or even, respectively (see [21, Theorem 1.15.2(d)]. In particular, Y is a simple algebraic group and we can use the tools of Shintani descent. To do this, consider the Frobenius morphism σ of X restricted to Y and note that

$$Y_{\sigma^e} = C_{X_{\sigma^e}}(\gamma) = \begin{cases} \mathrm{PGSp}_n(q) & \text{if } n \text{ is even;} \\ \mathrm{PSO}_n(q) = \mathrm{PO}_n(q) & \text{otherwise.} \end{cases}$$

Now $\iota\sigma$ is $\mathrm{PGL}_n(q)$-conjugate to $\gamma\sigma$, so let us assume that $g = \gamma\sigma$. Note that $\gamma\sigma = \sigma\gamma$.

By the theory of Shintani descent (see Lemma 2.13), there is a bijective map f between the set of Y_{σ^e}-classes in the coset σY_{σ^e} and the set of Y_σ-classes in Y_σ. Moreover, by arguing as in the proof of Lemma 4.2 we deduce that if $y \in Y_\sigma$ has determinant 1 then there exists $s \in Y_{\sigma^e}$ such that $\det(s) = 1$ and $f(\sigma s) = y$ (i.e. f maps the Y_{σ^e}-class of σs to the Y_σ-class of y). Now σs commutes with γ, so $(\gamma\sigma s)^{2e}$ is conjugate to y^2. Therefore, if $y \in \mathrm{PSp}_n(q_0)$ or $\mathrm{PSO}_n(q_0)$, in the cases n even and odd respectively, then there exists $s \in G_0$ such that $(gs)^{2e}$ is conjugate to y^2. Moreover, since $(\gamma\sigma s)^2 = \sigma^2 s^\sigma s$ and σ^2 acts as a field automorphism of order e on $\mathrm{PGL}_n(q)$ (since e is odd), we can use Corollary 2.15 and Proposition 2.16 to control the maximal subgroups of G containing y^2.

Lemma 5.7. *With the notation above, suppose $y \in \mathrm{PSp}_n(q_0)$ or $\mathrm{PSO}_n(q_0)$ in the respective cases n even and n odd, and fix an element $s \in G_0$ such that $(gs)^{2e}$ is Y-conjugate to y^2. Let $\mathcal{M}$ be the set of maximal subgroups of G containing gs and assume $e \geq 3$ is odd. Then the following hold:*

(i) *There are at most $|C_{\mathrm{PGL}_n(q_0)}(y^2)|$ distinct subgroups in $\mathcal{M}$ of a given type.*

(ii) *More precisely, the number of $\mathcal{C}_1$-subgroups in $\mathcal{M}$ of a given type (either $P_{n/2}$, $P_{i,n-i}$ or $\mathrm{GL}_i(q) \times \mathrm{GL}_{n-i}(q)$) is at most the number of reducible subgroups of the same type in $\mathrm{PGL}_n(q_0)$ containing y^2.*

Proof. First consider (i). Set $G_1 = \langle \mathrm{PGL}_n(q), \gamma\sigma \rangle$ and note that all subgroups $H \in \mathcal{M}$ of a given type are G_1-conjugate. Let H be a maximal subgroup of G containing $\gamma\sigma s$ and let N be the number of subgroups of type H in $\mathcal{M}$. Then H also contains $(\gamma\sigma s)^2 = \sigma^2 t$, where $t = s^\sigma s$, so

$$N \leq \frac{|(\sigma^2 t)^{G_1} \cap H|}{|(\sigma^2 t)^{G_1}|} \cdot \frac{|G_1|}{|H|}.$$

Further, since $|(\sigma^2 t)^{G_1} \cap H| \leq |H|/e$, we have

$$N \leq |C_{G_1}(\sigma^2 t)|/e = |C_{G_1}((\sigma s)^2)|/e.$$

Next let j be an integer such that $2j \equiv 1 \pmod{e}$ and $(j, |G|) = 1$. (For instance, let j be a solution to the system of congruences $j \equiv a \pmod{e}$ (where a is the multiplicative inverse of 2 in $\mathbb{Z}/e\mathbb{Z}$) and $j \equiv 1 \pmod{p_i}$ for all prime divisors p_i of $|G|$ with $(p_i, e) = 1$; a solution exists by the Chinese remainder theorem.) Now

$$C_{G_1}((\sigma s)^2) \leqslant C_{G_1}((\sigma s)^{2j})$$

(in fact equality holds) and $(\sigma s)^{2j} \in \sigma\mathrm{PGL}_n(q)$, so Lemma 2.13(i) implies that

$$|C_{G_1}((\sigma s)^{2j})| = e|C_{\mathrm{PGL}_n(q_0)}(b(\sigma s)^{2je}b^{-1})|$$

for some $b \in X$. Since $(j, |G|) = 1$, there exists an integer k such that $jk \equiv 1 \pmod{|G|}$ and we deduce that

$$e|C_{\mathrm{PGL}_n(q_0)}(b(\sigma s)^{2je}b^{-1})| \leq e|C_{\mathrm{PGL}_n(q_0)}(b(\sigma s)^{2jke}b^{-1})| = e|C_{\mathrm{PGL}_n(q_0)}(b(\sigma s)^{2e}b^{-1})|.$$

However, $b(\sigma s)^{2e}b^{-1}$ and y^2 are $\mathrm{PGL}_n(q_0)$-conjugate, so

$$e|C_{\mathrm{PGL}_n(q_0)}(b(\sigma s)^{2e}b^{-1})| = e|C_{\mathrm{PGL}_n(q_0)}(y^2)|$$

and the result follows.

Finally let us turn to (ii). Define the integers j and k as above. Let H be a maximal $\mathcal{C}_1$-subgroup of G containing $\gamma\sigma s$, of type T say. Then $(\gamma\sigma s)^2 = (\sigma s)^2 \in H$, hence $(\sigma s)^{2j} \in H$. Since $(\sigma s)^{2j} \in \sigma\mathrm{PGL}_n(q)$, Corollary 2.15 implies that the number of subgroups of G of type T containing $(\sigma s)^{2j}$ is the same as the number of subgroups of type T in $\mathrm{PGL}_n(q_0)$ containing $b(\sigma s)^{2je}b^{-1}$. But any such subgroup containing $b(\sigma s)^{2je}b^{-1}$ also contains $b(\sigma s)^{2jke}b^{-1}$, and this element is $\mathrm{PGL}_n(q_0)$-conjugate to y^2. This completes the proof of the lemma. □

We now partition the proof of Theorem 5.1 (with e odd) into several subcases. To do this, let us first define two sets of special cases (n, q_0), which we will consider separately:

$$\mathcal{A} = \{(5,2),(5,3),(7,2),(7,3),(9,2),(11,2),(13,2),(15,2)\};$$
$$\mathcal{B} = \{(4,2),(4,3),(6,2),(6,3),(8,2),(10,2),(12,2),(14,2)\}.$$

We start by assuming $n \geq 5$ is odd.

Proposition 5.8. *Theorem 5.1 holds when e is odd, $n \geq 5$ is odd and $(n, q_0) \notin \mathcal{A}$.*

Proof. Let $n = 2^{k_1} + 2^{k_2} + \cdots + 1$ be the binary representation of n (where $k_i > k_{i+1}$ for all i) and note that $2^{k_1} > n/2$. Set $y = [A_{2^{k_1}}, A_{2^{k_2}}, \ldots, A_1] \in \mathrm{PSO}_n(q_0)$, where $A_1 \in \mathbb{F}_{q_0}^*$ and each $A_m \in O_m^-(q_0)$ (with $m > 1$) is irreducible of order $q_0^{m/2} + 1$. Since $\det(y) = 1$ there exists $s \in G_0$ such that $(gs)^{2e}$ and y^2 are conjugate. As usual, let $\mathcal{M}$ be the set of maximal subgroups of G containing gs.

The order of some power of y is a primitive prime divisor of $q_0^{2^{k_1}} - 1$. Moreover, since e is odd and $(n, q_0) \notin \mathcal{A}$, [23, Lemma 2.1] implies that some power of y has order r, where either r is a primitive prime divisor of $q^{2^{k_1}} - 1$ with $r > 2^{k_1+1} + 1$, or r is a product of primitive prime divisors of $q^{2^{k_1}} - 1$. Therefore, we can use Theorem 2.12 to restrict the possible subgroups in $\mathcal{M}$. Furthermore, each $H \in \mathcal{M}$ contains a conjugate of y^2 and so by studying the maximal subgroups of G containing y^2, we can further restrict the possibilities in $\mathcal{M}$.

By Lemma 5.7(ii), the maximal $\mathcal{C}_1$-subgroups containing y^2 are as follows: one each of type $P_{1,n-1}$ and $\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$, together with at most one of type $P_{j,n-j}$ and also at most one of type $\mathrm{GL}_j(q) \times \mathrm{GL}_{n-j}(q)$ for all $2 \leq j < n/2$. In particular, by applying Theorem 2.7 we deduce that the entire contribution to $\alpha(z)$ from reducible subgroups is less than

$$2q^{-1} + 2q^{1-n} + \sum_{j \geq 2} 4q^{-j} = 2q^{-1} + 2q^{1-n} + 4/(q^2 - q).$$

Now assume $H \in \mathcal{M}$ is irreducible. In view of Theorem 2.12, it follows that H is a $\mathcal{C}_3$, $\mathcal{C}_5$ or $\mathcal{C}_8$ subgroup of G. We can immediately eliminate $\mathcal{C}_3$-subgroups since y^2 has only one eigenvalue in $\mathbb{F}_{q_0}$. Similarly, there are no $\mathcal{C}_8$-subgroups of type $\mathrm{GU}_n(q^{1/2})$ since y^2 acts irreducibly on a 2^{k_1}-dimensional subspace of V. By applying Lemma 5.7 we see that $\mathcal{M}$ contains at most $|C_{\mathrm{PGL}_n(q_0)}(y^2)| < q_0^{n-1}$ subfield subgroups for each prime divisor of e, and at most the same number of $\mathcal{C}_8$-subgroups of type $O_n(q)$ (when q is odd).

Therefore, if $z \in G$ has prime order then

$$\alpha(z) < 2q^{-1} + 2q^{1-n} + 4/(q^2 - q) + q^{(n-1)/e}((2, q-1) + \log(e)) \cdot f(n, q), \qquad (22)$$

which is less than $1/2$ (note that $(n, q) \neq (5, 8)$ since we are assuming $(n, q_0) \notin \mathcal{A}$).

From the previous bound it is clear that $\alpha(z) \to 0$ as $q \to \infty$, so the asymptotic statement in Theorem 5.1 also holds. However, we claim that if q is bounded then $\alpha(z)$ does *not* tend to zero as $n \to \infty$. To do this we will prove that if ne is odd then *every* $gs \in g\mathrm{PGL}_n(q)$ stabilizes a pair of subspaces (U, W) of V, where $\dim U = 1$ and $\dim W = n-1$. In particular, every such element is contained in a reducible subgroup of type $P_{1,n-1}$ or $\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$, so $\alpha(z) > q^{-3}$ if $z \in G_0$ is a transvection.

Without loss of generality, we may assume that $g = \iota\sigma$. For any $s \in \mathrm{PGL}_n(q)$ we have

$$(gs)^{2e} = s^{g^{2e-1}} s^{g^{2e-2}} \cdots s^g s,$$

and since e is odd this is equal to

$$s^{\sigma^{e-1}\iota} s^{\sigma^{e-2}} \cdots s^{\sigma\iota} s = z^\iota z,$$

where $z = s^{\sigma^{e-1}} s^{\sigma^{e-2}\iota} \cdots s^{\sigma\iota} s \in \mathrm{PGL}_n(q)$. In particular, $z^\iota z$ is $\mathrm{PGL}_n(q)$-conjugate to $z^{-\iota} z^\iota z z^\iota = z z^\iota = (z^\iota z)^\iota$. But every element in $\mathrm{PGL}_n(q)$ is conjugate to its transpose, hence $z^\iota z$ is conjugate to its inverse. Consequently, if $\lambda \in \overline{\mathbb{F}}_q$ is an eigenvalue of $z^\iota z$ on V then λ^{-1} is also an eigenvalue. Since n is odd, it follows that ± 1 occurs as an eigenvalue of $z^\iota z = (gs)^{2e}$. By the Shintani descent argument used in Lemma 5.7(ii), we deduce that $(gs)^2$ stabilizes a 1-dimensional subspace U and is therefore contained in a P_1 parabolic subgroup H of G. It follows that gs normalizes $H \cap H^{gs}$, and we note that H^{gs} stabilizes an $(n-1)$-dimensional subspace W (the inverse-transpose automorphism interchanges the stabilizers of i-dimensional and $(n-i)$-dimensional subspaces of V). There are two possibilities. If $U \subseteq W$ then $H \cap H^{gs}$ is a type $P_{1,n-1}$ maximal parabolic subgroup of G containing gs; otherwise $V = U \oplus W$ and $H \cap H^{gs}$ is a maximal subgroup of type $\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$ containing gs. This justifies the claim, namely, if q is bounded then $\alpha(z)$ does not tend to zero as n tends to infinity.

In fact, we claim that if $n \geq 5$ then $s(G) < (q+1)^2$, so $u(G)$ is bounded if q is bounded. We thank Bob Guralnick for suggesting the following argument. First fix a basis $\{v_1, \ldots, v_n\}$ for V and write $\mathbb{F}_q^* = \langle \omega \rangle$. Define $q+1$ hyperplanes $H_0, \ldots, H_q$ as follows:

$$H_0 = \langle v_1, v_3, \ldots, v_n \rangle,\ H_i = \langle v_1 + \omega^i v_2, v_3, \ldots, v_n \rangle\ (1 \leq i \leq q-1),\ H_q = \langle v_2, \ldots, v_n \rangle.$$

Consider $\bigcap_i H_i = \langle v_3, \ldots, v_n \rangle$ and note that $\bigcup_i H_i = V$. Set $W = \langle v_3, v_4 \rangle$ and label the 1-dimensional subspaces of W as follows:

$$L_0 = \langle v_3 \rangle,\ L_i = \langle v_3 + \omega^i v_4 \rangle\ (1 \leq i \leq q-1),\ L_q = \langle v_4 \rangle.$$

For each H_i and L_j let z_{ij} be the transvection in G_0 with centre H_i and axis L_j, so $L_j = [V, z_{ij}] \subset C_V(z_{ij}) = H_i$. Set $\mathcal{Z} = \{z_{ij} \mid 0 \leq i, j \leq q\}$.

Let H be a hyperplane in V and let L be a 1-dimensional subspace of V. Note that $\dim(H \cap W) \geq 1$ and $L \subset H_i$ for some i (since $V = \bigcup_i H_i$). In particular, some L_j is contained in $H \cap W$. Consider the transvection z_{ij}. By definition, z_{ij} acts trivially on H_i, so z_{ij} fixes L. In addition, since $[V, z_{ij}] = L_j$, it follows that z_{ij} also fixes H, whence z_{ij} fixes the pair of subspaces (L, H).

Now, if $s(G) \geq (q+1)^2$ then there exists an element $y \in G$ such that $G = \langle z, y \rangle$ for all $z \in \mathcal{Z}$. Necessarily, $y = gs$ for some $s \in G_0$, and recall that we have previously observed that every such element fixes a pair of subspaces (L, H), where $\dim L = 1$ and $\dim H = n-1$. By the previous argument, there exists $z \in \mathcal{Z}$ also fixing the pair (L, H), so $\langle z, y \rangle$ is contained in the G-stabilizer of (L, H) and thus $G \neq \langle z, y \rangle$. This is a contradiction, hence $s(G) < (q+1)^2$ as claimed. □

Proposition 5.9. *Theorem 5.1 holds when e is odd, n is even and $(n, q_0) \notin \mathcal{B}$.*

Proof. This is similar to the proof of the previous proposition. Let $n = 2^{k_1} + \cdots + 2^{k_\ell}$ be the binary representation of n (with $k_i > k_{i+1}$ for all i) and set $y = [A_{2^{k_1}}, A_{2^{k_2}}, \ldots, A_{2^{k_\ell}}] \in \mathrm{PSp}_n(q_0)$, where each $A_m \in \mathrm{GSp}_m(q_0)$ is irreducible of order $q_0^{m/2} + 1$. As in the proof of the previous proposition, Theorem 2.12 implies that each irreducible $H \in \mathcal{M}$ is a $\mathcal{C}_3$, $\mathcal{C}_5$ or $\mathcal{C}_8$-subgroup of G. More precisely, H is one of the following types:

$$\mathrm{GL}_{n/2}(q^2),\ \mathrm{GL}_n(q^{1/r}),\ \mathrm{Sp}_n(q),\ O_n^\epsilon(q)\ (q \text{ odd};\ \epsilon = \pm, \text{ but not both}), \tag{23}$$

and Lemma 5.7 implies that there are at most $|C_{\mathrm{PGL}_n(q_0)}(y^2)| < 2q_0^{n-1}$ subgroups of each type in $\mathcal{M}$. The reducible subgroups in $\mathcal{M}$ can be determined via Lemma 5.7(ii): there is at most one of type $P_{j,n-j}$ and one of type $\mathrm{GL}_j(q) \times \mathrm{GL}_{n-j}(q)$, for each even integer $j \leq n/2$. In particular, if $z \in G$ has prime order then Theorem 2.7 implies that the contribution to $\alpha(z)$ from reducible subgroups is less than $\sum_{t\geq 1} 4q^{-2t} = 4/(q^2-1)$. Consequently, if $n \geq 6$ then Corollary 2.9 implies that

$$\alpha(z) < 4/(q^2-1) + 2q^{(n-1)/e}(3 + \log(e)) \cdot f(n,q) < 1/2.$$

Finally, let us assume $n = 4$. Since $(n, q_0) \notin \mathcal{B}$ we may assume $q_0 \geq 4$. Here $|C_{\mathrm{PGL}_4(q_0)}(y)| = (q_0^4 - 1)/(q_0 - 1)$ and y^2 is irreducible, so each $H \in \mathcal{M}$ is irreducible and the possible types are given in (23). In addition, we note that if $H \in \mathcal{M}$ is a $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_2(q^2)$ then $C_G(y^2) = C_H(y^2)$ and $(y^2)^G \cap H = (y^2)^H$, so there is a unique such subgroup in $\mathcal{M}$. By applying the relevant fixed point ratio estimates in Lemma 2.11 we deduce that

$$\alpha(z) < \frac{d_1(q^3+2q+1)}{q^2(q^3-1)} + \left(\frac{q_0^4-1}{q_0-1}\right)\left(\frac{q^2}{d_2(q^3-1)} + \frac{4d_2(d_2-1)}{q^3-1} + \log(e)\cdot f(4,q)\right),$$

where $d_1 = (4, q-1)$ and $d_2 = (2, q-1)$. It follows that $\alpha(z) < 1/2$ for all $e \geq 5$.

To deal with the case $(n, e) = (4, 3)$ we need to improve the upper bound on the number of subgroups of type $\mathrm{Sp}_4(q)$ in $\mathcal{M}$. We claim that for any e there are at most $d_2^2(q_0+1)$ such subgroups.

To see this, let $G_1 = \langle \mathrm{PGL}_4(q), gs\rangle$ and observe that all subgroups of G_1 of type $\mathrm{Sp}_4(q)$ are G_1-conjugate. We may assume that $H \cap \mathrm{PGL}_4(q)$ is contained in $C_{\mathrm{PGL}_4(q)}(\gamma) = Y_{\sigma^e}$. As in the proof of Lemma 5.7, let j be an integer such that $2j \equiv 1 \pmod{e}$ and $(j, |G_1|) = 1$. Write $(gs)^2 = \sigma^2 t$, where $t = s^\sigma s$, and set $x_1 := (gs)^{2j} = (\sigma^2 t)^j \in \sigma Y_{\sigma^e}$. Note that x_1 has the same order as $\sigma^2 t$ since $(j, |G_1|) = 1$. We will count the number of subgroups of type $\mathrm{Sp}_4(q)$ containing x_1. Suppose that $x_2 \in x_1^{G_1} \cap H$. Now $x_1, x_2 \in \sigma Y_{\sigma^e}$ so we can consider their images $f(x_1), f(x_2)$ in Y_σ under the corresponding Shintani map f. Since the x_i are G_1-conjugate, it follows that the $f(x_i)$ are irreducible and have the same eigenvalues. Therefore $f(x_1)$ and $f(x_2)$ are Y_σ-conjugate, so x_1 and x_2 are actually Y_{σ^e}-conjugate and thus $|x_1^{G_1} \cap H| \leq |x_1^{Y_{\sigma^e}}|$. It follows that the number subgroups of type $\mathrm{Sp}_4(q)$ in $\mathcal{M}$ is at most

$$\frac{|x_1^{G_1} \cap H|}{|x_1^{G_1}|} \cdot \frac{|G_1|}{|H|} \leq \frac{|x_1^{Y_{\sigma^e}}|}{|x_1^{G_1}|} \cdot \frac{|G_1|}{|H|} = \frac{|Y_{\sigma^e}|}{|H|} \cdot \frac{|C_{G_1}(x_1)|}{|C_{Y_{\sigma^e}}(x_1)|}.$$

Further, by considering the Shintani map between $\mathrm{PGL}_4(q)$-classes in $\sigma\mathrm{PGL}_4(q)$ and $\mathrm{PGL}_4(q_0)$-classes in $\mathrm{PGL}_4(q_0)$, we deduce that

$$|C_{G_1}(x_1)| = 2e|C_{\mathrm{PGL}_4(q)}(x_1)| = 2e|C_{\mathrm{PGL}_4(q_0)}(y)| = 2e\left(\frac{q_0^4-1}{q_0-1}\right)$$

(see Lemma 2.13(i)). We also note that $x_1^e \in C_{Y_{\sigma^e}}(x_1)$ and $|x_1^e| = |y| = (q_0^2+1)/d$, so $|C_{Y_{\sigma^e}}(x_1)| \geq (q_0^2+1)/d_2$. Finally, since $|H| \geq 2e|\mathrm{PSp}_4(q)| = 2e|Y_{\sigma^e}|/d_2$ we conclude that

$$\frac{|Y_{\sigma^e}|}{|H|} \cdot \frac{|C_{G_1}(x_1)|}{|C_{Y_{\sigma^e}}(x_1)|} \leq d_2^2(q_0+1).$$

This justifies the claim. In particular, for $(n,e) = (4,3)$ we have

$$\alpha(z) < \frac{d_1(q^3+2q+1)}{q^2(q^3-1)} + \left(\frac{q_0^4-1}{q_0-1}\right)\left(\frac{4d_2(d_2-1)}{q^3-1} + f(4,q)\right) + d_2(q_0+1)\cdot\frac{q^2}{q^3-1}$$

and the result follows.

It is easy to check that the above bounds on $\alpha(z)$ imply that $\alpha(z) \to 0$ (and thus $u(G) \to \infty$) as $q \to \infty$. In contrast to the situation in Proposition 5.8, we claim that $u(G)$ also tends to infinity if q is bounded and $n \to \infty$.

To see this, we may assume that q (and therefore e) is bounded, and that n is large compared with e. Let k be an even integer such that $n/4 < k < n/2$, $(k,e) = (n-k,e) = 1$, and $(k, n-k) = 2$. Set $y = [A,B] \in \mathrm{PSp}_n(q_0)$ where A and B are irreducible of dimensions $n-k$ and k respectively. Since $(k,e) = (n-k,e) = 1$, it follows that A and B remain irreducible over $\mathbb{F}_q$. In addition, some power of y has order r, where either $r > 2(n-k)+1$ is a primitive prime divisor of $q^{n-k}-1$, or r is a product of primitive prime divisors of $q^{n-k}-1$. If $H \in \mathcal{M}$ is reducible then H is of type $\mathrm{GL}_k(q) \times \mathrm{GL}_{n-k}(q)$, and there is a unique such subgroup in $\mathcal{M}$. By Theorem 2.12, the irreducible subgroups in $\mathcal{M}$ are of type $\mathrm{GL}_{n/2}(q^2), \mathrm{GL}_n(q_1), \mathrm{Sp}_n(q)$ or $O_n^+(q)$, where $q = q_1^a$ for some prime divisor a of e. Since $|C_{\mathrm{PGL}_n(q_0)}(y^2)| \leq 2(q_0^{n-k}-1)(q_0^k-1)/(q_0-1)$ we conclude that

$$\alpha(z) < 2q^{-k} + \frac{2(3+\log(e))(q_0^{n-k}-1)(q_0^k-1)}{q_0-1}\cdot f(n,q),$$

which tends to 0 as $n \to \infty$. □

To complete the proof of Theorem 5.1, it remains to deal with the cases (n,q_0) in $\mathcal{A}$ and $\mathcal{B}$, together with the case $n = 3$.

Proposition 5.10. *Theorem 5.1 holds when e is odd and $(n,q_0) \in \mathcal{A} \cup \mathcal{B}$.*

Proof. Define the element y as in the proof of Propositions 5.8 or 5.9, according to the parity of n. As before, note that some power of y has order r, where r is a primitive prime divisor of $q^{2^{k_1}}-1$, so we can use the main theorem of [24] to restrict the subgroups containing gs. Also note that $(2^{k_1}, r) = (4,5)$ if $n \leq 7$, otherwise $(2^{k_1}, r) = (8,17)$. As usual, let $\mathcal{M}$ denote the set of maximal subgroups of G containing gs. We now inspect the various subgroup collections presented in [24, Section 2].

First assume n is odd. As in the proof of Proposition 5.8, the contribution to $\alpha(z)$ from reducible subgroups is less than $2q^{-1} + 2q^{1-n} + 4/(q^2-q)$. If $H \in \mathcal{M}$ is a $\mathcal{C}_2$-subgroup then [24, Example 2.3] implies that $n \leq 7$ and H is of type $\mathrm{GL}_1(q) \wr S_n$. By considering the eigenvalues of y we can eliminate $\mathcal{C}_3$-subgroups, while $\mathcal{C}_4$, $\mathcal{C}_6$ and $\mathcal{C}_7$-subgroups are ruled out by [24]. As usual, $\mathcal{M}$ contains subfield subgroups of type $\mathrm{GL}_n(q_1)$, where $q = q_1^a$ and a is a prime divisor of e; for each divisor a there are at most $|C_{\mathrm{PGL}_n(q_0)}(y^2)| < q_0^{n-1}$ such subgroups in $\mathcal{M}$ (see Lemma 5.7(i)). Similarly, the only $\mathcal{C}_8$-subgroups in $\mathcal{M}$ are of type $O_n(q)$ (assuming q is odd), and again there are fewer than q_0^{n-1} such subgroups.

To complete the analysis of $\mathcal{M}$ when n is odd, we may assume $H \in \mathcal{M}$ is a $\mathcal{C}_9$-subgroup. The various possibilities are listed in [24, Tables 2–8], and we inspect each table in turn. Let H_0 denote the socle of H. Since $q \neq p$, by [5, Table 7.19] we may assume $n \geq 7$.

By inspecting [24, Tables 2–5] we can quickly rule out any possibilities with H_0 an alternating or sporadic group. (Here it is helpful to note that if q_0 is prime (in terms of the notation in [24] – this number is listed in the sixth column of the relevant tables) then the corresponding almost simple subgroup H is contained in a proper subfield subgroup of G, hence H is non-maximal.) Similarly, we can rule out the cases appearing in [24, Tables 6 and 7]. It remains to deal with the cases listed in [24, Table 8]; here H_0 belongs to an infinite family of simple classical groups in characteristic $p' \neq p$. Since $n \geq 7$ is

odd and $2^{k_1} = 4$ or 8, we can quickly eliminate all cases unless $(n, q_0) = (9, 2)$ and $H_0 = \mathrm{PSL}_2(17)$. However, the 2-modular character table of $\mathrm{SL}_2(17)$ (see [29, p.11]) indicates that $\mathrm{SL}_2(17)$ does not admit a 9-dimensional irreducible representation in characteristic 2, so this possibility is also eliminated. We conclude that there are no $\mathcal{C}_9$-subgroups in $\mathcal{M}$.

It follows that if $n \geq 5$ is odd and $z \in G$ is an element of prime order, then (22) holds and thus we reduce to the case $(n, q) = (5, 8)$. However, if $n = 5$ then the only reducible subgroups in $\mathcal{M}$ are those of type $P_{1,4}$ and $\mathrm{GL}_1(q) \times \mathrm{GL}_4(q)$, so we can omit the $4/(q^2 - q)$ term in the upper bound in (22), and this yields $\alpha(z) < 1/2$.

Now assume n is even. As above, by inspecting [24] we deduce that if $H \in \mathcal{M}$ then either H is a subfield subgroup, a $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_{n/2}(q^2)$, a $\mathcal{C}_8$-subgroup of type $O_n^\epsilon(q)$ (q odd) or $\mathrm{Sp}_n(q)$, or $n = 6$ and H is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_6$. Therefore, if $n \geq 6$ we have

$$\alpha(z) < 4/(q^2 - 1) + 2q^{(n-1)/e}((2, q - 1) + 3 + \log(e)) \cdot f(n, q) < 1/2$$

and it is easy to see that $\alpha(z) \to 0$ as $q \to \infty$.

Finally, let us assume $n = 4$. Suppose $q_0 = 2$ and note that we may assume $q \geq 32$ (see Proposition 2.17). Now $|C_{\mathrm{PGL}_4(q_0)}(y^2)| = 15$ and by applying the bounds in Lemma 2.11, using the fact that y^2 is irreducible and belongs to a unique $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_2(q^2)$, we deduce that

$$\alpha(z) < \frac{q^3 + 2q + 1}{q^2(q^3 - 1)} + 15\left(\frac{q^2}{q^3 - 1} + \log(e) \cdot f(4, q)\right) < 1/2$$

if $q > 32$. Finally, if $(n, q) = (4, 32)$ then we can replace the term $\log(e)f(4, q)$ in the above bound by $1/1198336$ (indeed, if H is a subfield subgroup of type $\mathrm{GL}_4(2)$ then it is easy to check that $\mathrm{fpr}(z, G/H) \leq 1/1198336$ for all $z \in G$ of prime order), and this yields $\alpha(z) < 1/2$. Similarly, if $q_0 = 3$ then $|C_{\mathrm{PGL}_4(q_0)}(y^2)| = 40$ and we have

$$\alpha(z) < \frac{(4, q - 1) \cdot (q^3 + 2q + 1)}{q^2(q^3 - 1)} + 40\left(\frac{q^2}{2(q^3 - 1)} + \frac{8}{q^3 - 1} + \log(e) \cdot f(4, q)\right),$$

which is less than $1/2$ unless $(n, q) = (4, 27)$. As in the proof of Proposition 5.9, if $(n, q) = (4, 27)$ then there are at most $2^2(3 + 1) = 16$ subgroups of type $\mathrm{Sp}_4(q)$ in $\mathcal{M}$, whence

$$\alpha(z) < \frac{19738}{7174089} + \frac{2916}{9841} + \frac{160}{9841} + 40 \cdot f(4, 27) < 1/2$$

as required. □

Proposition 5.11. *Theorem 5.1 holds when e is odd and $n = 3$.*

Proof. In view of Proposition 2.17 we may assume $q \geq 27$. Set $y = [A_2, A_1] \in \mathrm{PO}_3(q_0)$, where $A_2 \in O_2^-(q_0)$ is irreducible (over both $\mathbb{F}_{q_0}$ and $\mathbb{F}_q$). By inspecting the explicit list of maximal subgroups of G given in [5], we deduce that the possibilities for $H \in \mathcal{M}$ are as follows: we get reducible subgroups of type $P_{1,2}$ and $\mathrm{GL}_1(q) \times \mathrm{GL}_2(q)$ (exactly one of each type); $\mathcal{C}_2$-subgroups of type $\mathrm{GL}_1(q) \wr S_3$; subfield subgroups of type $\mathrm{GL}_3(q_1)$ and $\mathcal{C}_8$-subgroups of type $O_3(q)$ (with q odd). Now $|C_{\mathrm{PGL}_3(q_0)}(y^2)| \leq q_0^2 - 1$ and thus Lemma 2.10 implies that

$$\alpha(z) < 2q^{-1} + 2q^{-2} + (q_0^2 - 1)\left((2, q - 1) + \log(e)\right)(q^2 + q + 1)^{-1} < 1/2$$

for all $q \geq 27$. □

This completes the proof of Theorem 5.1.

6. Graph automorphisms

In this section we complete the proof of Theorems 2, 3 and 4 by considering the case where $G = \langle G_0, g\rangle$ with g a graph automorphism of G_0. Here $n \geq 3$ and g is of the form $g = \iota x$, where ι is the inverse-transpose map and $x \in \mathrm{PGL}_n(q)$. As usual, we may replace x by $\delta = [\lambda, I_{n-1}]$ for some $\lambda \in \mathbb{F}_q^*$, so $g^2 = (\iota\delta)^2 = \delta^\iota\delta = 1$ and thus g is an involutory graph automorphism.

The $\mathrm{PGL}_n(q)$-classes of involutory graph automorphisms of G_0 are described in Lemma 6.1 below. First we require some notation. For n even we define

$$S = \begin{pmatrix} 0 & -1 & & & & \\ 1 & 0 & & & & \\ & & 0 & -1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \end{pmatrix} \quad S^+ = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \end{pmatrix} \tag{24}$$

and $t = [J_2, I_{n-2}]$. In addition, if n is even and q is odd we set

$$S^- = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & \mu & \\ & & & & & & 1 \end{pmatrix} \tag{25}$$

where $-\mu/2 \in \mathbb{F}_q$ is a non-square.

Lemma 6.1. *Let $g \in \mathrm{Aut}(G_0)$ be an involutory graph automorphism.*

(i) *If n is odd then g is $\mathrm{PGL}_n(q)$-conjugate to ι, and $C_{G_0}(\iota)$ is of type $O_n(q)$;*
(ii) *If n and q are even then g is $\mathrm{PGL}_n(q)$-conjugate to ιS or ιSt, where $C_{G_0}(\iota S) = \mathrm{Sp}_n(q)$ and $C_{G_0}(\iota St) = C_{\mathrm{Sp}_n(q)}(t)$;*
(iii) *If n is even and q is odd then g is $\mathrm{PGL}_n(q)$-conjugate to ιS, ιS^+ or ιS^-, and the respective centralizers are of type $\mathrm{Sp}_n(q)$, $O_n^+(q)$ and $O_n^-(q)$.*

Proof. This is well known. For example, see [2, Section 19] when q is even, and [34, Lemma 3.7] when q is odd. □

Our main result is the following (here $\mathrm{PSL}_4(3).2_2 \cong \langle \mathrm{PSL}_4(3), \iota\rangle$, where ι is the inverse-transpose graph automorphism):

Theorem 6.2. *Let $G_0 = \mathrm{PSL}_n(q)$ and $G = \langle G_0, g\rangle$, where $g = \iota x$ is the product of the inverse-transpose graph automorphism ι and $x \in \mathrm{PGL}_n(q)$. If we assume $G \neq \mathrm{PSL}_4(2).2$, $\mathrm{PSL}_4(3).2_2$ then there exists $s \in G_0$ such that*

$$\sum_{H \in \mathcal{M}(gs)} \mathrm{fpr}(z, G/H) < 1/2 \tag{26}$$

for all $z \in G$ of prime order. In particular, $u(G) \geq 2$ for all G. Moreover, $u(G)$ is bounded as $|G| \to \infty$ if and only if q is bounded and n is odd.

Remark 6.3. The excluded cases $G = \mathrm{PSL}_4(2).2$ and $\mathrm{PSL}_4(3).2_2$ are genuine exceptions to the bound in (26), but it is easy to check that $u(G) \geq 2$ (see Proposition 2.18).

We partition the proof of Theorem 6.2 into a number of subcases. We begin by assuming $n \geq 5$ is odd.

Proposition 6.4. *Theorem 6.2 holds when $n \geq 5$ is odd.*

Proof. Let $\mathcal{A} = \{(9,2),(7,2),(5,4),(5,3),(5,2)\}$. If $(n,q) \in \mathcal{A}$ then Proposition 2.17 applies, so we may assume otherwise. Without loss of generality, we may assume that $g = \iota$ (see Lemma 6.1) and thus $C_{G_0}(g)$ is of type $O_n(q)$. In particular, we may choose $s \in C_{G_0}(g)$ such that $s = [A,1]$ (modulo scalars), where $A \in \mathrm{SO}^-_{n-1}(q)$ is irreducible of order $q^{(n-1)/2}+1$. Set $y = (gs)^2 = s^2 = [A^2,1]$ and note that

$$|y| = (q^{(n-1)/2}+1)/(2,q-1), \tag{27}$$

so some power of y has order r, where r is a primitive prime divisor of $q^{n-1}-1$.

Let $\mathcal{M}$ be the set of maximal subgroups of G containing gs and suppose $H \in \mathcal{M}$. We claim that one of the following holds:

(i) H is a $\mathcal{C}_1$-subgroup of type $\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$; there is exactly one such subgroup in $\mathcal{M}$.

(ii) H is a $\mathcal{C}_8$-subgroup of type $O_n(q)$, q is odd and there are at most $2q^{(n-1)/2}$ such subgroups in $\mathcal{M}$.

First assume H is reducible. Visibly, y fixes a decomposition $V = U \oplus W$ of the natural G_0-module V, where $\dim U = n-1$. Moreover, U and W are the only proper y-invariant subspaces of V since A^2 acts irreducibly on U. Since H is normalized by gs, it follows that $\mathcal{M}$ contains a unique reducible subgroup, which is of type $\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$. For the remainder, we may assume $H \in \mathcal{M}$ is irreducible; we consider each of the Aschbacher families in turn, using [24] to restrict the possibilities.

If H is a $\mathcal{C}_2$-subgroup then [24, Example 2.3] indicates that H is of type $\mathrm{GL}_1(q) \wr S_n$ with $q \geq 5$, and we quickly deduce that $|y| \leq (q-1)n$. However, this is incompatible with (27) unless $n = 5$ and $q \leq 8$. If $n = 5$ and $q = 5, 8$ then $r = 13$ does not divide $|H \cap \mathrm{PGL}(V)|$. Similarly, if $(n,q) = (5,7)$ then $|y| = 25$, but $|H \cap \mathrm{PGL}(V)|$ is not divisible by 25, so there are no $\mathcal{C}_2$-subgroups in $\mathcal{M}$.

We can eliminate subfield subgroups since $|\mathrm{PGL}_n(q_1)|$ is indivisible by r. Similarly, there are no $\mathcal{C}_8$-subgroups of type $\mathrm{GU}_n(q^{1/2})$ in $\mathcal{M}$, and the main theorem of [24] immediately rules out any $\mathcal{C}_4$, $\mathcal{C}_6$ or $\mathcal{C}_7$-subgroups.

By [24, Example 2.4], if H is a $\mathcal{C}_3$-subgroup then $n = r$ and H is of type $\mathrm{GL}_1(q^r)$. Here $H \cap \mathrm{PGL}(V) \leqslant B.r$, where B is a cyclic group of order $m = (q^r-1)/(q-1)$. In view of (27), it follows that $|y| > r$ (since $(n,q) \notin \mathcal{A}$) and thus $y^r \in B$ is nontrivial. In particular, 1 has multiplicity 1 as an eigenvalue of y^r, but all the eigenvalues of any element of B have the same multiplicative order in $\mathbb{F}_{q^r}^*$. This is a contradiction, so there are no $\mathcal{C}_3$-subgroups in $\mathcal{M}$.

Next suppose q is odd and $H \in \mathcal{M}$ is a $\mathcal{C}_8$-subgroup of type $O_n(q)$. Set $c = (n, q-1)$ and let N be the number of distinct G-conjugates of H in $\mathcal{M}$, so

$$N \leq \frac{|y^G \cap H|}{|y^G|} \cdot [G:H]. \tag{28}$$

By [33, Proposition 4.8.4] we have

$$[G:H] = \frac{|\mathrm{SL}_n(q)|}{c|\mathrm{SO}_n(q)|} < c^{-1}q^{\frac{1}{2}(n^2+n-2)}$$

and we calculate that

$$|y^G \cap H| = \frac{|\mathrm{SO}_n(q)|}{q^{(n-1)/2}+1} < q^{\frac{1}{2}(n^2-2n+1)}, \quad |y^G| > \frac{1}{2}q^{n^2-n}.$$

Therefore (28) yields $N < 2c^{-1}q^{(n-1)/2}$. Finally, since there are at most c distinct G-classes of such subgroups (see [33, Proposition 4.8.4]), it follows that there are at most $2q^{(n-1)/2}$ subgroups of this type in $\mathcal{M}$.

To complete the analysis of $\mathcal{M}$ we may assume $H \in \mathcal{C}_9$ is almost simple with socle H_0. According to [24, Example 2.6], H_0 is not an alternating group. If H_0 is a sporadic group then by inspecting [24, Table 5] we reduce to the case $(G_0, H_0) = (\mathrm{PSL}_{11}(2), \mathrm{M}_{24})$, which we can immediately eliminate since $|y| = 33$ by (27), but $|x| \leq 23$ for all $x \in \mathrm{M}_{24}$. Now assume H_0 is a simple group of Lie type in characteristic ℓ. By inspecting [24, Table 6] we see that no cases arise when $\ell = p$, so let us assume $\ell \neq p$. Here the relevant cases are recorded in [24, Tables 7 and 8] and it is straightforward to rule out them all. For example, suppose $H_0 = \mathrm{PSL}_d(s)$, where s is an ℓ-power and $d \geq 3$ is prime. Then $n = r = (s^d - 1)/(s - 1)$, so (27) implies that

$$|y| = 2^{(n-1)/2} + 1 = 2^{((s^d-1)/(s-1)-1)/2} + 1 > s^d - 1$$

for all possible s and d. However, we have $|x| \leq s^d - 1$ for all $x \in H \cap \mathrm{PGL}(V)$ (indeed, $|x| \leq s^d - 1$ for all $x \in \mathrm{GL}_d(s)$ – see [17, Corollary 2], for example), so this case does not arise.

We are now in a position to complete the proof of the proposition. Let $z \in G$ be an element of prime order and define $\alpha(z)$ as in (14). By applying Proposition 2.8 we deduce that if $(n, q) \notin \mathcal{A}$ then

$$\alpha(z) < q^{-2} + ((2, q-1) - 1) \cdot 2q^{(n-1)/2} \cdot 2q^{1-n} \leq q^{-1}$$

and the result follows.

Note that the above bound implies that $\alpha(z) \to 0$ as $q \to \infty$. However, we claim that if q is bounded then $\alpha(z)$ does *not* tend to zero as n tends to infinity. To do this we prove that *every* element $\iota x \in \iota\mathrm{PGL}_n(q)$ is contained in at least one reducible subgroup of type $P_{1,n-1}$ or $\mathrm{GL}_1(q) \times \mathrm{GL}_{n-1}(q)$. First, note that if $\lambda \in \overline{\mathbb{F}}_q$ is an eigenvalue of $(\iota x)^2$ on V then λ^{-1} must also occur as an eigenvalue (see [19, Theorem 4.2]). Since n is odd, it follows that $(\iota x)^2$ has at least one eigenvalue equal to 1 or -1. In particular, $(\iota x)^2$ stabilizes a 1-dimensional subspace U of V, and we complete the argument as in the proof of Proposition 5.8. Moreover, by repeating the final argument in the proof of Proposition 5.8 we deduce that $s(G) < (q+1)^2$ if $n \geq 5$, so indeed we see that $u(G)$ is bounded if q is bounded. □

Proposition 6.5. *Theorem 6.2 holds when* $n \equiv 2 \pmod 4$.

Proof. Let $\mathcal{B} = \{(10, 2), (6, 2), (6, 3), (6, 4)\}$. If $(n, q) \in \mathcal{B}$ then Proposition 2.17 applies, so assume otherwise. Set $t = [J_2, I_{n-2}]$ and define the matrix S as in (24). By Lemma 6.1, if q is even then there are two $\mathrm{PGL}_n(q)$-classes of involutory graph automorphisms, with representatives ιS and ιSt. Clearly these representatives are in the same G_0-coset, so we may assume that $g = \iota S$ and $C_{G_0}(g)$ is of type $\mathrm{Sp}_n(q)$. Similarly, if q is odd and $\det(\delta) = \lambda$ is a square in $\mathbb{F}_q$ then we may assume that $g = \iota S$. On the other hand, if λ is a non-square then we may assume $g = \iota S\delta$. Now $C_{\mathrm{PGL}_n(q)}(\iota S) = \mathrm{PGSp}_n(q)$ contains an element δ of determinant $\lambda^{n/2}$, so if λ is a non-square we may assume that $g = \iota S\delta$ with $\delta \in C_{\mathrm{PGL}_n(q)}(\iota S)$.

Set $k = n/2+1$, so k is even and $(k, n-k) = 2$. If q is even then set $s \in C_{G_0}(g) = \mathrm{Sp}_n(q)$ with $s = [A, B]$, where $A \in \mathrm{Sp}_k(q)$ and $B \in \mathrm{Sp}_{n-k}(q)$ are irreducible. Similarly, if q is odd we choose $s \in C_{G_0}(\iota S)$ so that s (or δs if $g = \iota S\delta$) is of the form $[A, B]$ with A, B as before. For all q we set $y = (gs)^2 = [A^2, B^2]$ and we note that A^2 and B^2 are irreducible. Now

$$|y| \geq (q^{k/2} + 1)/(2, q-1)^2 \tag{29}$$

and we see that some power of y has order r, where r is a primitive prime divisor of $p^{fk}-1$ (where $q=p^f$ and p is a prime).

As before, let $\mathcal{M}$ be the set of maximal subgroups of G containing gs. We claim that if $H \in \mathcal{M}$ then one of the following holds:

(i) H is a $\mathcal{C}_1$-subgroup of type $\mathrm{GL}_k(q) \times \mathrm{GL}_{n-k}(q)$; there is exactly one such subgroup in $\mathcal{M}$.

(ii) H is a $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_{n/2}(q^2)$; there is exactly one such subgroup in $\mathcal{M}$.

(iii) H is a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_n(q)$ or $O_n^+(q)$ (q odd); there are at most $2q^{n/2-1}$ subgroups of each type in $\mathcal{M}$.

To determine the reducible subgroups in $\mathcal{M}$ we argue as in the proof of Proposition 6.4. Now assume H is irreducible. To determine the possibilities for H we apply the main theorem of [24], considering the various $\mathcal{C}_i$ families in turn.

Suppose H is a $\mathcal{C}_2$-subgroup. Then according to [24, Example 2.3], we may assume H is of type $\mathrm{GL}_1(q) \wr S_n$, so $H \cap \mathrm{PGL}(V) \leqslant (q-1)^{n-1}.S_n$ and $q \geq 5$ (see [33, Table 3.5.H]). If $(n,q) \neq (10,5)$ then [23, Lemma 2.1] implies that some power of y has order r', where r' is either a primitive prime divisor of q^k-1 with $r' > 2k+1$, or r' is a product of primitive prime divisors of q^k-1. In this case, $\mathcal{C}_2$-subgroups are ruled out by Theorem 2.12. Finally, if $(n,q)=(10,5)$ then the order of $s=[A,B]$ is at least $\mathrm{lcm}(5^3+1, 5^2+1) = 1638$, so $|y| \geq 819$. However, we have $|x| \leq 120$ for all $x \in H \cap \mathrm{PGL}(V)$, so there are no $\mathcal{C}_2$-subgroups in $\mathcal{M}$.

Next suppose $H \in \mathcal{M}$ is a $\mathcal{C}_3$-subgroup. By [24, Example 2.3], H is of type $\mathrm{GL}_{n/2}(q^2)$ since $(k, n-k)=2$, and [33, Proposition 4.3.6] indicates that G has a unique conjugacy class of such subgroups. Now $y^G \cap H = y^H$ since any two semisimple elements in $\mathrm{PGL}_{n/2}(q^2)$ with identical eigenvalues are $\mathrm{PSL}_{n/2}(q^2)$-conjugate. In addition, $C_G(y)$ is of type $Z_{q^k-1} \times Z_{q^{n-k}-1}$, so $C_G(y)$ is contained in a $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_{n/2}(q^2)$ and therefore we may assume that $C_G(y) \leqslant H$. By applying Corollary 2.5, it follows that y is contained in a unique such subgroup.

By the main theorem of [24], there are no $\mathcal{C}_4$, $\mathcal{C}_6$ or $\mathcal{C}_7$-subgroups in $\mathcal{M}$, and we can eliminate subfield subgroups and $\mathcal{C}_8$-subgroups of type $\mathrm{GU}_n(q^{1/2})$ since r must divide $|H \cap \mathrm{PGL}(V)|$. Next suppose $H \in \mathcal{M}$ is a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_n(q)$ or $O_n^\epsilon(q)$. In the latter case note that q is odd and $\epsilon = +$ is the only possibility since y fixes a decomposition $V = U \oplus W$, where U and W are both non-degenerate orthogonal subspaces of minus-type. Suppose $H \in \mathcal{M}$ is of type $\mathrm{Sp}_n(q)$. Set $c=(q-1, n/2)$ and let N be the number of distinct G-conjugates of H containing y. By [33, Proposition 4.8.3] we have

$$[G:H] = \frac{|\mathrm{SL}_n(q)|}{c|\mathrm{Sp}_n(q)|} < c^{-1}q^{\frac{1}{2}(n^2-n-2)},$$

while

$$|y^G \cap H| = \frac{|\mathrm{Sp}_n(q)|}{(q^{k/2}+1)(q^{(n-k)/2}+1)} < q^{\frac{1}{2}n^2}, \quad |y^G| = \frac{|\mathrm{GL}_n(q)|}{(q^k-1)(q^{n-k}-1)} > \frac{1}{2}q^{n^2-n}.$$

Therefore (28) gives $N < 2c^{-1}q^{n/2-1}$. In addition, there are at most c distinct G-classes of subgroups of type $\mathrm{Sp}_n(q)$ in G (see [33, Proposition 4.8.3]), so there are at most $2q^{n/2-1}$ such subgroups in $\mathcal{M}$. Similarly, by applying [33, Proposition 4.8.4], we also find that $\mathcal{M}$ contains at most $2q^{n/2-1}$ subgroups of type $O_n^+(q)$.

To complete the analysis of $\mathcal{M}$ we may assume $H \in \mathcal{C}_9$ is almost simple with socle H_0. First assume $H_0 = A_d$ is an alternating group – the various possibilities are described in cases (a)–(c) in [24, Example 2.6]. No examples arise in (a) and (c) since $H \cap \mathrm{PGL}(V)$ fixes a non-degenerate form on V in each relevant case. In (b), there are a couple of possibilities

when $n = 6$ and $d = 6$ or 7. However, [24, Table 3] indicates that $q \geq 7$, so $|y| \geq 13$ by (29) but $|x| \leq 12$ for all $x \in H$, so no examples arise. Similarly, by inspecting [24, Table 5] we can rule out any possibilities with H_0 a sporadic group.

Finally, suppose H_0 is a simple group of Lie type in characteristic ℓ. If $\ell = p$ is the defining characteristic then H must appear in [24, Table 6], but there are no relevant cases. Finally, let us assume $\ell \neq p$. By inspecting [24, Tables 7, 8], and by considering the corresponding Frobenius–Schur indicators (see [15] and [29]) to determine whether or not $H \cap \mathrm{PGL}(V)$ fixes an appropriate form on V, we reduce to the following cases:

	H_0	α	n	p
(i)	$\mathrm{PSU}_4(3)$	28	6	$p \equiv 1 \pmod 6$
(ii)	$\mathrm{PSL}_3(4)$	21	6	$p \equiv 1 \pmod 6$
(iii)	$\mathrm{PSL}_2(11)$	12	6	$p \neq 2, 11$

Here α denotes the maximal order of an element of $\mathrm{Aut}(H_0)$. In (i) and (ii) we have $|y| > \alpha$ if $p > 7$ (see (29)), so we may assume $G_0 = \mathrm{PSL}_6(7)$. Here $|y| \geq \mathrm{lcm}((7^2+1)/2, (7+1)/2) = 100$, so this case does not arise. Similarly, in (iii) we may assume $q \geq 5$ (since $(n, q) \notin \mathcal{B}$), hence $|y| \geq 13$ and this case can also be discarded.

Let $z \in G$ be an element of prime order. By applying Theorem 2.7 and Proposition 2.8 we deduce that if $(n, q) \notin \mathcal{B}$ then

$$\alpha(z) < 2q^{k-n} + 4q^{1-n/2} + ((2, q-1) - 1) \cdot 4q^{-\frac{1}{2}n} + 2q^{8-2n} < 1/2. \tag{30}$$

Moreover, it is straightforward to check that $\alpha(z) < q^{-n/6}$ if $n > 12$ or $q > 5$, whence $\alpha(z) \to 0$ as $|G| \to \infty$. □

Proposition 6.6. *Theorem 6.2 holds when $n \equiv 0 \pmod 4$ and $n \geq 8$.*

Proof. If $(n, q) = (8, 2)$ then the desired result follows from Proposition 2.17, so we will assume otherwise. By Lemma 6.1, there are three $\mathrm{PGL}_n(q)$-classes of involutory graph automorphisms, with representatives ιS, ιS^+, and ιS^-, and respective centralizers of type $\mathrm{Sp}_n(q)$, $O_n^+(q)$ and $O_n^-(q)$. Now $\det(S^+) = (-1)^{n/2} = 1$ so ιS and ιS^+ are in the same G_0-coset and thus we reduce to the two cases $g = \iota S$ and $g = \iota S^-$.

First assume $g = \iota S$. This is very similar to the proof of the previous proposition. Set $k = n/2 + 2$, so k is even and $(k, n-k) = 2$ or 4. As before, we may take $s \in G_0$ such that $y = (gs)^2 = [A^2, B^2]$ where $A \in \mathrm{Sp}_k(q)$ and $B \in \mathrm{Sp}_{n-k}(q)$ are irreducible. Then (29) holds and the subsequent analysis of $\mathcal{M}$ is entirely similar, except that we need an additional argument to eliminate $\mathcal{C}_6$ subgroups. Suppose $H \in \mathcal{M}$ is a $\mathcal{C}_6$-subgroup. According to [24, Example 2.5], we may assume that $q = p \equiv 1 \pmod 4$ and $n = 2^m$ with $m \geq 3$. Now $H \cap \mathrm{PGL}(V) \leqslant 2^{2m}.\mathrm{Sp}_{2m}(2)$, where 2^{2m} is elementary abelian of order 2^{2m}, so $|z| \leq 2\alpha$ for all $z \in H \cap \mathrm{PGL}(V)$ where α is the maximal order of an element of $\mathrm{Sp}_{2m}(2)$. Clearly $\alpha \leq 2^{2m} - 1$ (see [17, Corollary 2], for example), so by considering (29) we reduce to the case $(n, q) = (8, 5)$. Here $\alpha = 15$ and $|y| \geq (5^3 + 1)/4$, so there are no $\mathcal{C}_6$-subgroups in $\mathcal{M}$. In this way we deduce that (30) holds and the result quickly follows. We leave the reader to check the details.

For the remainder of the proof we may assume $g = \iota S^-$. Here $C_{G_0}(g)$ is of type $O_n^-(q)$ and we set $y = (gs)^2 = s^2$ where $s \in C_{G_0}(g)$ is irreducible. Let $\mathcal{M}$ denote the set of maximal subgroups of G containing gs. Note that there are no reducible subgroups in $\mathcal{M}$, and also note that some power of y has order r, where r is a primitive prime divisor of $p^{fn} - 1$ (recall that $q = p^f$ and p is a prime).

To begin with, let us assume $(n, q) \neq (12, 2)$ or $(20, 2)$. Then [23, Lemma 2.1] implies that some power of y has order r', where either $r' > 2n + 1$ is a primitive prime divisor of $q^n - 1$, or r' is a product of primitive prime divisors of $q^n - 1$. Therefore, Theorem 2.12 implies that each $H \in \mathcal{M}$ is of type $\mathrm{GL}_{n/k}(q^k)$ (where k is a prime divisor of n), $\mathrm{Sp}_n(q)$ or

$O_n^-(q)$ (with q odd). Note that there are no subfield subgroups nor $\mathcal{C}_8$-subgroups of type $\mathrm{GU}_n(q^{1/2})$ in $\mathcal{M}$ since $|H \cap \mathrm{PGL}(V)|$ must be divisible by r. Also, since y is irreducible we deduce that $\mathcal{M}$ contains a unique $\mathcal{C}_3$-subgroup of type $\mathrm{GL}_{n/k}(q^k)$ for each prime divisor k of n, while the usual argument reveals that there are at most $2q^{n/2-1}$ subgroups of type $\mathrm{Sp}_n(q)$ or $O_n^-(q)$ in $\mathcal{M}$. By applying Proposition 2.8 and Corollary 2.9 we deduce that

$$\alpha(z) < (\log(n)+1) \cdot f(n,q) + 2q^{n/2-1}\left(2q^{2-n} + ((2,q-1)-1) \cdot 2q^{1-n}\right) < 1/2 \qquad (31)$$

for all $z \in G$ of prime order. Moreover, if $n > 12$ or $q > 4$ then (31) yields $\alpha(z) < q^{-n/4}$, so the desired asymptotic result also holds.

Finally, suppose $(n,q) = (12,2)$ or $(20,2)$. By applying the main theorem of [24], we calculate that in both of these cases there are no additional subgroups in $\mathcal{M}$. For example, if $(n,q) = (20,2)$ then $r = 41$ and by inspecting [24] we deduce that each $H \in \mathcal{M}$ is of type

$$\mathrm{GL}_{10}(4),\ \mathrm{GL}_4(32),\ \mathrm{Sp}_{20}(2) \text{ or } \mathrm{PSL}_2(41).$$

Here the last case is a $\mathcal{C}_9$-subgroup appearing in [24, Table 8], but we can eliminate it since the Frobenius–Schur indicator of the underlying irreducible representation of $\mathrm{SL}_2(41)$ is of minus type (see [28, Table 2(b)], for example), hence H is contained in a $\mathcal{C}_8$-subgroup of type $\mathrm{Sp}_{20}(2)$. The case $(n,q) = (12,2)$ is entirely similar. We conclude that (31) holds and the result follows. □

To complete the proof of Theorem 6.2 we may assume $n = 4$ or 3.

Proposition 6.7. *Theorem 6.2 holds when $n = 4$.*

Proof. If $q \leq 9$ then Proposition 2.17 applies, so let us assume $q \geq 11$. As in the proof of Proposition 6.6, we may assume $g = \iota S$ or ιS^-. In both cases we may choose $s \in G_0$ such that $y = (gs)^2 \in G_0$ is irreducible on V and

$$|y| = (q^2+1)/(2,q-1). \qquad (32)$$

As before, let $\mathcal{M}$ be the set of maximal subgroups of G containing gs. Since we are assuming $q \geq 11$, [23, Lemma 2.1] implies that some power of y has order r, where either $r > 9$ is a primitive prime divisor of q^4-1, or r is a product of primitive prime divisors of q^4-1. Therefore Theorem 2.12 applies and we quickly deduce that each $H \in \mathcal{M}$ is of type $\mathrm{GL}_2(q^2)$, $\mathrm{Sp}_4(q)$ or $O_4^-(q)$ (with q odd). (Note that $|y|$ does not divide $|\mathrm{PGL}_4(q_1)|$ (where $q = q_1^a$ for some prime a), $|\mathrm{PGU}_4(q^{1/2})|$ or $|O_4^+(q)|$, so these subgroups do not arise.)

Since y is irreducible, the usual argument reveals that $\mathcal{M}$ contains a unique subgroup of type $\mathrm{GL}_2(q^2)$. Next assume q is odd and H is of type $O_4^-(q)$. Set $c = (q-1,4)/2$ and let N be the number of distinct G-conjugates of H containing y, so (28) holds. Now

$$[G:H] = \frac{|\mathrm{SL}_4(q)|}{2c|\mathrm{SO}_4^-(q)|},\ \ |y^G \cap H| \leq \frac{2|\mathrm{SO}_4^-(q)|}{q^2+1},\ \ |y^G| = \frac{|\mathrm{GL}_4(q)|}{q^4-1}$$

(see [33, Proposition 4.8.4]) and thus $N \leq (q+1)/c$. Since there are at most c distinct G-classes of such subgroups, we conclude that there are at most $q+1$ subgroups of type $O_4^-(q)$ in $\mathcal{M}$.

Now let N be the number of subgroups of type $\mathrm{Sp}_4(q)$ in $\mathcal{M}$. We claim that $N \leq (2,q-1)^3$. To see this, let $G_1 = \langle \mathrm{PGL}_4(q), g\rangle$ and observe that all subgroups of G_1 of type $\mathrm{Sp}_4(q)$ are G_1-conjugate, so we have

$$N \leq \frac{|(gs)^{G_1} \cap H|}{|(gs)^{G_1}|} \cdot \frac{|G_1|}{|H|}.$$

In order to derive an upper bound on $|(gs)^{G_1} \cap H|$, we are free to assume that $H \leqslant C_{G_1}(\iota S)$. Suppose that $\iota St_1, \iota St_2 \in (gs)^{G_1} \cap H$, where $t_1, t_2 \in \mathrm{PGL}_4(q)$. Now $(\iota St_1)^2 = t_1^2$ and $(\iota St_2)^2 = t_2^2$ are elements of $H \cap \mathrm{PGL}_4(q)$ with the same set of eigenvalues,

$$\mathcal{E} = \{\lambda, \lambda^{q_0}, \lambda^{q_0^2} = \lambda^{-1}, \lambda^{q_0^3} = \lambda^{-q_0}\},$$

say. Therefore, it follows that the eigenvalues of t_1 and t_2 are either $\{\mu, \mu^{q_0}, \mu^{q_0^2}, \mu^{q_0^3}\}$ or $\{-\mu, (-\mu)^{q_0}, (-\mu)^{q_0^2}, (-\mu)^{q_0^3}\}$, where $\mu^2 = \lambda$. But any two irreducible semisimple elements in $\mathrm{PGSp}_4(q)$ with the same eigenvalues are $\mathrm{PGSp}_4(q)$-conjugate (since $\mathrm{PGSp}_4(q) \cong \mathrm{SO}_5(q)$, this follows from [47, Section 2.6]; it can also be deduced from [44, Table 1]) so t_1 and t_2 are $\mathrm{PGSp}_4(q)$-conjugate, and the same is true for ιSt_1 and ιSt_2. This implies that $|(gs)^{G_1} \cap H| \leq (2, q-1)|(gs)^{\mathrm{PGSp}_4(q)}|$.

Let $m = |gs|$ and observe that m is even and

$$C_{\mathrm{PGL}_4(q)}(gs) \leqslant C_{\mathrm{PGL}_4(q)}((gs)^{m/2}) \cap C_{\mathrm{PGL}_4(q)}((gs)^2).$$

Now $C_{\mathrm{PGL}_4(q)}((gs)^2)$ is cyclic of order $(q^4-1)/(q-1)$ and $(gs)^{m/2}$ is an involution. Since $C_{\mathrm{PGL}_4(q)}((gs)^{m/2})$ contains $(gs)^2$, by inspecting the involution classes in the full automorphism group of G_0 we deduce that $C_{\mathrm{PGL}_4(q)}((gs)^{m/2})$ is of type $\mathrm{GL}_2(q^2)$, $\mathrm{Sp}_4(q)$ or $O_4^-(q)$. Therefore $C_{\mathrm{PGL}_4(q)}(gs)$ is cyclic of order at most q^2+1, hence $|C_{G_1}(gs)| \leq 2(q^2+1)$ and thus

$$N \leq \frac{(2, q-1)|(gs)^{\mathrm{PGSp}_4(q)}|}{|(gs)^{G_1}|} \cdot \frac{|G_1|}{|H|} \leq \frac{(2, q-1)^2|C_{G_1}(gs)|}{|C_H(gs)|}.$$

But $|C_H(gs)| \geq |gs| = 2(q^2+1)/(2, q-1)$ since H contains gs, and this yields $N \leq (2, q-1)^3$ as claimed.

By applying Lemma 2.11 we conclude that if $z \in G$ has prime order then

$$\alpha(z) \leq \frac{d_2^2 q^2}{q^3-1} + \frac{2d_1(d_2-1)(q+1)}{q^3-1} + \frac{d_1(q^3+2q+1)}{q^2(q^3-1)} < q^{-1/3}$$

for all $q \geq 11$, where $d_1 = (4, q-1)$ and $d_2 = (2, q-1)$. □

Proposition 6.8. *Theorem 4.1 holds when $n = 3$.*

Proof. If $q \leq 16$ then Proposition 2.17 applies, so let us assume $q \geq 17$. We may assume $g = \iota$ (see Lemma 6.1). Take $s = [A, 1] \in C_{G_0}(g)$, where $A \in \mathrm{SO}_2^-(q)$ is irreducible of order $q+1$, and set $y = (gs)^2 = [A^2, 1]$. Define $\mathcal{M}$ in the usual way and note that

$$|y| = (2, q-1)^{-1}(q+1). \tag{33}$$

Clearly, if $H \in \mathcal{M}$ is reducible then H is of type $\mathrm{GL}_1(q) \times \mathrm{GL}_2(q)$, and there is a unique such subgroup in $\mathcal{M}$. Now assume $H \in \mathcal{M}$ is irreducible. We claim that q is odd and H is of type $O_3(q)$.

Suppose $H \in \mathcal{M}$ is a $\mathcal{C}_2$-subgroup of type $\mathrm{GL}_1(q) \wr S_3$. If $x \in H \cap \mathrm{PGL}(V)$ then $|x|$ divides $2(q-1)$ or $3(q-1)$, but this is incompatible with (33) since $q \geq 16$. Similarly, since $|y|$ does not divide $|\mathrm{PGL}_3(q_1)|$ nor $|\mathrm{PGU}_3(q^{1/2})|$ we deduce that there are no subfield subgroups or $\mathcal{C}_8$-subgroups of type $\mathrm{GU}_3(q^{1/2})$ in $\mathcal{M}$. We can also eliminate $\mathcal{C}_3$-subgroups of type $\mathrm{GL}_1(q^3)$ since $|y|$ does not divide $3(q^2+q+1)$. Similarly, if H is a $\mathcal{C}_6$-subgroup of type $3^2.\mathrm{Sp}_2(3)$ then $q = p \equiv 1 \pmod 3$, so $q \geq 19$ and $|y| \geq 10$, but $|x| \leq 7$ for all $x \in H$. This rules out $\mathcal{C}_6$-subgroups.

Finally, suppose $H \in \mathcal{M}$ is a $\mathcal{C}_9$-subgroup with socle H_0. The possibilities for H are listed in [5, Table 7.4]; either $H_0 = \mathrm{PSL}_2(7)$ or A_6. Suppose $H_0 = \mathrm{PSL}_2(7)$, so $q = p \equiv 1, 2, 4 \pmod 7$. Here the congruence condition implies that $q \geq 23$ and thus $|y| \geq 12$, which is a contradiction since $|x| \leq 8$ for all $x \in H$. Similar reasoning applies in the case $H_0 = A_6$. This justifies the claim.

Suppose gs is contained in a subgroup H of type $O_3(q)$, where q is odd. Let N be the number of G-conjugates of H containing $y = (gs)^2$. Let $c = (3, q-1)$. By [33, Proposition 4.8.4] we have $[G : H] = c^{-1}[\mathrm{SL}_3(q) : \mathrm{SO}_3(q)]$ and there are at most c distinct G-classes of these subgroups in G. In addition, we compute

$$|y^G \cap H| = |y^H| = \frac{|\mathrm{SO}_3(q)|}{|\mathrm{GU}_1(q)|}, \;\; |y^G| = \frac{|\mathrm{GL}_3(q)|}{|\mathrm{GL}_1(q)||\mathrm{GL}_1(q^2)|}$$

and thus there are at most $q-1$ subgroups of type $O_3(q)$ in $\mathcal{M}$.

By applying Theorem 2.7 and Lemma 2.10 we conclude that if $z \in G$ has prime order then

$$\alpha(z) \leq q^{-1} + q^{-2} + ((2, q-1) - 1) \cdot \frac{q-1}{q^2+q+1} < 2q^{-1}$$

for all $q \geq 16$. □

This completes the proof of Theorem 6.2. Furthermore, in view of Theorems 3.1, 4.1 and 5.1, the proof of Theorem 2.3 is complete. As explained in Section 2, Theorems 2 and 3 are easily deduced from Theorem 2.3.

7. Proof of Corollary 5

In this final section we explain how Corollary 5 quickly follows from Theorems 2 and 3. Recall that Corollary 5 states that if G is an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$ then

$$d(G) = \max\{2, d(G/G_0)\} \leq 3,$$

where $d(L)$ is the minimal size of a generating set for the finite group L.

Write $d = d(G/G_0)$. If $d = 1$ then G/G_0 is cyclic and thus Theorem 2 implies that G is 2-generated. Next suppose $d = 2$. Choose $y_1, y_2 \in G$ such that $G = \langle G_0, y_1, y_2 \rangle$ and set $k = [\langle G_0, y_2 \rangle : G_0]$. Fix $h \in G_0$ such that $|y_2 h| > k$ (this is possible by the main lemma in [41, Section 2]). By applying Theorem 3 to the group $G_1 = \langle G_0, y_1 \rangle$, with $y = (y_2 h)^k \in G_0$ (note that $y \neq 1$ since $|y_2 h| > k$), we deduce that there exists an element $s \in G_0$ and a conjugate $z \in (y_1 s)^{G_1}$ such that $G_1 = \langle y, z \rangle$. It follows that $G = \langle y_2 h, z \rangle$ is 2-generated.

Finally, suppose $d = 3$, say $G = \langle G_0, y_1, y_2, y_3 \rangle$ for some $y_1, y_2, y_3 \in G$. Let $G_2 = \langle G_0, y_1, y_2 \rangle$. Since $d(G_2/G_0) = 2$ the above argument implies that there exists $z_1, z_2 \in G_2$ such that $G_2 = \langle z_1, z_2 \rangle$, and thus $G = \langle z_1, z_2, y_3 \rangle$.

This completes the proof of Corollary 5.

References

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

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

[3] G.J. Binder, *The two-element bases of the symmetric group*, Izv. Vyssh. Uchebn. Zaved. Mat. **90** (1970), 9–11.

[4] W. Bosma and J.J. Cannon, *Handbook of* Magma *functions*, School of Mathematics and Statistics, University of Sydney, Sydney, 1995.

[5] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The Maximal Subgroups of the Low-dimensional Finite Classical Groups*, to appear in the LMS Lecture Note Series, Cambridge University Press.

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

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

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

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

[10] T.C. Burness, *Fixed point ratios in actions of finite classical groups,* II, J. Algebra **309** (2007), 80–138.
[11] T.C. Burness, *Fixed point ratios in actions of finite classical groups,* III, J. Algebra **314** (2007), 693–748.
[12] T.C. Burness, *Fixed point ratios in actions of finite classical groups,* IV, J. Algebra **314** (2007), 749–788.
[13] J.J. Cannon and D.F. Holt, *Automorphism group computation testing in finite groups*, J. Symbolic Comput. **35** (2003), 241–267.
[14] J.J. Cannon and D.F. Holt, *Computing maximal subgroups of finite groups*, J. Symbolic Comput. **37** (2004), 589–609.
[15] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.
[16] F. Dalla Volta and A. Lucchini, *Generation of almost simple groups*, J. Algebra **178** (1995), 194–223.
[17] M.R. Darafsheh, *Orders of elements in the groups related to the general linear group*, Finite Fields Appl. **11** (2005), 738–747.
[18] J.D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.
[19] J. Fulman and R. Guralnick, *Conjugacy class properties of the extension of* $\mathrm{GL}(n,q)$ *generated by the inverse-transpose involution*, J. Algebra **275** (2004), 356–396.
[20] D. Gorenstein and R. Lyons, *The local structure of finite groups of characteristic 2 type*, Mem. Amer. Math. Soc. **276** (1983).
[21] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Mathematical Surveys and Monographs, vol. 40, Amer. Math. Soc., 1998.
[22] R.M. Guralnick, *The spread of finite groups*, in preparation.
[23] R.M. Guralnick and G. Malle, *Products of conjugacy classes and fixed point spaces*, J. Amer. Math. Soc. **25** (2012), 77–121.
[24] R. Guralnick, T. Pentilla, C.E. Praeger, and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. London Math. Soc. **78** (1999), 167–214.
[25] R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.
[26] R.M. Guralnick and J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), 519–571.
[27] R.M. Guralnick and A. Shalev, *On the spread of finite simple groups*, Combinatorica **23** (2003), 73–87.
[28] G. Hiss and G. Malle, *Low dimensional representations of quasi-simple groups*, LMS J. Comput. Math. **4** (2001), 22–63.
[29] C. Jansen, K. Lux, R. Parker, and R. Wilson, *An Atlas of Brauer Characters*, Clarendon Press, Oxford, 1995.
[30] W. Kantor, *Subgroups of classical groups generated by long root elements*, Trans. Amer. Math. Soc. **248** (1979), 347–379.
[31] W.M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.
[32] N. Kawanaka, *On the irreducible characters of the finite unitary groups*, J. Math. Soc. Japan **29** (1977), 425–450.
[33] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.
[34] M.W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Camb. Phil. Soc. **102** (1987), 33–47.
[35] M.W. Liebeck and J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces*, Proc. London Math. Soc. **63** (1991), 266–314.
[36] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.
[37] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.
[38] M.W. Liebeck and A. Shalev, *Classical groups, probabilistic methods, and the* $(2,3)$*-generation problem*, Annals of Math. **144** (1996), 77–125.
[39] M.W. Liebeck and A. Shalev, *Random* (r,s)*-generation of finite classical groups*, Bull. London Math. Soc. **34** (2002), 185–188.
[40] F. Lübeck and G. Malle, $(2,3)$*-generation of exceptional groups*, J. London Math. Soc. **59** (1999), 109–122.
[41] A. Lucchini and F. Menegazzo, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Sem. Mat. Univ. Padova **98** (1997), 173–191.
[42] S. Ramanujan, *A proof of Bertrand's Postulate*, J. Indian Math. Soc. **11** (1919), 181–182.

[43] A. Shalev, *Random generation of finite simple groups by p-regular or p-singular elements*, Israel J. Math. **125** (2001), 53–60.
[44] K. Shinoda, *The characters of the finite conformal symplectic group,* CSp(4, q), Comm. Algebra **10** (1982), 1369–1419.
[45] R. Steinberg, *Generators for simple groups*, Canad. J. of Math. **14** (1962), 277–283.
[46] R. Steinberg, *Lectures on Chevalley groups*, Yale University, 1968.
[47] G.E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. **3** (1963), 1–62.
[48] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.

School of Mathematics, University of Southampton, Southampton SO17 1BJ, UK
E-mail address: t.burness@soton.ac.uk

Department of Mathematics, Baylor University, Waco TX 76798, USA

Current address for S. Guest:

School of Mathematics, University of Southampton, Southampton SO17 1BJ, UK
E-mail address: guest.simon@gmail.com