Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 320 (2008) 443–494
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Probabilistic generation of finite simple groups, II

Thomas Breuer [a], Robert M. Guralnick [b,*,1], William M. Kantor [c,1]

[a] *Lehrstuhl D für Mathematik, RWTH, 52056 Aachen, Germany*
[b] *Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA*
[c] *Department of Mathematics, University of Oregon, Eugene, OR 97403-1222, USA*

Received 25 August 2005

Available online 20 February 2008

Communicated by Gunter Malle

Abstract

In earlier work it was shown that each nonabelian finite simple group G has a conjugacy class C such that, whenever $1 \neq x \in G$, the probability is greater than $1/10$ that $G = \langle x, y\rangle$ for a random $y \in C$. Much stronger asymptotic results were also proved. Here we show that, allowing equality, the bound $1/10$ can be replaced by $13/42$; and, excluding an explicitly listed set of simple groups, the bound $2/3$ holds.

We use these results to show that any nonabelian finite simple group G has a conjugacy class C such that, if x_1, x_2 are nontrivial elements of G, then there exists $y \in C$ such that $G = \langle x_1, y\rangle = \langle x_2, y\rangle$. Similarly, aside from one infinite family and a small, explicit finite set of simple groups, G has a conjugacy class C such that, if x_1, x_2, x_3 are nontrivial elements of G, then there exists $y \in C$ such that $G = \langle x_1, y\rangle = \langle x_2, y\rangle = \langle x_3, y\rangle$.

We also prove analogous but weaker results for almost simple groups.

Keywords: Finite simple groups; Generation of groups; Probabilistic generation; Spread; $3/2$ generation

Contents

* Corresponding author.
E-mail addresses: sam@math.rwth-aachen.de (T. Breuer), guralnic@usc.edu (R.M. Guralnick), kantor@math.uoregon.edu (W.M. Kantor).

[1] The second and third authors were partially supported by NSF grants DMS 0140578 and DMS 0242983.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2007.10.028

1. Introduction

In [16, Theorem I], it was shown that each nonabelian finite simple group G has a conjugacy class C such that, whenever $1 \neq x \in G$, the probability is greater than $1/10$ that $G = \langle x, y \rangle$ for a random $y \in C$. The purpose of this note is to show that, aside from specific exceptions, the bound $1/10$ can be replaced by $2/3$. For $g, s \in G$, let

$$P(g,s) := \left|\left\{ s^h \in G \;\middle|\; h \in G,\ \langle s^h, g \rangle \neq G \right\}\right| \Big/ \left|s^G\right|$$

and

$$P_G := \min_{1 \neq s \in G} \max_{1 \neq g \in G} P(g,s).$$

Table 1
Exceptions in Theorem 1.1

G	P_G	$\lvert s\rvert$
$\Omega^+(8,2)$	29/42	15
$A_6 \cong \mathrm{Sp}(4,2)'$	5/9	5
$\Omega(7,3)$	155/351	14
$\mathrm{P}\Omega^+(8,3)$	194/455	20
A_7	2/5	7
$\mathrm{PSp}(4,3) \cong \mathrm{SU}(4,2)$	2/5	9
A_5	1/3	5
M_{11}	1/3	11

Then the following is our main result:

Theorem 1.1. *Let G be a nonabelian finite simple group. Then one of the following holds*:

(1) $P_G < 1/3$,
(2) $P_G = 1/3$ *and* $G = \Omega(2m+1,3)$, $m \geqslant 4$ *even*,
(3) $1/2 < P_G \leqslant 1/2 + 1/(2^{m+1}-2)$ *and* $G = \mathrm{Sp}(2m,2)$, $m \geqslant 3$, *or*
(4) G *is in Table* 1.

In particular, $P_G \leqslant 29/42$ *in all cases.*

Note that $\Omega(2m+1,3)$, $m = 2, 3$, are in Table 1 (as $\Omega(5,3) \cong \mathrm{PSp}(4,3)$). Since $\mathrm{Sp}(2m,2) = \Omega(2m+1,2)$, the two infinite families of special cases in Theorem 1.1 are $\Omega(2m+1,q)$ with $q \leqslant 3$.

The proof is in the same spirit as [16], using the classification of finite simple groups. The classification is used both for the list of simple groups to consider and for information about maximal subgroups of these simple groups. However, this time much more care is needed in small dimensions and for groups of Lie type over small fields. In general, the probabilistic arguments in [16] settle most of what we need if the field or dimension is somewhat large (as already noted in [16,20]); but we need to improve some results of [16] about fixed point ratios in certain actions of finite simple groups. A crucial part of our argument consists of computations with the computer system GAP [14]: we do not know any other way to handle quite a few cases involving small fields and dimensions.

We apply Theorem 1.1 in the following situation. For any finite simple group G and any nonidentity element $x \in G$ there is an element $y \in G$ such that $G = \langle x, y\rangle$ (see [16, Section 1]); this property is called "3/2-generation" of simple groups. The above theorem immediately implies the following stronger version of this property, but some care is needed in dealing with the exceptions in the theorem.

Theorem 1.2. *Let G be a nonabelian finite simple group. Then G contains a conjugacy class C of elements such that, for each choice of nonidentity $x, y \in G$, there is an element s in C such that $G = \langle x, s\rangle = \langle y, s\rangle$.*

Moreover aside from the cases $G = \mathrm{Sp}(2m,2)$ $(m \geqslant 3)$, A_5, A_6, and $\Omega^+(8,2)$, for any nonidentity $x, y, z \in G$ there is an element $s \in C$ with $G = \langle x, s\rangle = \langle y, s\rangle = \langle z, s\rangle$.

The notion of the *spread* of a group G is intended to provide a generalization of 3/2-generation: a group is said to have *spread at least k* if, for any nonidentity $x_1, \ldots, x_k \in G$, there is some $y \in G$ such that $G = \langle x_i, y\rangle$ whenever $1 \leqslant i \leqslant k$. There are quite a few papers concerning spread [1,3–7,12,16,20]. In [16] and [20] it was shown that all but at most finitely many simple groups have spread at least 2, and there are infinitely many simple groups (such as $\mathrm{Sp}(2m, 2)$ for $m \geqslant 3$) that have spread exactly 2. Asymptotic results for the spread are in [1,16,20]. As a consequence of Theorem 1.2, we settle the question of spread 2. More generally, we also handle the more restricted notion of *uniform spread*, where we require s to lie in a single conjugacy class of G independent of the choice of the elements x_i:

Corollary 1.3. *Every nonabelian finite simple group has uniform spread at least* 2. *The groups that have uniform spread exactly* 2 *are* $\mathrm{Sp}(2m, 2)$ (*for* $m \geqslant 3$), A_5, A_6, *and* $\Omega^+(8, 2)$; *these exceptions also have spread exactly* 2.

In general, spread and uniform spread need not coincide. For example, the group $\mathrm{SL}(3, 2)$ has uniform spread exactly 3 but spread exactly 4. Note that the above corollary is clearly true for the abelian simple groups as well.

In [16] we proved versions of the above results for each *almost simple group G* whose socle is a nonabelian simple group S (so $F^*(G) = S \leqslant G \leqslant \mathrm{Aut}(S)$). It was shown in this slightly more general setting that there is still a conjugacy class C of elements of G such that each nonidentity element in G generates at least S with each of more than $1/10$ of the elements in C. Here we improve this to $1/2$ (with a small number of exceptions plus the one infinite family $\mathrm{Sp}(2m, 2)$). If $g, s \in G$, define

$$P'(g, s) := 1 - \left|\left\{t \in s^G \;\middle|\; \langle t, g\rangle \geqslant S\right\}\right| \Big/ \left|s^G\right|. \tag{1.1}$$

Clearly $P(g, s) = P'(g, s)$ when $G = S$.

Theorem 1.4. *Let S be a nonabelian finite simple group and G a group with* $F^*(G) = S$. *Then there exists an* $s \in G$ *such that one of the following holds*:

(1) $P'(g, s) < 1/2$ *for all nontrivial* $g \in G$;
(2) $G = \mathrm{Sp}(2m, 2)$, $m \geqslant 3$, *and* $P'(g, s) < 1/2$ *unless* $g \in G$ *is a transvection or is trivial*; *or*
(3) $S = A_6$ *or* $\Omega^+(8, 2)$, *and* $P'(g, s) \leqslant 29/42$ *for all nontrivial* $g \in G$.

Except when $S = A_6$ *or* $G = S_{2m+1}$, *we can choose* $s \in S$. *Moreover, except when* $S = A_{2m+1}, A_6, \Omega^+(8, 2)$ *or* $\mathrm{P}\Omega^+(8, 3)$, *we can choose s independent of the specific subgroup* $G \geqslant S$ *of* $\mathrm{Aut}(S)$.

In the following corollary some care has to be taken when dealing with case (3) of Theorem 1.4. Case (2) has already been dealt with in Theorem 1.2. Note that it has been known for quite a while that S_n has spread at least 2 [4].

Corollary 1.5. *Let G be a finite group with* $S := F^*(G)$ *nonabelian simple. If x, y are nontrivial elements of G, then there exists* $s \in G$ *such that* $\langle x, s\rangle$ *and* $\langle y, s\rangle$ *both contain S. Moreover, aside from the case* $S = A_6$, *we can choose* $s \in S$.

Remark 1.6. Except when S is one of the groups $\Omega^+(8,2)$, $\mathrm{P}\Omega^+(8,3)$, or A_6, s can be chosen from a prescribed conjugacy class of elements in S (independent of G). In the first two of these exceptional cases, s can be chosen from a prescribed $\mathrm{Aut}(S)$-conjugacy class of elements in S. For $S = A_6$, computation shows that no such restriction is possible.

The preceding corollary (as well as the weaker main theorem in [16]) can be used to characterize the solvable radical of a finite group (see [17] for this and further results in the same vein):

Corollary 1.7. *Let G be a finite group.*

(1) *For $x \in G$, $\langle x^G \rangle$ is solvable if and only if $\langle x, y \rangle$ is solvable for each $y \in G$; and*
(2) *if x and y are elements of G neither of which is in the solvable radical of G, then there exists $s \in G$ with $\langle x, s \rangle$ and $\langle y, s \rangle$ both nonsolvable.*

Corollary 1.5 is a bit weaker than saying that G has spread at least 2—in that we generate at least S but not necessarily G. That corollary does not even imply that an almost simple group G has spread at least 1; $G/F^*(G)$ could be noncyclic. Nevertheless, our proofs show that, if $F^*(G)$ is a simple group of Lie type and $G/F^*(G)$ is generated by a diagonal automorphism, then G has spread at least 2.

As noted above, symmetric groups have spread at least two; the same holds for all three subgroups of index two in $\mathrm{Aut}(A_6)$. Table 7 and the last two columns of Table 9 show that the same holds for almost simple groups with sporadic socle.

Conjecture 1.8. *Let G be a finite group. Then G has spread at least 1 if and only if G/N is cyclic for every nontrivial normal subgroup N of G.*

It is not difficult to see that, in order to prove the conjecture, it suffices to consider the case that G has a unique minimal normal subgroup that is a direct product of nonabelian simple groups. The forward implication in the conjecture is clear. We know of no finite group having spread at least 1 that does not have spread at least 2.

We have already noted that, as in [16], our basic tool is fixed point ratios. Section 2 contains background concerning these, together with remarks concerning the computational methodology we use involving GAP [14]. Section 3 contains calculations concerning some specific fixed point ratios. In Section 4, we give detailed results and tables for some smaller groups that were handled computationally. In Sections 5 and 6, we run through all of the types of nonabelian finite simple groups in order to verify Theorems 1.1, 1.2, and 1.4, and Corollaries 1.3 and 1.5.

2. Preliminaries

2.1. Fixed point ratios

All groups will be finite, as will the sets on which they act.

For a given group G and $g, s \in G$, as above let

$$P(g,s) = \left|\left\{s^h \in G \;\middle|\; h \in G,\ \langle s^h, g\rangle \neq G\right\}\right| \Big/ \left|s^G\right|,$$

the proportion of elements in the class s^G which fail to generate with g. Thus, Theorem 1.1 states that $P(g,s) < 1/3$ for $s \in C$ whenever $1 \neq g \in G$ (aside from the exceptions). Note that $P(g,s)$ is also the probability that random elements $g' \in g^G$ and $s' \in s^G$ do not generate G. In particular,

$$P(g,s) = P(s,g). \tag{2.2}$$

For any action of G on a set $\mathbf{X}$, and for any $g \in G$, consider the set $\mathrm{Fix}_{\mathbf{X}}(g)$ of fixed points of g on $\mathbf{X}$, and the *fixed point ratios*

$$\mu(g,\mathbf{X}) := \big|\mathrm{Fix}_{\mathbf{X}}(g)\big|/|\mathbf{X}|$$

and

$$\mu(G,\mathbf{X}) := \max\big\{\mu(g,\mathbf{X}) \;\big|\; g \in G,\ g \neq 1 \text{ on } \mathbf{X}\big\}.$$

If G/M denotes the set of cosets of a subgroup M in G, then

$$\mu(g, G/M) = \big|g^G \cap M\big| \,/\, \big|g^G\big| = \big|g^G \cap M\big|\big|C_G(g)\big|/|G| \tag{2.3}$$

(cf. [16, Section 2]).

For $s \in G$, let $\mathcal{M}(G,s)$ denote the set of maximal subgroups of G that contain s. Then

$$P(g,s) \leqslant \sigma(g,s) := \sum_{M \in \mathcal{M}(G,s)} \mu(g, G/M). \tag{2.4}$$

Thus, in order to prove Theorem 1.1 for the group G, it is sufficient to show that

$$\sigma(G,s) := \max\big\{\sigma(g,s) \;\big|\; 1 \neq g \in G\big\} \tag{2.5}$$

is less than $1/3$ for some $s \in G$. Note that this is usually the case, but occasionally fails to hold (see Section 2.5 for further discussion).

For convenience, we define

$$P(G,s) := \max\big\{P(g,s) \;\big|\; 1 \neq g \in G\big\}. \tag{2.6}$$

Note that, throughout this paper, $\mathrm{SU}(d,q)$ and $\mathrm{GU}(d,q)$ denote the special and the general unitary group with natural module of dimension d over the field $\mathbb{F}_{q^2}$. We regard these groups as defined over the field $\mathbb{F}_q$.

We will use the following general upper bound for $\mu(G, G/M)$:

Theorem 2.1. (See [25].) *Suppose that L is a simple group of Lie type over $\mathbb{F}_q$, not isomorphic to any 2-dimensional linear group, alternating group or* $\mathrm{PSp}(4,3)$*, and let G be a group such that $L \leqslant G \leqslant \mathrm{Aut}(L)$. Then $\mu(G, G/M) \leqslant 4/3q$ for any proper subgroup M of G not containing L.*

We will also use the following bound in the proof of Theorem 1.4:

Theorem 2.2. (See [18].) *Let $F^*(G)$ be a nonabelian simple group S acting primitively on a set $\mathbf{X}$. Let H denote the stabilizer of some $x \in \mathbf{X}$. If $1 \neq g \in G$ fixes at least $|\mathbf{X}|/2$ points, then one of the following holds (up to applying an automorphism of G):*

(1) $S = A_n$ *and* $\mathbf{X}$ *is the set of* k*-subsets for some* $1 \leqslant k < n/2$;
(2) $G = S = \mathrm{Sp}(2m, 2)$, $m > 2$, $H = \Omega^-(2m, 2)$ *and* g *is a transvection*;
(3) $G = \mathrm{O}^-(2m, 2) \neq S$, $m > 2$, g *is a transvection and* $\mathbf{X}$ *is the set of singular points*; *or*
(4) $G = \mathrm{O}^+(2m, 2) \neq S$, $m > 2$, g *is a transvection and* $\mathbf{X}$ *is the set of nonsingular points.*

The next, much more elementary result, gives an upper bound for fixed point ratios for an element that is in a proper subgroup about which we already have information concerning fixed point ratios.

Lemma 2.3. *Let* G *be a finite group acting transitively on a set, with point stabilizer* U. *Let* $g \in G$ *and suppose that* H *is a subgroup of* G *such that* $g \in H$ *and* $\mu(g, H/V) \leqslant \delta$ *for every proper subgroup* V *of* H. *Then* $\mu(g, G/U) \leqslant \delta + c/|G : U|$, *where* c *is the number of fixed points of* H *on* G/U.

In particular, if H *is not conjugate to a subgroup of* U *then* $\mu(g, G/U) \leqslant \delta$.

Proof. If $\Omega_1, \Omega_2, \ldots$ are the nontrivial H-orbits on G/U, then $\sum_i |\Omega_i| = |G/U| - c$. By hypothesis, g fixes at most $\delta|\Omega_i|$ points of Ω_i. Then g fixes at most $\delta(|G/U| - c) + c = \delta|G/U| + c(1 - \delta)$ points of G/U. Thus, $\mu(g, G/U) \leqslant \delta + c/|G : U|$. □

This lemma will be used when G is a simple group of Lie type—in particular for symplectic groups in odd characteristic—and H is an extension field subgroup (in particular, defined over a larger field than G), in which case we can usually use the bound in Theorem 2.1 for H.

However, occasionally we need to be a bit careful when using that result since H need not even be almost simple. If N is a normal subgroup of H and H/N is an almost simple group, then $\mu(g, H/V) \leqslant \mu(g, H/(VN)) = \mu(gN, (H/N)/(VN/N))$ implies that a known global bound for H/N can be used if $g \notin N$; this condition is satisfied if $H = \langle g^H \rangle$.

2.2. Almost simple groups

Consider Theorem 1.4, so that $F^*(G) = S$ is a nonabelian finite simple group. We now discuss $P'(g, s)$ (cf. (1.1)). For the time being we will assume that Theorem 1.1 has been proved; note that the constants required in these two theorems are different.

Fix a suitably chosen nontrivial element $s \in S$ (by Theorem 1.1, in almost all cases we can assume that $P(g, s) < 1/2$ for each $1 \neq g \in S$), and let $\mathcal{M}(S, s)$ be as above.

We first make some comments about computing $\mathcal{M}(G, s)$ in terms of $\mathcal{M}(S, s)$. Let $\mathcal{M}'(G, s)$ denote those subgroups in $\mathcal{M}(G, s)$ that do not contain S.

For purposes of Theorem 1.4 we may assume that g induces an outer automorphism of prime order and $G = \langle S, g \rangle$. Set $J := \langle s^{\langle g \rangle} \rangle$. This is normalized by $\langle g, s \rangle$.

Lemma 2.4.

(1) $J = S$ *if and only if* $G = \langle g, s \rangle$.
(2) $\mathcal{M}'(G, s)$ *consists of the maximal elements in the set of normalizers in* G *of intersections of those subsets of* $\mathcal{M}(S, s)$ *all of whose members are* G*-conjugate.*

Proof. (1) J is normal in $\langle g, s \rangle$, $J \leqslant S$ and $|G : S|$ is prime.

(2) Consider $M \in \mathcal{M}'(G, s)$. Let $h \in M \setminus S$ and $M \cap S \leqslant M_1 \in \mathcal{M}(S, s)$. Clearly $X := \bigcap_i M_1^{h^i}$ is one of the intersections in (2). Since $M \cap S$ normalizes each conjugate $M_1^{h^i}$, we have $M = \langle M \cap S, h \rangle \leqslant N_G(X)$ and so $M = N_G(X)$. □

In the special case that $\mathcal{M}(S,s)$ consists of nonconjugate subgroups of S, the preceding discussion shows that:

Lemma 2.5. *Assume that $\mathcal{M}(S,s)$ consists of subgroups no two of which are conjugate in S. Then $|\mathcal{M}'(G,s)| \leqslant |\mathcal{M}(S,s)|$. If no two members of $\mathcal{M}(S,s)$ are conjugate in G, then $\mathcal{M}'(G,s) = \{N_G(M) \mid N_G(M) \neq M \in \mathcal{M}(S,s)\}$.*

(Here $N_G(M) \neq M$ since no proper subgroup of S can be maximal in G.)

We see that Theorem 1.4 will follow using fixed point ratio results in the same manner as for the simple group; usually the estimates for fixed point ratios are the same for the simple group and the almost simple group, and even when they are weaker for the almost simple group, we are only aiming for $1/2$ rather than $1/3$ as an upper bound. A special case which often occurs is when $|\mathcal{M}(S,s)| = 1$:

Proposition 2.6. *Let S be a nonabelian finite simple group not isomorphic to an alternating group,* $\mathrm{Sp}(2m,2)$ *or* $\Omega^{\pm}(2m,2)$*, $m > 2$. Let $s \in S$ and assume that either $|\mathcal{M}(S,s)| = 1$ or $|\mathcal{M}'(G,s)| \leqslant 1$. If $1 \neq g \in \mathrm{Aut}(S)$, then $P'(g,s) < 1/2$.*

Proof. By the preceding lemma, the hypotheses imply that $|\mathcal{M}'(G,s)| \leqslant 1$. If $\mathcal{M}'(G,s)$ is empty, then $\langle x, s\rangle = G$ for each $x \in G \setminus S$. Otherwise, if $\mathcal{M}'(G,s) = \{M\}$ then $P'(g,s) = \mu(g, G/M) < 1/2$ by Theorem 2.2. □

If some distinct members of $\mathcal{M}(S,s)$ are S-conjugate then the situation is more complicated, and individual arguments are needed. (For the elements we use, this happens only for $\mathrm{Sp}(4m,q)$ (q odd) and $\Omega^{+}(4m,q)$.)

There is one more situation where we can compute $\mathcal{M}(G,s)$ rather easily from $\mathcal{M}(S,s)$:

Lemma 2.7. *Assume that $\mathcal{M}(S,s) = \{M_1, M_2, M_3, \ldots, M_t\}$, where $M_1 \cap M_2 \leqslant M_3$ and M_i and M_j are not conjugate in G for all pairs $\{i,j\} \neq \{1,2\}$. Then $\mathcal{M}'(G,s) \subseteq \{N_G(M_i) \mid 1 \leqslant i \leqslant t\}$.*

Proof. By Lemma 2.4, any member of $\mathcal{M}'(G,s)$ is either $N_G(M_i)$ for some i or $N_G(M_1 \cap M_2)$. Moreover, if $h \in N_G(M_1 \cap M_2)$ then $M_3^h \geqslant (M_1 \cap M_2)^h = M_1 \cap M_2$, so $M_3^h \in \mathcal{M}(S,s)$ and hence $M_3 = M_3^h$ by hypothesis. Thus, $N_G(M_1 \cap M_2) \leqslant N_G(M_3)$. □

In various cases, if information concerning $\mathcal{M}(G,s)$ is readily available we will use this set rather than $\mathcal{M}(S,s)$ in order to compute directly (cf. Section 4.8).

2.3. Irreducible subspaces for $\mathrm{GU}(d,q)$ *and* $\mathrm{O}^{\pm}(d,q)$

The following result will be quite useful. We do not give the proof—it follows from the description of the maximal tori in classical groups. One can also give an elementary argument. In most cases, when we apply the lemma, a power of the element will be of prime order and act irreducibly; the result then follows from the order formulas for the groups in question.

Lemma 2.8.

(a) *Let* $G = \mathrm{GU}(d,q)$ *with natural module* V. *If* $g \in G$ *and* W *is a nondegenerate* $\langle g\rangle$*-irreducible subspace of* V, *then* $\dim W$ *is odd.*
(b) *Let* $G = \mathrm{O}^{\pm}(d,q)$ *with natural module* V. *If* $g \in G$ *and* W *is a nondegenerate* $\langle g\rangle$*-irreducible subspace of* V, *then either* $\dim W = 1$ *or* $\dim W$ *is even and* W *is of* $-$ *type.*

2.4. Some conjugacy lemmas

We record some results about conjugacy classes of semisimple elements in symplectic and orthogonal groups.

Proposition 2.9. *Let* $G = \mathrm{Sp}(d,q) < \mathrm{GL}(d,q)$ *with* $\bar{G}$ *the corresponding algebraic group.*

(1) *If* $x \in \bar{G}$ *is semisimple, then its centralizer is connected.*
(2) *If* $x, y \in G$ *are semisimple elements, then* x *and* y *are conjugate in* G *if and only if they are conjugate in* $\mathrm{GL}(d,q)$.

Proof. Let $\bar{V}$ be the underlying d-dimensional space over the algebraic closure $\bar{\mathbb{F}}$. Let x be a semisimple element. Then $\bar{V}$ is an orthogonal direct sum of subspaces V_i such that the only eigenvalues of x on V_i are α_i and α_i^{-1} for some nonzero distinct α_i. Then $C_{\bar{G}}(x)$ is a direct product of the corresponding centralizers on V_i. If $d_i = \dim V_i$, then the centralizer on V_i is either $\mathrm{GL}(d_i/2, \bar{\mathbb{F}})$ if $\alpha_i \neq \pm 1$ or $\mathrm{Sp}(d_i, \bar{\mathbb{F}})$ if $\alpha_i = \pm 1$. Thus, $C_{\bar{G}}(x)$ is connected. By Lang's Theorem, this implies that semisimple elements $x, y \in G$ are conjugate in G if and only if they are conjugate in $\bar{G}$.

Thus, to prove (2) it suffices to show that the corresponding statement is true for the algebraic group. One direction is clear. So assume that x and y are conjugate in $\mathrm{GL}(\bar{V})$. Then we can decompose $\bar{V}$ as above. Since $\bar{G}$ is transitive on the nondegenerate spaces of a given dimension, we reduce to the case where $\bar{V} = V_i$. If $\alpha_i = \pm 1$, the result is clear. If not, then $\bar{V} = U_1 \oplus U_{-1}$ where U_j is the α_i^j eigenspace of x on $\bar{V}$. Since $\bar{G}$ is transitive on pairs of complementary totally isotropic subspaces, x and y are conjugate. □

The previous result is a special case of a more general result about semisimple elements in a simply connected group. Since orthogonal groups in odd characteristic are not simply connected, the result is somewhat more complicated in that case. Let $x \in G = \mathrm{O}^{\pm}(d,q)$ be a semisimple element. Let V be the underlying natural module over $\mathbb{F}_q$. Write $V = V_1 \perp V_{-1} \perp V_0$ where $V_{\pm 1}$ is the ± 1-eigenspace of x for $i = \pm 1$ and $V_0 = (V_1 \perp V_{-1})^{\perp}$.

Remark 2.10. Note that the type of V_0 is determined by the type of V and the $\mathrm{GL}(V)$ conjugacy class of x. For we may write V as a direct sum of its homogeneous components. If W is a nonself-dual component, then $W \oplus W^*$ is of $+$ type; if W is self-dual, then W has $+$ type if the multiplicity of the simple composition factor is even and $-$ type otherwise (using Lemma 2.8). Thus, the type of V_1 is uniquely determined by the type of V and the $\mathrm{GL}(V)$-class of x.

Proposition 2.11. *Let* $G = \mathrm{O}^{\pm}(d,q)$. *Let* x *be a semisimple element of* G *and let* V *be the natural module for* G *over* $\mathbb{F}_q$. *There exists* $y \in G$ *that is* $\mathrm{GL}(V)$*-conjugate but not* G*-conjugate to* x *if and only if* q *is odd and* ± 1 *are both eigenvalues of* x (*in particular,* x *has even order*).

Proof. $\Leftarrow$: Keeping the notation as above, we suppose that V_i are both nonzero for $i = \pm 1$. Then we may write $V_1 \perp V_{-1} = U_1 \perp U_{-1}$ where $\dim U_i = \dim V_i$ but the type of U_i is the opposite of V_i. Now take $y = x$ on V_0 but with U_1 and U_{-1} its ± 1 eigenspaces. Clearly, x and y are $\mathrm{GL}(V)$-conjugate, but since their eigenspaces are not isometric, they are not $\mathrm{O}(V)$-conjugate.

$\Rightarrow$: First assume that 1 and -1 are not eigenvalues of x on V. Then, precisely as in the symplectic case, the centralizer of x is connected and it suffices to prove the result over the algebraic group. The same proof as in the symplectic case is valid (i.e., the algebraic group is transitive on nondegenerate subspaces of a given isometry type and on complementary pairs of totally singular subspaces).

Thus we can assume that x has an eigenvalue ± 1, but not both. Replacing x by $-x$ if necessary, we may assume that 1 is an eigenvalue of x (so that -1 is not an eigenvalue when q is odd).

Now write $V = V_1 \perp [x, V]$. As we noted prior to the proposition, the type of $[x, V]$ and so the type of $V_1 = C_V(x)$ $(= \mathrm{Fix}_V(x))$ is determined by the $\mathrm{GL}(V)$ class of x. So, if $y \in G$ is $\mathrm{GL}(V)$-conjugate to x, then by conjugating in G (since G is transitive on nondegenerate subspaces of a given type and dimension), we may assume that y is also trivial on V_1 and $[x, V] = [y, V]$. Then x and y are conjugate on $[x, V]$ by the first paragraph, and hence also on V. □

We will often use the following elementary result without comment.

Lemma 2.12. *Let V be the natural module for a classical group G of dimension d over $F := \mathbb{F}_q$. Assume that x lies in an extension field subgroup M of G over $\mathbb{F}_{q^e}$.*

(a) *If x^e is irreducible on V, then M is the only subgroup of G containing x corresponding to an extension field of degree e over F.*
(b) *In particular, if x has order divisible by a primitive prime divisor p of $q^d - 1$ not dividing e, then M is the only subgroup of G containing x corresponding to an extension field of degree e over F.*

Proof. (a) Note that M has a normal subgroup M_0 of index e: the subgroup that acts linearly on V over the corresponding extension field $E := \mathbb{F}_{q^e}$. Then M/M_0 acts as field automorphisms on E/F. So if x is in a subgroup of G corresponding to an extension field of degree e, then x^e must centralize that extension field. Since x^e is irreducible, $C_{\mathrm{GL}(V)}(x^e)$ is cyclic and so x^e centralizes a unique extension field of degree e.

(b) x^e also has order divisible by p and so is irreducible. □

2.5. Computational methodology

For a small number of groups G, the upper bounds given in Theorem 2.1 and Lemma 2.3 are not adequate to prove Theorem 1.1 for G. In these cases, and for obtaining the exceptions in Theorem 1.2, we use GAP [14] for explicit checks. The results are collected in Section 4. See [8] for more information.

For simple groups G, three different tasks arise. First, we want to compute, for a given $s \in G$, either the exact value of $\sigma(G, s)$ or an upper bound for $\sigma(G, s)$. Second, if this is not smaller than $1/3$, we want to compute $P(G, s)$ (cf. (2.6)). Third, if this value is still too large, we want to show the existence or nonexistence of an element s with the property stated in Theorem 1.2.

The optimal situation for computing $\sigma(G, s)$ is the availability of the character table and of all primitive permutation characters of G. In this case, even $\min\{\sigma(G, s) \mid 1 \neq s \in G\}$ can be computed easily, as follows.

Let 1_M^G denote the permutation character of the action of G on the right cosets of a subgroup M. Then $\mu(g, G/M) = 1_M^G(g)/1_M^G(1)$. If M is a maximal subgroup of G that is not normal in G, then $1_M^G(s)$ equals the number of G-conjugates of M that contain s, so

$$\sigma(g, s) = \sum_M 1_M^G(g) \cdot 1_M^G(s)/1_M^G(1), \tag{2.7}$$

where the sum is taken over a set of representatives M of *G-conjugacy classes* in $\mathcal{M}(G, s)$.

We are in this (optimal) situation when the table of marks (Burnside matrix) of G [10, Section 180] is available or if the character tables of G and of all its maximal subgroups (and the necessary class fusions) are available.

If not all primitive permutation characters of G are available then we first choose a suitable element s, determine the set $\mathcal{M}(G, s)$, and try to compute the permutation character values $1_M^G(g)$ for $M \in \mathcal{M}(G, s)$ and conjugacy class representatives g of prime order. If the character table of G is known then this can be done either by computing the conjugacy classes of M and their class fusion in G, or by combinatorial means (cf. [9]). Without access to the character table of G, we can compute (or estimate) the values $|g^M|$ and $|g^G \cap M|$ for the relevant elements g.

Computing $P(g, s)$ is necessary only for those—fortunately few—conjugacy class representatives g for which $\sigma(g, s)$ is too large. The above character-theoretic methods are not sufficient for this task. Since the conjugacy classes of these elements g are quite small (and much smaller than the class of s), we actually compute $P(s, g)$. In the computations, the question of whether g together with the fixed element s generate G can be reformulated as the question of whether $\mathrm{Fix}_X(s) \cap \mathrm{Fix}_X(g)$ is empty, where X is chosen as the disjoint union of the sets G/M, for $M \in \mathcal{M}(G, s)$. So we can compute $P(g, s)$ as the proportion of those point sets in the G-orbit of $|\mathrm{Fix}_X(g)|$ that intersect $\mathrm{Fix}_X(s)$ nontrivially. For example, if $\mathcal{M}(G, s) = \{M\}$ then we take the permutation representation of G on G/M and count the number of those sets in the G-orbit of $\mathrm{Fix}_{G/M}(g)$ that contain the unique fixed point of s on G/M.

Finally, if we have to decide whether, for each triple (x, y, z) in the Cartesian product $x^G \times y^G \times z^G$ of conjugacy classes, an element s (in a prescribed conjugacy class C of G) exists such that $G = \langle x, s\rangle = \langle y, s\rangle = \langle z, s\rangle$, we restrict the test to orbit representatives on $x^G \times y^G \times z^G$ under the conjugation action. The existence of s can often be established by trying a few random elements (in the class C), but exhaustive searches are needed for proving the *nonexistence* of such an s, in order to establish the exceptions in Theorems 1.1, 1.2, 1.4 and Corollary 1.3.

In order to prove the statements about almost simple groups G, we have to consider only the case that $S = F^*(G)$ has prime index in G, and use the same methods as for the simple groups. In particular, Eq. (2.7) holds for the given $s \in S$ and $g \in G \setminus S$, where the sum is taken over representatives M of G-conjugacy classes in $\mathcal{M}(G, s)$. If no two members of $\mathcal{M}(S, s)$ are conjugate in G then the permutation character 1_M^G in the equation is just the extension of the permutation character $1_{M\cap S}^S$ that has been considered for the simple group S. In those cases where some members of $\mathcal{M}(S, s)$ are G-conjugate, we use that the set $\mathcal{M}(G, s)$ is known—the main source for this is [11]. Note that nothing has to be shown in the case $|\mathcal{M}(S, s)| = 1$, by Proposition 2.6.

Most of the computations, in particular the character-theoretic ones, can be regarded as routine calculations. However, these are based on the electronic availability of character tables of finite

simple groups and related groups, and in fact several of these tables have been computed for this paper.

The character-theoretic computations using known character tables required only a few seconds of CPU time, whereas the computations of $P(g,s)$ altogether took several hours of CPU time (on a 2.5 GHz Pentium 4).

3. Some fixed point ratios

In this section we consider fixed point ratios for some actions of orthogonal, symplectic, and linear groups. In each case let V denote the natural module.

3.1. $\mathrm{Sp}(2m,q)$, $\Omega^+(2m,q)$ *and quadratic extension fields*

Let $F=\mathbb{F}_q \subset E=\mathbb{F}_{q^2}$.

Let $G=\mathrm{Sp}(2m,q)$, where we *assume that* $m>2$ *is even*. We may identify V with an m-dimensional space over E in such a way that $H=\mathrm{Sp}(m,q^2).2<G$.

If $1\leqslant k=2\ell\leqslant m$, let $N_{2m}(k,q)$ denote the number of nondegenerate k-dimensional subspaces of V (with respect to the alternating bilinear form defining G). Since all such subspaces are in a single G-orbit,

$$\begin{aligned} N_{2m}(k,q) &= \frac{q^{m^2}(q^{2m}-1)\cdots(q^2-1)}{q^{\ell^2+(m-\ell)^2}(q^{2\ell}-1)\cdots(q^2-1)\cdot(q^{2(m-\ell)}-1)\cdots(q^2-1)} \\ &= \frac{q^{2\ell(m-\ell)}(q^{2m}-1)\cdots(q^{2(m-\ell+1)}-1)}{(q^{2\ell}-1)\cdots(q^2-1)}. \end{aligned}$$

Similarly, if $1\leqslant k\leqslant m$ and $S_{2m}(k,q)$ is the number of totally singular k-spaces, then

$$S_{2m}(k,q)=\frac{(q^{2m}-1)\cdots(q^{2m-2k+2}-1)}{(q^k-1)\cdots(q-1)}.$$

Lemma 3.1. *Let k be a multiple of 4 such that $4\leqslant k\leqslant m/2$. Then*

$$N_{2m}(k,q)/N_m\big(k/2,q^2\big)\geqslant q^{4m-8}.$$

Proof. If $k=2\ell$, the above formula implies that

$$N_{2m}(2k,q)/N_m\big(k,q^2\big)=\frac{q^{\ell(m-\ell)}(q^{2m-2}-1)(q^{2m-6}-1)\cdots(q^{2m-2\ell+2}-1)}{(q^{2\ell-2}-1)(q^{2\ell-6}-1)\cdots(q^2-1)}.$$

This is smallest for $l=2$, and so $N_{2m}(2k,q)/N_m(k,q^2)>q^{2m-4}\cdot q^{2m-4}$. □

Lemma 3.2. *Suppose that k and m are even with $2\leqslant k\leqslant m$ and $m\geqslant 4$.*

(a) *Then* $S_{2m}(k,q)/S_m(k/2,q^2)>q^{2m-3}$.
(b) *If* $m\geqslant 6$, *then* $S_{2m}(m,q)/S_m(m/2,q^2)>q^{4m-8}$.

Proof. From the above formula,

$$\frac{S_{2m}(k,q)}{S_m(k/2,q^2)} = \frac{(q^{2m-2}-1)(q^{2m-4}-1)\cdots(q^{2m-2k+2}-1)}{(q^{k-1}-1)(q^{k-3}-1)\cdots(q-1)}.$$

By calculus, the minimum of the right-hand side is achieved for $k=2$, and is $(q^{2m-2}-1)/(q-1) > q^{2m-3}$.

Moreover, when $k=m$ and $m \geqslant 6$, the right-hand side is at least

$$\bigl(q^{m-1}+1\bigr)\bigl(q^{2m-4}-1\bigr)\bigl(q^{m-3}+1\bigr) > q^{4m-8},$$

as required in (b). □

We next record additional elementary estimates:

Lemma 3.3.

(a) $\frac{|\mathrm{GU}(2d,q)|}{|\mathrm{GL}(d,q^2)|} < 2q^{2d^2}$.
(b) $\frac{|\mathrm{Sp}(2m,q)|}{|\mathrm{Sp}(m,q^2)|} > 2q^{m^2}/3$ *if* m *is even.*

Proof. (a) Since

$$\frac{|\mathrm{GU}(2d,q)|}{|\mathrm{GL}(d,q^2)|} = q^{d^2}(q+1)\bigl(q^3+1\bigr)\cdots\bigl(q^{2d-1}+1\bigr) < q^{2d^2}\prod_{i=1}^{\infty}\bigl(1+2^{1-2i}\bigr),$$

it suffices to check that $\prod_{i=1}^{\infty}(1+2^{1-2i}) \leqslant 2$. Take logarithms and note that $\ln(1+2^{1-2i}) < 2^{1-2i}$, while $\sum_{i=1}^{\infty} 2^{1-2i} = 2/3 < \ln 2$.

(b) This time

$$\begin{aligned}\frac{|\mathrm{Sp}(2m,q)|}{|\mathrm{Sp}(m,q^2)|} &= q^{m^2/2}\prod_{\text{odd } i=1}^{m-1}\bigl(q^{2i}-1\bigr)\\ &= q^{m^2}\prod_{\text{odd } i=1}^{m-1}\bigl(1-q^{-2i}\bigr) > q^{m^2}\left[1-\sum_{\text{odd } i=1}^{m-1} q^{-2i}\right]\\ &> q^{m^2}\bigl[1-1/\bigl(q^2-1\bigr)\bigr] \geqslant q^{m^2}(1-1/3),\end{aligned}$$

as required. □

Lemma 3.4. *Let* $H = \mathrm{Sp}(m,q^2).2 < G = \mathrm{Sp}(2m,q)$ *with* $m \geqslant 4$ *even. If* g *is any element in* $G \setminus Z(G)$*, then*

(a) $\mu(g, G/H) \leqslant 1/q^{2m-3}$ *for* $m > 4$; *and*
(b) $\mu(g, G/H) \leqslant 1/(q-1)(q^3-1)$ *if* $m = 4$.

Proof. We may assume that $g \in H$ and $|g| = r$ is prime or $g^2 \in Z(G)$. We will use (2.3). Recall that F is a field of size q and $E \supset F$ a field of size q^2.

Case 1. *r is odd and g semisimple*. Then V is a completely reducible $F[g]$-module and $g \in H'$ (since r is odd).

Subcase 1a. *V restricted to g is not homogeneous* (i.e., there are at least two nonisomorphic simple $F[g]$-submodules of V). Then either

(i) $V = W \perp W'$ for some nondegenerate $F[g]$-submodules W and W' such that $0 < \dim W \leqslant m$ and $\hom_{F[g]}(W, W') = 0$, or
(ii) $V = W \oplus W'$, where the $F[g]$-modules W and W' are totally singular of dimension m and $\hom_{F[g]}(W, W') = 0$.

Since $g \in H' = \mathrm{Sp}(m, E)$, it follows that E commutes with g and hence leaves invariant all its homogeneous components; in particular, W and W' are E-spaces.

Consider (i) with $d = \dim W$. The probability that a random element of g^G is in H is at most the probability that a random nondegenerate d-space is an E-subspace. Thus,

$$\mu(g, G/H) \leqslant N_m\big(2d, q^2\big)/N_{2m}(d, q) \leqslant 1/q^{4m-8}$$

by Lemma 3.1. In (ii), by Lemma 3.2 the same reasoning shows that

$$\mu(g, G/H) \leqslant S_m\big(m/2, q^2\big)/S_{2m}(m, q) \leqslant 1/q^{2m-3}.$$

Subcase 1b. *g acts homogeneously on V*. Note that g has no eigenvalues equal to ± 1 (since it is homogeneous and noncentral). If W is an irreducible $F[g]$-submodule of V, then $V \cong fW$ for some positive integer f. Since V is self-dual, so is W. It follows that $\dim W = 2e$ is even. Then $2m = f \cdot 2e$ and $K = \mathrm{End}_{F[g]}(V)$ is a field of size q^{2e}. We may assume that $F \subset E \subseteq K$.

Clearly g has $2e$ distinct eigenvalues in K. Since G contains an element having the same eigenvalues and preserving a decomposition of V into the pairwise orthogonal sum of $f = 2m/2e$ nondegenerate $2e$-spaces, Proposition 2.9 implies that g preserves such a decomposition. In particular, we may assume that *W is nondegenerate.* Similarly, as long as g does not act irreducibly, *g leaves invariant a totally singular $2e$-space*—for, G has an element $g^{\#}$ having the same eigenvalues and leaving invariant a totally singular subspace. By Proposition 2.9, g and $g^{\#}$ are conjugate in G.

Note that $D := \mathrm{GU}(m/e, q^e)$ naturally embeds in G. Moreover, $Z = Z(D)$ is cyclic of order $q^e + 1$, and V is a homogeneous $F[Z]$-module. By Proposition 2.9, we may assume that g is a power of a generator g' of Z, in which case $C_{\mathrm{GL}(V)}(g) = C_{\mathrm{GL}(V)}(g') = C_{\mathrm{GL}(V)}(Z)$. Since H is the intersection of G and the centralizer of some element in $\mathrm{GL}(V)$, it follows that $\mu(g, G/H) = \mu(g', G/H)$, so we may now assume that $g = g'$ has order $q^e + 1$. (Consequently, we no longer assume that g has prime order.)

We claim that D is $C_G(g) = C_G(Z)$. If $m = e$, this is clear since Z is a maximal torus of G and so is self-centralizing. If $m > e$, then $D \leqslant C_{\mathrm{GL}(2m,q)}(Z) = \mathrm{GL}(m/e, q^{2e})$ and D is generated by some reflections within $\mathrm{GL}(m/e, q^{2e})$. Consequently, by [29], the only overgroups of D in $\mathrm{GL}(m/e, q^{2e})$ either normalize D or contain $\mathrm{SL}(m/e, q^{2e})$. However, the latter group cannot occur: it acts transitively on the Z-invariant $2e$-dimensional subspaces of V, whereas we have

seen that Z leaves invariant both totally singular and nondegenerate $2e$-spaces. Thus, $C_G(Z)$ normalizes D. Since $N_G(D)/D$ is cyclic of order $2e$ and acts faithfully on Z, this implies the claim.

Recall that $g \in H'$ and V is the direct sum of $f = m/e$ irreducible $F[g]$-modules, each of which is K-invariant and hence also an $E[g]$-module (since $E \subseteq K$). If σ denotes the qth power Frobenius map on E, then there are precisely two irreducible $E[g]$-modules U and U^σ that are $F[g]$-isomorphic to W. Thus, as an $E[g]$-module, $V \cong aU \oplus bU^\sigma$ for nonnegative integers a, b such that $a + b = m/e = f$.

Each eigenvalue of g on U or W has order $q^e + 1$. Since the eigenvalues of g on U^σ are obtained by applying σ to those on U, while those on the dual of U are the reciprocals of those on U, it follows that U and U^σ are dual $E[g]$-modules if and only if $e = 1$. Moreover, if $e > 1$ we see that U is self-dual.

Subsubcase 1bi. $e = 1$. Since U^σ is the dual of U, and V is a self-dual $E[g]$-module, we have $a = b$. Hence, the H-class g^H is uniquely determined: $g^G \cap H = g^H = g^{H'}$.

As noted above, g has two invariant complementary totally singular F-subspaces; each is a homogeneous $E[g]$-module. Since each irreducible $E[g]$-module has E-dimension $e = 1$, this implies that $C_{H'}(g) \geqslant \mathrm{GL}(m/2, q^2)$. Since $g^G \cap H = g^H = g^{H'}$, $C_H(g)$ covers H/H', so that $|C_H(g)| \geqslant 2|\mathrm{GL}(m/2, q^2)|$.

Consequently, by Lemma 3.3,

$$\mu(g, G/H) = \frac{|g^H|}{|g^G|} \leqslant \frac{|H||\mathrm{GU}(m, q)|}{|G| \cdot 2|\mathrm{GL}(m/2, q^2)|} \leqslant \frac{2q^{m^2/2}}{2q^{m^2}/3} \leqslant q^{3-2m},$$

as required.

Subsubcase 1bii. $e > 1$. We have seen that U is self-dual. There are $f + 1$ ordered pairs (a, b) of nonnegative integers satisfying $a + b = f$, each of which produces a conjugacy class g_a^H, where g_a decomposes the E-space V into the perpendicular sum of a copies of U and b copies of U^σ. Thus, $g^G \cap H = g^G \cap H'$ is the union of $f + 1 = m/e + 1$ conjugacy classes of H'. Moreover, $|C_{H'}(g_a)| \geqslant (q^e + 1)^{m/e} > q^m$.

Thus,

$$\mu(g, G/H) < \frac{(m/e + 1)|H'|/q^m}{|g^G|} < \frac{m|H'||C_G(g)|}{q^m|G|}.$$

Since $|C_G(g)| = |D| = |\mathrm{GU}(m/e, q^e)| \leqslant 2q^{m^2/e} \leqslant 2q^{m^2/2}$, by Lemma 3.3(b) we obtain

$$\mu(g, G/H) < \frac{m \cdot 2q^{m^2/2}}{q^m \cdot 2q^{m^2}/3} \leqslant \frac{1}{q^{2m-3}},$$

as required.

Case 2. *$g \in H$ is an involution and q is even.*

Subcase 2a. *g is conjugate to an element of H' but not to an element of $H \setminus H'$.* Then the radical W of $C_V(g)$ is a totally singular subspace of V canonically associated to g. As in Case 1a we obtain $\mu(g, G/H) < 1/q^{2m-3}$.

Subcase 2b. *g is (conjugate to) an element of $H \setminus H'$.* By Lang's Theorem [15, Proposition 4.9.1(d)], all such involutions g are H'-conjugate to field automorphisms. Thus, $g^G \cap (H \setminus H') = g^{H'}$, $\dim_F C_V(g) = m$, and $C_{H'}(g) = \mathrm{Sp}(m, q)$. Moreover, $C_V(g)$ is a totally singular m-space (since q is even). Then $C_G(g) = Q \cdot \mathrm{Sp}(m, q)$, where Q is the unipotent radical of the stabilizer of this maximal totally singular subspace. Thus,

$$\frac{|g^G \cap (H \setminus H')|}{|g^G|} = \frac{|H' : C_{H'}(g)|}{|G : C_G(g)|} = \frac{q^{m(m+1)/2}}{[G : H']}.$$

Suppose that g is also conjugate to an element of H'. As in Case 1b, we obtain $|g^G \cap H'|/|g^G| \leqslant 1/q^{4m-8}$. Consequently,

$$\left|g^G \cap H\right| \,/\, \left|g^G\right| \leqslant 1/q^{4m-8} + q^m/\left(q^2-1\right)\left(q^6-1\right)\cdots\left(q^{2m-2}-1\right),$$

so that (a) or (b) holds.

Case 3. *$g \in H$ is an involution and q is odd.*

Subcase 3a. *g is conjugate to an element of H' but not to an element of $H \setminus H'$.*
Argue precisely as in Cases 1 and 2 for semisimple elements.

Subcase 3b. *g is (conjugate to) an element of $H \setminus H'$.* By Lang's Theorem [15, Proposition 4.9.1(d)], all such involutions g are H'-conjugate to field automorphisms. Thus, $g^G \cap (H \setminus H') = g^{H'}$, $\dim_F C_V(g) = m$, and $C_{H'}(g) = \mathrm{Sp}(m, q)$. Moreover, $C_V(g)$ is a nondegenerate m-space (since q is odd). Then $C_G(g) = \mathrm{Sp}(m, q) \times \mathrm{Sp}(m, q)$, Thus,

$$\frac{|g^G \cap (H \setminus H')|}{|g^G|} = \frac{|H' : C_{H'}(g)|}{|G : C_G(g)|} = \frac{|\mathrm{Sp}(m, q)|}{[G : H']} \leqslant \frac{q^{m(m+1)/2}}{[G : H']}.$$

Suppose that g is also conjugate to an element h of H'. Then $g^G \cap H' = h^{H'}$ and $C_{H'}(h) = \mathrm{Sp}(m/2, q^2) \times \mathrm{Sp}(m/2, q^2)$ (in particular, m must be divisible by 4). Arguing as in the semisimple case, we obtain $|g^G \cap H'|/|g^G| \leqslant 1/q^{4m-8}$. Thus, we obtain the same bound as in Case 2. □

For orthogonal groups the next lemma contains the same bound as in the preceding one. (N.B.—The "real" bound is considerably better, but the next lemma is already much more precise than we need.)

Lemma 3.5. *Let q and $m > 4$ both be even and $G = \mathrm{O}^{\pm}(2m, q)$. Let $H = \mathrm{O}^{\pm}(m, q^2).2 < G$. If $1 \neq g \in G$ then $\mu(g, G/H) \leqslant 1/q^{2m-3}$.*

Proof. Let $X = \mathrm{Sp}(2m, q)$ and $Y = \mathrm{Sp}(m, q^2).2 \leqslant X$ with $Y \cap G = H$. Then $X = GY$, because $[X : Y] = [G : H]$. Thus, G/H and X/Y are isomorphic as G-sets, and the result follows from Lemma 3.4. □

3.2. An action of $\Omega^+(8,q)$

For q even or odd, the case $G = \Omega^+(8,q) = \Omega^+(V)$ is exceptional in our later arguments (Section 5.7). We begin with an elementary observation:

Lemma 3.6. *If* $s \in G$ *has order* $(q^2+1)/\gcd(2,q-1)$ *and leaves invariant two* $F[s]$*-isomorphic irreducible* 4*-spaces, then* $|C_G(s)| \leqslant 4q^2(q^4-1)(q^2+1) < 8q^8$.

Proof. By hypothesis V is a vector space over $F[s] \cong \mathbb{F}_{q^4}$. Then s leaves invariant precisely q^4+1 four-dimensional subspaces V (corresponding to the 1-spaces over $\mathbb{F}_{q^4}$). Suppose that a of these 4-spaces are totally singular and b are nonsingular. Then $a+b = q^4+1$, while $a(q^4-1)+b(q^2+1)(q-1) = (q^4-1)(q^3+1)$ is the number of nonzero singular vectors, so that $a = q^2+1$.

Apply triality to s in order to obtain $s' \in G$ fixing exactly q^2+1 singular points. Then $C_G(s')/\langle -1\rangle$ is a proper subgroup of $\mathrm{O}^-(4,q^2) \times (\mathbb{Z}_{q^2+1} : 4)$, so that $|C_G(s)|$ behaves as stated. □

We note that this lemma can undoubtedly be proved without triality, but using triality seems entertaining.

We will need information concerning a specific action of G when $q \geqslant 4$. Let $\delta = \gcd(2,q-1)$. Let $V = U_1 \perp U_2$ with U_i of type 4^-, and let $M < (\mathrm{O}^-(4,q) \times \mathrm{O}^-(4,q))2$ be the stabilizer in G of $\{U_1, U_2\}$. Note that $n := |G:M| = q^8(q^2-1)(q^6-1)/4$. Also, note that $2n$ is the number of nondegenerate spaces of 4^- type.

Lemma 3.7. *For any* $g \neq \pm 1$ *in* G, $\mu(g, G/M) < 8/q^4$.

Proof. The proof is straightforward but a little tedious. Let G be the corresponding linear group (so if q is odd, the order is doubled). We may assume that $|g|$ is prime modulo $Z(G)$. We use (2.3). We also use the fact that the nontrivial eigenvalues of g on U_i occur in reciprocal pairs. Slightly more care is needed when g has even order. Note that $|G:M|$ is $1/2$ times the number of nondegenerate spaces of type 4^-—i.e. it is $q^8(q^6-1)(q^2-1)/2$.

Case 1. *g has odd order dividing $q-1$.* If g has at least 3 nontrivial eigenvalues, we can replace g by g' of the same order with only 2 nontrivial eigenvalues that fixes fewer nondegenerate 4 spaces than g.

Any nondegenerate 4 space fixed by g is the sum of g-eigenspacing (with the nontrivial eigenvalues coming in pairs). Let a be a nontrivial eigenvalue. It suffices to count the number of nondegenerate 4-spaces U_1 of $-$ type fixed by g where g acts nontrivially. The dimension of the a-eigenspace is at most 4 and it is straightforward to see that the worst case is when it is 1-dimensional.

Let W be the fixed space of g. So W is nondegenerate and $W^\perp$ is contained in X. Suppose that $W^\perp$ is of ϵ type. Thus, the number of such X is precisely the number of nondegenerate 2-spaces of $-\epsilon$ type in X. One computes that this is at most $q^3(q+1)^2(q^2+1)$, whence the result holds.

Case 2. *g has odd order not dividing $q(q-1)$.* Again, we can count the number of g-invariant nondegenerate 4-spaces X of $-$ type on which g acts nontrivially. Note that g must have fixed points on X or act irreducibly on X (otherwise X would be of $+$ type). If g acts irreducibly,

then the total number of g-invariant 4 spaces on which it is nontrivial is at most q^4+1 and we are done as above. If g has fixed points on X, then the worst case is that the fixed space of g is 6-dimensional. The same estimate as in Case 1 holds.

Case 3. *g has odd order dividing q.*

Case 3a. *$g=1$ on U_2.* Then $|g^G\cap M| = |g^M| \leqslant 2\cdot q^2(q^2+1)/2$ in view of the structure of $\mathrm{O}^-(4,q)\cong \mathrm{PGL}(2,q^2):2$. If $g\in G$ is not a root element then $|g^G|>q^9$, and (2.3) yields $\mu(g,G/M)<q^2(q^2+1)/q^9<1/q^4$. If g is a root element then $|g^G\cap M|/|g^G| = 2(q^2-1)/(q^4-1)(q^3+1)<1/q^4$.

Case 3b. *$|g|$ divides q, and g acts nontrivially on both U_1 and U_2.* Then $|g^M|\leqslant (q^2-1)^2$ while $|g^G|>q^9$ once again. Then $|g^G\cap M|/|g^G|<q^4/q^9<1/q^4$.

Case 4. *g interchanges U_1 and U_2, q odd.* In particular, g^2 is central and so is ± 1.

We first count the number of conjugates of g in M which do not fix U_1. All such elements are conjugate in $\mathrm{O}^-(4,q)\wr\mathbb{Z}/2$ and so the number of such is at most $|\mathrm{O}^-(4,q)| = 2q^2(q^2-1)^2 < 2q^6$.

The number of conjugates of g in M that fix both U_1 and U_2 can be estimated as above. If $g^2=1$, then there are fewer than q^8 such conjugates of $g\in M$, whence $|g^G\cap M|<q^9$. Since $C_G(g)\leqslant \mathrm{O}^+(4,q)\times\mathrm{O}^+(4,q)$, $|g^G\cap M|/|g^G|<2q^9/q^{16}$, whence the result holds.

If $g^2=-1$, then no conjugate of g can fix U_1 (for either $4\mid(q-1)$ in which case each eigenspace is totally singular and so must be 2-dimensional and U_1 has no such subspaces or 4 does not divide $q-1$ in which case U_1 would be the sum of two irreducible g-submodules which would either be totally singular or of $-$ type; an impossibility). So in this case $|g^G\cap M|<2q^6$ while $|C_G(g)|\leqslant|\mathrm{GL}(4,q)|<q^{16}$ and again the result follows.

Case 5. *g interchanges U_1 and U_2, q even.* Thus, g is an involution and $C_V(g)$ is a totally singular 4-space (i.e., if $u,v\in U_1$ then $(u+u^g, v+v^g) = (u,v)+(u^g,v^g)+(u,v^g)+(u^g,v) = 0+0$). Then (with respect to a hyperbolic basis of V) g is conjugate to a matrix $\left(\begin{smallmatrix} I & A \\ O & I\end{smallmatrix}\right)$ for a nonsingular skew-symmetric 4×4 matrix A. A simple calculation shows that $C_G(g)$ is a group of the form $q^6\mathrm{Sp}(4,q)$, so that $|C_G(g)|<q^6q^6(q^4-1)$. Also, $|C_M(g)|\geqslant|\Omega^-(4,q)|2 = 2q^2(q^4-1)$.

We claim that g cannot fix U_1—for any involution fixing U_1 does not have a totally singular fixed space. Thus, as in the previous case $|g^G\cap M|\leqslant|\mathrm{O}^-(4,q)|<2q^6$ while $|g^G|\geqslant q^{12}/2$.

Case 6. *g has order 2 modulo $Z(G)$. q is odd and g fixes U_1.* We may assume by Case 4 that no conjugate of g interchanges U_1 and U_2. Arguing as above, we also see that $g^2=1$ in the linear group.

By replacing g by $-g$ if necessary, we may assume that the fixed space of g is either 4-dimensional or 6-dimensional. In the first case, the centralizer of g is contained in the stabilizer of a nondegenerate 4-space and this gives a lower bound on $|g^G|$. Bounding $|g^G\cap M|$ by the number of involutions in the stabilizer of U_1 gives the result. In the second case, $\dim C_{U_1}(g)=2$, 3 or 4 (and $\dim C_{U_2}(g) = 6-\dim C_{U_1}(g)$). An easy computation shows that $|g^G\cap M|$ is on the order of q^6, while $|g^G|$ is approximately q^{12}.

Case 7. *$|g|=2$, q is even and g fixes U_1.* This is done essentially as in the previous case. Again, we may assume that no conjugate of g interchanges the U_i. Again, the fixed space of g

is has dimension 4 or 6. In the first case, one bounds $|g^G \cap M|$ by the number of involutions in $\mathrm{O}^-(4,q) \times \mathrm{O}^-(4,q)$ to see that the result holds. In the second case, $|g^G|$ is approximately q^{12}. The number of conjugates of g in M that are trivial on one of the U_i is at most q^4 while the number that are nontrivial on each U_i is approximately q^6, whence the result follows. □

3.3. $\mathrm{SL}(d,q)$ *for prime* d

Lemma 3.8. *Let* $G = \mathrm{SL}(d,q)$ *with* $d \geqslant 5$ *prime, and let* M *be the normalizer of an irreducible torus* T. *Then* $\mu(g, G/M) < q^{-d}$ *whenever* $g \in G \setminus Z(G)$.

Proof. We have $|T| = (q^d - 1)/(q-1)$ and $|M/T| = d$. We may assume that $gZ(G)$ has prime order and that $g \in M$ (if g is not conjugate to an element of M, then g has no fixed points on G/M).

If $g \in M \setminus T$ then $gZ(G)$ has order d. If also $d \mid q$, then there is a regular unipotent element in $gZ(G)$ and so $|C_G(g)| \leqslant q^{d-1}(q-1) < q^d$. If not, then the minimal polynomial of g is $x^d - a$ for some nonzero scalar a, so g is a regular semisimple element. Thus either g acts irreducibly and so its centralizer is a conjugate of T, or g is diagonalizable with distinct eigenvalues. In either case, its centralizer (even in $\mathrm{GL}(d,q)$) has order less than q^d. Thus $\mu(g, G/M) = |g^G \cap M|/|g^G| < |M||C_G(g)|/|G| < d(q^d-1)q^d/|G| < q^{-d}$.

The remaining case to consider is when g is in $T \setminus Z(G)$ and is not conjugate to an element in $M \setminus T$. Then $|g^G \cap M| < |T| = (q^d-1)/(q-1)$. Since d is prime, every element of T either is in $Z(G)$ or acts irreducibly (since there are no subfields properly between $\mathbb{F}_q$ and $\mathbb{F}_{q^d}$). In particular, $T = C_G(g)$ for any such g, so that $\mu(g, G/M) < |T|q^d/|G| < q^{-d}$. □

3.4. *An action of* $\Omega^-(10,4)$

Let $G = \Omega^-(10,4)$ and let H be the maximal subgroup $\mathrm{GU}(5,4)$ embedded naturally. We need an upper bound for the fixed point ratios of this action. Our vector space V is also unitary over $\mathbb{F}_{16}$. Note that, for any $\mathbb{F}_{16}$-subspace W, the subspace $W^\perp$ is the same computed using the unitary or the orthogonal structure of V. In particular, the radical of W is the same for both structures.

Lemma 3.9. *If* $1 \neq g \in G$ *then* $\mu(g, G/H) \leqslant 1/64$.

Proof. We may assume that $g \in H$ has prime order $r = 2, 3, 5, 13, 17$, or 41.

If $r = 41$ then g is irreducible, and its centralizer in H is a Singer cycle of order $4^5 + 1$. So $\mu(g, G/H) < |H|/|g^G| = 1025|H|/|G| < 1/64$. (N.B.—By Lemma 2.12, g has a unique fixed point.)

If $r = 13$ or 17 then g has an eigenvalue 1 and its fixed space is a nondegenerate $2k$-space over $\mathbb{F}_4$ of some type ϵ. Viewing g in the unitary group, we see that its fixed space is nondegenerate of dimension k over $\mathbb{F}_{16}$. Thus,

$$\mu(g, G/H) = \left|g^G \cap H\right| \,/\, \left|g^G\right| \leqslant N(k,H)/N(2k,\epsilon,G),$$

where $N(k,H)$ is the number of nondegenerate k-spaces when V is viewed as a 5-dimensional unitary space, and $N(2k,\epsilon,G)$ is the number of nondegenerate $2k$-spaces of V of type ϵ. It is straightforward to see that this ratio is smallest when $k = 1$ and $\epsilon = -$. One computes in that

case that $N(1, H) = 4^4(4^4 - 1)$ and $N(2, -, G) = 4^8(4^5 + 1)(4^4 - 1)/2$ so the ratio is less than $1/64$.

When $r = 3$ we claim that any element $h \in H$ of order 3 has 1 as an eigenvalue. For h and h^{-1} are conjugate and so the 1-eigenspace of h is odd-dimensional (on the unitary space) and in particular is nontrivial. So the argument in the preceding paragraph applies here as well.

Now suppose that $r = 5$. If g has a nontrivial fixed vector, we argue as above. If the minimal polynomial of g (over $\mathbb{F}_4$) has degree larger than 2, then the kernel of some (irreducible) quadratic factor applied to g will be a canonical invariant nondegenerate space and the above argument applies. The remaining case is when the minimal polynomial of g has degree 2 (and so is either 1 or 2 over $\mathbb{F}_{16}$). Choose $x \in Z(H)$ of order 5. One of the eigenvalues of g (over $\mathbb{F}_{16}$) has odd multiplicity and replacing g by a power, we may assume that this eigenvalue is equal to the unique eigenvalue of x. It follows from Proposition 2.11 that g and x are conjugate in G. So we see that $g^G \cap H$ is a union of three H-conjugacy classes with centralizers H, $\mathrm{GU}(5, 4) \times \mathbb{Z}/5$ and $\mathrm{GU}(3, 4) \times \mathrm{GU}(2, 4)$. On the other hand, $C_G(g)$ is conjugate to H. An easy computation now shows that $|x^G| > 4^{19}$ while $|g^G \cap H| < 4^{13}$, whence $|g^G \cap H|/|g^G| < 4^{-6}$ as required.

Finally, assume that $|g| = 2$. In H, there are two conjugacy classes of involutions. and there is no fusion—i.e. $g^G \cap H$ is a conjugacy class of H. So the radical of the fixed space of g is either 1-dimensional (for a transvection) or 2-dimensional over $\mathbb{F}_{16}$.

Thus, as above,

$$\mu(g, G/H) = \left|g^G \cap H\right| \Big/ \left|g^G\right| \leqslant S(k, H)/S(2k, G),$$

where $S(k, H)$ denotes the number of totally singular k-spaces in the unitary space and $S(2k, H)$ is the number of totally singular $2k$-spaces in the orthogonal space (note $k \leqslant 2$). This ratio is smallest for $k = 1$, where we compute that the ratio is $(51 \cdot 1025)/(7 \cdot 51 \cdot 257 \cdot 1025) = 1/(7 \cdot 257) < 1/64$. □

4. Computer calculations

In this section, we collect those computations that were done using the GAP system. These cases cover the simple groups G in Table 1—for which we had to compute P_G—as well as the exceptions A_5, A_6, and $\Omega^+(8, 2)$ in Theorem 1.2 and Corollary 1.3—for which we had to compute the exact (uniform) spread—and the exceptional cases with socle A_6, $\Omega^+(8, 2)$, and $\mathrm{P}\Omega^+(8, 3)$ in Theorem 1.4.

Tables 2–5 list those classical groups for which we used explicit GAP computations. When we deal with a classical group defined on a vector space, we may replace the simple group by

Table 2
Computations for $\mathrm{Sp}(d, q)$

d	q	$\lvert s\rvert$	$\mathcal{M}(G, s)$	$\sigma(G, s)$	$P(G, s)$
4	4	17	$\Omega^-(d, q).2$, $\mathrm{Sp}(2, 16).2$	4/15	
6	2	9	$\Omega^-(d, q).2$, $\mathrm{Sp}(d/3, q^3).3$, $\mathrm{Sp}(d/3, q^3).3$, $\mathrm{Sp}(d/3, q^3).3$	4/7	4/7
6	3	28	$N_G(\mathrm{SU}(d/2, q))$, $\mathrm{Sp}(d/3, q^3).3$	1/117	
6	4	65	$\Omega^-(d, q).2$, $\mathrm{Sp}(d/3, q^3).3$	16/63	
8	2	17	$\Omega^-(d, q).2$, $\mathrm{Sp}(d/2, q^2).2$, $\mathrm{PSL}(2, 17)$	8/15	8/15
8	3	82	$\mathrm{Sp}(d/2, q^2).2$	1/546	

Table 3
Computations for $\Omega^\epsilon(d,q)$

d and s	q	$\lvert s\rvert$	$\mathcal{M}(G,s)$	$\sigma(G,s)$	$P(G,s)$
$8^+ = 4^- \perp 4^-$	2	15	$\mathrm{Sp}(6,2)$, $2^6:A_8$, $2^6:A_8$, A_9, A_9, $(3\times\Omega^-(6,2)).2$, $(\Omega^-(4,2)\times\Omega^-(4,2)).2^2$	334/315	29/42
$8^+ = 4^- \perp 4^-$	3	40	$2.\Omega(7,3)$, $2.\Omega(7,3)$, $3^6:2.\mathrm{PSL}(4,3)$, $3^6:2.\mathrm{PSL}(4,3)$, $\mathrm{SU}(4,3).2^2$, $2.(\mathrm{PSp}(2,3)\otimes\mathrm{PSp}(4,3)).2$, $2.(\mathrm{PSp}(2,3)\otimes\mathrm{PSp}(4,3)).2$, $2.(\mathrm{P}\Omega^-(4,3)\times\mathrm{P}\Omega^-(4,3)).2^2$	863/1820	194/455
$8^+ = 2^- \perp 6^-$	4	65	$(5\times\Omega^-(6,4)).2$, $(5\times\Omega^-(6,4)).2$, $(5\times\Omega^-(6,4)).2$	$\leqslant 3385/121\,856$	
$10^+ = 4^- \perp 6^-$	2	45	$(\Omega^-(4,2)\times\Omega^-(6,2)).2$	43/4216	
$12^+ = 4^- \perp 8^-$	2	85	G_8, $\Omega^+(6,4).2^2$, $\Omega^+(6,4).2^2$	7675/1 031 184	
$12^+ = 4^- \perp 8^-$	3	410	G_8, $\Omega^+(6,9).2^2$, $\Omega^+(6,9).2^2$	$\leqslant 6901/88\,209$	
8^-	2	17	$\Omega^-(4,4).2$	1/63	
8^-	3	41	$\Omega^-(4,9).2$	1/567	
10^-	2	33	$\mathrm{GU}(5,2)$	1/119	
10^-	3	122	$2\times\mathrm{SU}(5,3)$	1/1066	
12^-	2	65	$\Omega^-(6,4).2$, $\Omega^-(4,8).3$	1/1023	
14^-	2	129	$\mathrm{GU}(7,2)$	1/2015	
$7 = 1 + 6^-$	3	14	$\Omega^-(6,3).2$, S_9, S_9	199/351	155/351

Table 4
Computations for $\mathrm{SU}(d,q)$

d	q	$\lvert s\rvert$	$\mathcal{M}(G,s)$	$\sigma(G,s)$	$P(G,s)$
3	3	6	$3_+^{1+2}:8$, $\mathrm{GU}(2,3)$	16/63	
3	5	30	$3\times 5_+^{1+2}:8$, $\mathrm{GU}(2,5)$	46/525	
5	2	11	$\mathrm{PSL}(2,11)$	1/54	
4	2	9	$\mathrm{GU}(3,2)$, $3^3:S_4$	3/5	2/5
4	3	28	$4_2.\mathrm{PSL}(3,4)$, $4_2.\mathrm{PSL}(3,4)$, $\mathrm{GU}(3,3)$, $4.A_7$, $4.A_7$, $4.A_7$, $4.A_7$	53/135	43/135
4	4	65	$\mathrm{GU}(3,4)$	209/3264	
6	2	33	$\mathrm{GU}(5,2)$, $3.M_{22}$, $3.M_{22}$, $3.M_{22}$	5/21	
6	3	244	$\mathrm{GU}(5,3)$	353/3159	
8	2	129	$\mathrm{GU}(7,2)$	2753/10 880	

the associated linear group, and hence deal with linear transformations s rather than elements in the simple group. The first two columns of the tables list the dimension d (in Table 3, also the type and the decomposition of the natural module under s is listed) and the size q of the defining field (note that in the unitary case, the natural module is $\mathbb{F}_{q^2}^d$), the third column lists the order $|s|$ of the element s in the linear group, the fourth column lists the collection $\mathcal{M}(G,s)$ of maximal subgroups of G that contain s, and the last two columns list the quantities $\sigma(G,s)$ and $P(G,s)$ (the latter only if the former is not smaller than $1/3$).

Table 5
Computations for $\mathrm{SL}(d,q)$

d	q	$\lvert s\rvert$	$\mathcal{M}(G,s)$	$\sigma(G,s)$
3	2	7	7 : 3	1/4
3	3	13	13 : 3	1/24
3	4	21	$N_G(\mathrm{SL}(3,2))$, $N_G(\mathrm{SL}(3,2))$, $N_G(\mathrm{SL}(3,2))$	1/5
4	2	15	$N_G(\mathrm{SL}(2,4))$	3/14
4	3	40	$N_G(\mathrm{SL}(2,9))$	53/1053
4	4	85	$N_G(\mathrm{SL}(2,16))$	1/108
6	2	63	$N_G(\mathrm{SL}(3,4))$, $N_G(\mathrm{SL}(2,8))$	365/55 552
6	3	364	$N_G(\mathrm{SL}(3,9))$, $N_G(\mathrm{SL}(2,27))$	22 843/123 845 436
6	4	1365	$N_G(\mathrm{SL}(3,16))$, $N_G(\mathrm{SL}(2,64))$	1/85 932
6	5	3906	$N_G(\mathrm{SL}(3,25))$, $N_G(\mathrm{SL}(2,125))$	1/484 220
8	2	255	$N_G(\mathrm{SL}(4,4))$	1/7874
10	2	1023	$N_G(\mathrm{SL}(5,4))$, $N_G(\mathrm{SL}(2,32))$	1/129 794

Table 6
Alternating groups of odd degree

n	$\mathcal{M}(G,s)$	$\sigma(G,s)$	$P(G,s)$
5	5 : 2	1/3	1/3
7	$\mathrm{PSL}(2,7)$, $\mathrm{PSL}(2,7)$	2/5	2/5
9	$\mathrm{P\Gamma L}(2,8)$, $\mathrm{P\Gamma L}(2,8)$, $\mathrm{P\Gamma L}(2,8)$, $(S_3 \wr S_3) \cap A_9$	9/35	
11	M_{11}, M_{11}	2/105	
13	13 : 6, $\mathrm{PSL}(3,3)$, $\mathrm{PSL}(3,3)$, $\mathrm{PSL}(3,3)$, $\mathrm{PSL}(3,3)$	4/1155	
15	$(S_3 \wr S_5) \cap A_{15}$, $(S_3 \wr S_5) \cap A_{15}$, $\mathrm{PSL}(4,2)$, $\mathrm{PSL}(4,2)$	29/273	
17	$\mathrm{P\Gamma L}(2,16)$, $\mathrm{P\Gamma L}(2,16)$	2/135 135	
19	19 : 9	1/6 098 892 800	
21	$(S_3 \wr S_7) \cap A_{21}$, $(S_7 \wr S_3) \cap A_{21}$, $\mathrm{PGL}(3,4)$, $\mathrm{PGL}(3,4)$	29/285	
23	M_{23}, M_{23}	2/130 945 815	

Tables 6 and 7 deal with alternating groups and sporadic groups. Table 8 deals with small almost simple classical groups. Table 9 deals with the 12 sporadic groups having nontrivial outer automorphisms.

4.1. The exceptional case $\Omega^+(8,2)$

The simple group $G = \Omega^+(8,2)$ behaves exceptionally. For Theorem 1.1 and thus also Theorem 1.4, we computed $P_G = 29/42$. To that end, we first excluded most of the candidates for s with calculations involving only permutation characters, and then we considered $P(g,s)$ for the few remaining choices s and the necessary elements g. For Theorem 1.2 and Corollary 1.3, we computed that G has uniform spread 2, with s of order 15, and that, for any triple (x,y,z) of elements in the involution class of size 1575 such that $xy = z$, each element in G generates a proper subgroup of G together with one of x, y, z.

However, G is *not* an exception in Corollary 1.5. By the above, this is clear for $x, y \in G$. The extension $G.3$ of G by a triality automorphism causes no problem because $\langle x, s\rangle = G.3$ holds *for*

Table 7
Sporadic simple groups

G	s^G	$\mathcal{M}(G,s)$	$\sigma(G,s)$	$P(G,s)$
B	47A	$47:23$	$< 1/10^{29}$	
Co_1	35A	$(A_5 \times J_2):2$, $(A_6 \times \mathrm{PSU}(3,3)):2$, $(A_6 \times \mathrm{PSU}(3,3)):2$, $(A_7 \times \mathrm{PSL}(2,7)):2$	421/1 545 600	
Co_2	23A	M_{23}	1/270	
Co_3	21A	$\mathrm{PSU}(3,5).S_3$, $\mathrm{PSU}(3,5).S_3$, $\mathrm{PSL}(3,4).D_{12}$, $S_3 \times \mathrm{PSL}(2,8).3$	64/6325	
Fi_{22}	16A	$2^{10}:M_{22}$, $(2 \times 2^{1+8}):\mathrm{PSU}(4,2):2$, ${}^2F_4(2)'$, ${}^2F_4(2)'$, ${}^2F_4(2)'$, ${}^2F_4(2)'$, $2^{5+8}:(S_3 \times A_6)$	43/585	
Fi_{23}	23A	$2^{11}.M_{23}$, $\mathrm{PSL}(2,23)$	2651/2 416 635	
Fi'_{24}	29A	$29:14$	1/269 631 216 855	
He	14C	$2^{1+6}.\mathrm{PSL}(3,2)$, $7^2:2.\mathrm{PSL}(2,7)$, $7^{1+2}:(S_3 \times 3)$	3/595	
HN	19A	$\mathrm{PSU}(3,8).3_1$	4/34 375	
HS	15A	S_8, $5:4 \times A_5$	64/1155	
J_1	19A	$19:6$	1/77	
J_2	10C	$2^{1+4}:A_5$, $A_5 \times D_{10}$, $5^2:D_{12}$	5/28	
J_3	19A	$\mathrm{PSL}(2,19)$, $\mathrm{PSL}(2,19)$	2/153	
J_4	29A	$29:28$	1/1 647 124 116	
Ly	37A	$37:18$	1/35 049 375	
M	59A	$\mathrm{PSL}(2,59)$	$< 1/10^{24}$	
M_{11}	11A	$\mathrm{PSL}(2,11)$	1/3	1/3
M_{12}	10A	$A_6.2^2$, $A_6.2^2$, $2 \times S_5$	1/3	31/99
M_{22}	11A	$\mathrm{PSL}(2,11)$	1/21	
M_{23}	23A	$23:11$	1/8064	
M_{24}	21A	$\mathrm{PSL}(3,4).S_3$, $2^6:(\mathrm{PSL}(3,2) \times S_3)$	108/1265	
McL	15A	$3^{1+4}:2S_5$, $2.A_8$, $5^{1+2}:3:8$	317/22 275	
$O'N$	31A	$\mathrm{PSL}(2,31)$, $\mathrm{PSL}(2,31)$	10/30 723	
Ru	29A	$\mathrm{PSL}(2,29)$	1/2880	
Suz	14A	$J_2.2$, $J_2.2$, $(A_4 \times \mathrm{PSL}(3,4)):2$	141/5720	
Th	27A	$[3^9].2S_4$, $3^2.[3^7].2S_4$	2/267 995	

each $x \in G.3 \setminus G$. In an extension of type $G.2 \cong \mathrm{SO}^+(8,2)$, there are two G-classes of elements s of order 15 such that each $x \in G.2 \setminus G$ satisfies $\langle x, s\rangle = G.2$, whereas for s chosen in the third G-class of elements of order 15, each element x in the involution class of size 120 in $G.2 \setminus G$ together with s generates a proper subgroup of $G.2$. Since triality permutes the three G-classes of element order 15 (and the subgroups of the type $G.2$ inside $\mathrm{Aut}(G)$) transitively, we cannot choose s from a prescribed conjugacy class of G; but for given elements x, y in groups of type $G.2$ but outside G, we computed that there is always a G-class of elements of order 15 in which each element s satisfies the condition of Corollary 1.5.

4.2. $G = \mathrm{Sp}(2m,q)$

In each of the cases listed for $G = \mathrm{Sp}(2m,q)$ (Table 2), we chose s irreducible of order q^m+1. For $\mathrm{Sp}(6,2)$ and $\mathrm{Sp}(8,2)$, we computed that part (c) (and for the latter group also part (b)) of Proposition 5.8 hold.

4.3. $G = \Omega^{\epsilon}(d, q)$

Table 3 lists the examples computed for orthogonal groups. For $G = \Omega^{-}(2m, q)$, we chose s irreducible of order $(q^m + 1)/\gcd(2, q - 1)$, and for $G = \Omega^{+}(2m, q)$ and $\Omega(2m + 1, q)$, several types of reducible elements (stated in the first column) were used.

The case $G = \Omega^{+}(8, 2)$ has been described in Section 4.1. When $G = \Omega(7, 3)$ or $\Omega^{+}(8, 3)$, we computed P_G in the same way. We also computed that the two groups have uniform spread at least 3.

4.4. $G = \mathrm{SU}(d, q)$

In each of the cases listed for $G = \mathrm{SU}(2m, q)$ (Table 4, lower part), we chose s of type $1 \perp 2m - 1$ and of order $q^{2m-1} + 1$ (for $\mathrm{SU}(2m, q)$ in general, see Proposition 5.22). For the three cases listed for $G = \mathrm{SU}(2m + 1, q)$ (Table 4, upper part), the irreducible element of order $(q^{2m+1} + 1)/(q + 1)$ used in Proposition 5.21 was chosen only for $\mathrm{SU}(5, 2)$; for $\mathrm{SU}(3, 3)$ and $\mathrm{SU}(3, 5)$, the chosen elements of order 6 and 30, respectively, yield better bounds. (N.B.—Each of these elements is a product of a commuting involution and transvection.)

The only unitary groups G in the table for which computing $\sigma(G, s)$ is not sufficient are $\mathrm{PSU}(4, 3)$ and $\mathrm{SU}(4, 2) \cong \mathrm{PSp}(4, 3)$. In the former case, $\sigma(g, s) < 1/3$ except if $g \in G$ is an involution, so it suffices to compute $P(g, s)$ for this choice. In the latter case—which is one of the exceptions in Theorem 1.1—we computed that $P_G = 2/5$ and that the uniform spread of G is at least 3.

4.5. $G = \mathrm{SL}(d, q)$

In each of the cases listed for $G = \mathrm{SL}(d, q)$ (Table 5), we chose s irreducible of order $(q^d - 1)/(q - 1)$, and computed $\sigma(G, s)$ either from the full list of primitive permutation characters of G or from the ratios $|g^G \cap M|/|g^G|$, for $M \in \mathcal{M}(G, s)$ and conjugacy class representatives g of prime order.

4.6. $G = A_n$

Table 6 lists the character-theoretic results for small alternating groups of odd degree n, where s is an n-cycle in each case. The sets $\mathcal{M}(G, s)$ are obtained from GAP's library of transitive groups; the computation of the relevant permutation character values from the natural permutation representation of A_n is straightforward.

For the groups A_5, A_6, and A_7, we computed the values P_G stated in Table 1.

When $G = A_6$ take $s \in G$ of order 4. We calculated that, for each pair of nonidentity elements $x, y \in G$, there exists $g \in G$ such that $\langle x, s^g \rangle = \langle y, s^g \rangle = G$. (Note that $P_G = 5/9$ is attained only for s of order 5, but this choice is not suitable for showing that the spread of A_6 is 2: just choose disjoint 3-cycles x, y.)

The fact that $G = A_5$ and A_6 are exceptions in Theorem 1.2 (which is mentioned already in [6]) follows by showing that any element of G generates a proper subgroup of G with one of $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, $(1, 4)(2, 3)$. For $G = A_7$, we calculated that the uniform spread is exactly 3, with s of order 7.

4.7. Sporadic simple groups

Table 7 lists the results for the sporadic simple groups. For all except the Baby Monster and the Monster, $\mathcal{M}(G,s)$ and $\sigma(G,s)$ are computed using the complete lists of character tables of maximal subgroups in GAP; for the Baby Monster or the Monster, the statement about $\mathcal{M}(G,s)$ follows from [31] and [21], respectively. The notation for the subgroups follows [11]. In [13], essentially the same approach was taken, but the bounds in Table 7 are better for 12 groups (and the bound stated for HN in [13] is incorrect).

For $G = M_{11}$ or M_{12} and $s \in G$ as in Table 7, $\sigma(g,s) = 1/3$ holds exactly for involutions $g \in G$; for all other $g \neq 1$, the value is less than $1/3$. Thus, considering involutions suffices to show that $P(G,s) < 1/3$ in the case $G = M_{12}$, and to show that $G = M_{11}$ has uniform spread at least 3.

4.8. Almost simple groups

Let S be a finite simple group. We say that G is an *automorphic extension* of S if $S \leqslant G \leqslant \mathrm{Aut}(S)$. Tables 8 and 9 list automorphic extensions G of simple groups S by elements of prime order, for classical and sporadic simple groups, respectively.

We do not list the cases where $S = \mathrm{Aut}(S)$. We also do not list the cases where $\mathcal{M}(S,s)$ consists of a single element (for then we can apply Lemma 2.6). The names of the automorphic extensions in Table 8 follow [11]. The case of the simple group $S = \Omega^+(8,2)$ is a bit subtle. The group S contains three conjugacy classes of elements of order 15. In each of the three subgroups of the type $S.2$ in $\mathrm{Aut}(S) \cong S.S_3$, one of these three classes is invariant, and the other two classes are fused, such that each of the three classes is invariant in exactly one subgroup $S.2$ in $\mathrm{Aut}(S)$. We choose an element s of order 15 in S. Then we denote by $\Omega^+(8,2).2$ the $S.2$ subgroup of $\mathrm{Aut}(S)$ that fixes the class s^S, and by $\Omega^+(8,2).2'$ one of the other two $S.2$ subgroups of $\mathrm{Aut}(S)$. A similar situation occurs for $\Omega^+(8,3)$; for this group, we give the information for the simple group $S = \mathrm{P}\Omega^+(8,3)$ not the matrix group $\Omega^+(8,3)$, because not all outer automorphisms of S act on the latter. For G in Table 8 such that $S = F^*(G)$ admits more than one automorphic extension of prime index p then $p = 2$ holds, and there are exactly three different such automorphic extensions, which are called $S.2_1$, $S.2_2$, and $S.2_3$. If these names are not in [11] then $S.2_1$ describes the extension of S by a graph automorphism, and $S.2_2$ describes the extension by a diagonal or field automorphism. (There is no case in the table where both a diagonal and a field automorphism of order two occurs.)

Recall that $\mathcal{M}'(G,s)$ was defined in Section 2.2. If each element of $\mathcal{M}'(G,s)$ intersects S in a maximal subgroup of S, the corresponding line in Table 8 or 9 contains the string "(extensions)" instead of listing $\mathcal{M}'(G,s)$. (The last two columns in Table 9 are needed only for the confirmation that the spread of the automorphism groups of sporadic simple groups is at least two.)

In the character-theoretic considerations, we computed

$$\sigma'(G,s) := \max\bigl\{\sigma(g,s) \bigm| g \in G \setminus S,\ |g| \text{ is prime}\bigr\},$$

so that $P'(g,s) \leqslant \max\{\sigma(S,s), \sigma'(G,s)\}$ for all $1 \neq g \in G$.

Where these bounds on $P'(g,s)$ were not sufficient, we computed

$$P'(G,s) := \max\bigl\{P'(g,s) \bigm| g \in G \setminus S,\ |g| \text{ is prime}\bigr\},$$

Table 8
Automorphic extensions of classical groups

G	$\lvert s\rvert$	$\mathcal{M}(G,s)'$	$\sigma'(G,s)$	$P'(G,s)$
$\mathrm{Sp}(4,4).2$	17	(extensions)	0	
$\mathrm{Sp}(6,3).2$	28	(extensions)	7/3240	
$\mathrm{Sp}(6,4).2$	65	(extensions)	0	
$\Omega^+(8,2).2$	15	(extensions)		1
$\Omega^+(8,2).2'$	15		0	
$\Omega^+(8,2).3$	15		0	
$\mathrm{P}\Omega^+(8,3).2_1$	20	(extensions)	574/1215	
$\mathrm{P}\Omega^+(8,3).2'_1$	20	$\mathrm{PSL}(4,3).2^2$, $3^6:\mathrm{PSL}(4,3).2$, $3^6:\mathrm{PSL}(4,3).2$, $2.\mathrm{PSU}(4,3).[2^3]$, $(A_6\times A_6):[2^3]$	83/567	
$\mathrm{P}\Omega^+(8,3).2_2$	20	(extensions)		1
$\mathrm{P}\Omega^+(8,3).2''_2$	20		0	
$\mathrm{P}\Omega^+(8,3).3$	20		0	
$\Omega^+(8,4).2_1$	65	$(5\times\Omega^-(6,4)).2.2$	$<1/2$	
$\Omega^+(8,4).2_2$	65	(extensions)	0	
$\Omega^+(8,4).2_3$	65	$(5\times\Omega^-(6,4)).2.2$	$<1/2$	
$\Omega^+(8,4).3$	65	$(5\times\mathrm{GU}(3,4)).2$	$<1/2$	
$\Omega^-(12,2).2$	65	(extensions)	1/347 820	
$\Omega(7,3).2$	14	$\mathrm{GO}^-(6,3)$	1/3	
$\mathrm{SU}(3,3).2$	6	(extensions)	2/7	
$\mathrm{SU}(3,5).2$	30	(extensions)	2/21	
$\mathrm{SU}(3,5).3$	30	(extensions)	46/525	
$\mathrm{SU}(4,2).2$	9	(extensions)	7/20	
$\mathrm{SU}(4,3).2_1$	7	$4_2.\mathrm{PSL}(3,4).2_2$, $4_2.\mathrm{PSL}(3,4).2_2$, $4\times\mathrm{PSU}(3,3)\times 2$	76/135	13/27
$\mathrm{SU}(4,3).2_2$	7	$(4\times\mathrm{PSU}(3,3)):2$, $2.(2\times S_7)$, $2.(2\times S_7)$	1/3	
$\mathrm{SU}(4,3).2_3$	7	$4_2.\mathrm{PSL}(3,4):2_3$, $4_2.\mathrm{PSL}(3,4):2_1$, $(4\times\mathrm{PSU}(3,3)):2$	31/162	
$\mathrm{SU}(6,2).2$	33	$\mathrm{GU}(5,2).2$, $3.M_{22}.2$	5/96	
$\mathrm{SU}(6,2).3$	33	$\mathrm{GU}(5,2)\times 3$	59/224	
$\mathrm{SL}(3,4).2_1$	21	(extensions)	3/10	
$\mathrm{SL}(3,4).2_2$	21	$\mathrm{PSL}(3,2)\times S_3$	11/60	
$\mathrm{SL}(3,4).2_3$	21	$(\mathrm{PSL}(3,2)\times 3).2$	1/12	
$\mathrm{SL}(3,4).3$	21	$(9\times 7):3$	1/64	
$\mathrm{SL}(6,2).2$	63	(extensions)	41/1984	
$\mathrm{SL}(6,3).2_1$	364	(extensions)	541/352 836	
$\mathrm{SL}(6,3).2_2$	364	(extensions)	41/882 090	
$\mathrm{SL}(6,3).2_3$	364	(extensions)	25/352 836	
$\mathrm{SL}(6,4).2_1$	1365	(extensions)	$<10^{-5}$	
$\mathrm{SL}(6,4).2_2$	1365	(extensions)	1/34 467 840	
$\mathrm{SL}(6,4).2_3$	1365	(extensions)	1/10 792 960	
$\mathrm{SL}(6,4).3$	1365	(extensions)	1/87 296	
$\mathrm{SL}(6,5).2_1$	3906	(extensions)	$<10^{-4}$	
$\mathrm{SL}(6,5).2_2$	3906	(extensions)	$<10^{-5}$	
$\mathrm{SL}(6,5).2_3$	3906	(extensions)	$<10^{-6}$	
$\mathrm{SL}(10,2).2$	1023	(extensions)	$<10^{-5}$	

Table 9
Automorphism groups of sporadic simple groups

G	s^G	$\mathcal{M}(G,s)'$	$\sigma'(G,s)$	$\hat{s}^G$	$\sigma(G,\hat{s})$
$Fi_{22}.2$	16AB	(extensions)	251/3861	42A	163/1170
$Fi'_{24}.2$	29AB	(extensions)	0	46A	566/5481
$HN.2$	19AB	(extensions)	1/6875	44A	997/192 375
$HS.2$	15A	(extensions)	36/275	30A	36/275
$He.2$	14CD	(extensions)	37/9520	42A	1/119
$J_2.2$	10CD	(extensions)	1/15	14A	1/15
$J_3.2$	19AB	19 : 18	1/1080	34A	77/10 260
$M_{12}.2$	10A	$(2^2 \times A_5) : 2$	4/99	12B	113/495
$M_{22}.2$	11AB	(extensions)	1/21	10A	8/33
$McL.2$	15AB	(extensions)	1/63	22A	1/135
$O'N.2$	31AB	31 : 30	1/84 672	38A	61/109 368
$Suz.2$	14A	(extensions)	661/46 332	28A	1/351

so that $P'(g,s) \leqslant \max\{P(S,s), P'(G,s)\}$ for all $1 \neq g \in G$.

We conclude with remarks concerning some special cases.

$\Omega^+(8,2)$ has been described in Section 4.1.

$G = \mathrm{P}\Omega^+(8,3)$ behaves similar to this group, in the following sense. For an extension of type $G.2_2$ by an involution outside the derived subgroup of $\mathrm{Aut}(G)/G \cong S_4$, the element s cannot be chosen from a prescribed conjugacy class of G but from an $\mathrm{Aut}(G)$-class of elements of order 20. For each element s in G, there is an extension $G.2_2$ such that s and any g in the outer involution class of size 1080 generate a proper subgroup of $G.2_2$.

For A_6, proportions of nongeneration do not help us. In fact, A_6 really is an exception in Corollary 1.5.

We computed that the three groups $\Omega^+(8,2)$, $\mathrm{P}\Omega^+(8,3)$ and A_6 are not exceptions in Corollary 1.5, and that the automorphic extensions $\mathrm{PGL}(2,9)$ and M_{10} of A_6 satisfy $\sigma(\mathrm{PGL}(2,9),s) = 1/6$ and $\sigma(M_{10},s) = 1/9$, with s of order 10 and 8, respectively.

For each sporadic simple group S with full automorphism group $G > S$, the set $\mathcal{M}(G,s)$ is determined using that $\mathcal{M}(S,s)$ is known (see Table 7), and using the information in [11]. Then $\sigma'(G,s)$ is computed either from the character tables of the maximal subgroups in GAP or, if applicable, by extending the known permutation characters of S to G (cf. [9]). We similarly compute $\sigma(G,\hat{s})$ for an element $\hat{s}$ in the nontrivial coset of S. This shows that each of the 12 almost simple groups that are not simple has spread at least four (and much larger in most cases).

5. Classical groups

We now begin the proofs of Theorems 1.1 and 1.2. The latter theorem is clear unless G is one of the exceptional cases in the former one, and these exceptions have been discussed in [20] and in Section 4. We will also prove Theorem 1.4 and Corollary 1.5. Typically, the proofs for the almost simple groups are identical to the proofs for the simple groups.

In this section we will deal with the case of a classical group G defined on a vector space V of dimension d over $F = \mathbb{F}_q$ or $\mathbb{F}_{q^2}$. As noted earlier, here we consider the corresponding linear group G and linear transformations s.

We need to find an element s such that $P(g,s) < 1/3$ for all nonscalar $g \in G$. For this purpose we choose s such that $|\mathcal{M}(G,s)|$ is small (preferably 1). If G contains irreducible cyclic subgroups then it might be reasonable to choose s to generate such a subgroup, so that $\mathcal{M}(G,s)$

consists in almost all cases of groups of extension field type (see [2]). Often, however, a reducible s of carefully chosen shape appears to be easier for our purposes: $|\mathcal{M}(G,s)|$ is smaller. Thus, our philosophy in choosing s is not necessarily to pick an "obvious" element but instead to pick one that will have an "easily" handled collection of maximal overgroups. Consequently, our main difficulty is to (try to) avoid the aforementioned extension field groups (including the case of unitary subgroups of orthogonal or symplectic groups), since the number of them need not even be bounded. However, in some cases, we use irreducible elements even for unbounded dimension and deal with the fact that $\mathcal{M}(s)$ is large.

The element s will be described using $|s|$ and the degrees and structures of its irreducible constituents. For example, $s : 4^- \perp (2m-4)^-$ means that s decomposes the $2m$-dimensional space into the sum of two orthogonal irreducible subspaces (of minus type) of dimensions 4 and $2m-4$, respectively. In the descriptions of the maximal subgroups containing s, for example G_4 denotes the stabilizer of a 4-space implicit in the description of s; and similarly for other subscripts.

5.1. Primitive prime divisors

In the discussion of a group of dimension d defined over $\mathbb{F}_q$ (recall that the natural module is defined over $\mathbb{F}_{q^2}$ in the unitary case), with $q = p^k$ for a prime p, we usually choose s of order divisible by a primitive prime divisor of $p^{ke} - 1$ w.r.t. p (see [19,32]), with $e > d/2$. Then we can apply the classification in [19], which provides a list of those subgroups containing s that belong to one of the following nine classes:

(1) classical [19, Ex. 2.1],
(2) reducible [19, Ex. 2.2],
(3) imprimitive [19, Ex. 2.3],
(4) extension field type [19, Ex. 2.4],
(5) symplectic type [19, Ex. 2.5],
(6) alternating or symmetric (on the heart of the permutation module) [19, Ex. 2.6],
(7) sporadic [19, Ex. 2.7],
(8) Lie type in the same characteristic p [19, Ex. 2.8], and
(9) Lie type in different characteristic [19, Ex. 2.9].

The element s will also have very large order (typically on the order of magnitude q^m where m is the rank of the group). This will eliminate many of the small cases using upper bounds for the order of elements in some of the cases (1)–(9) (see Remark 5.1): s will have order greater than these upper bounds. Also, the element s we choose will have only a small number of invariant subspaces.

As in most of this paper, we need to be careful for small fields and small dimensions.

We make a few remarks which the reader can use to verify our statements about $\mathcal{M}(G,s)$. The natural families of subgroups occurring in the main result of [19] are classical subgroups, subfield subgroups, extension field subgroups, reducible subgroups and imprimitive subgroups. Aside from the latter case, it is quite easy to decide which such subgroups (if any) contain our chosen element s. In particular, using Lemma 2.8, we can often rule out classical subgroups. We now make some remarks about the other cases.

Remark 5.1. (i) In [19, Ex. 2.3], s lies in a wreathed product $\mathrm{GL}(1,q) \wr S_d$, and there is a prime $r \leqslant d$ that divides $|s|$ but not $q-1$. We typically choose our element s to have a small number c of irreducible constituents (often just 2).

This forces s to have c cycles within S_d. It follows that the order of s is less than $(q-1)(d/c)^c$ (strictly less comes from noting that one cycle must have size greater than $d/2$).

(ii) Similarly, in [19, Ex. 2.6(a)], $s \in S_n \times Z$ for $d+1 \leqslant n \leqslant d+2$ and Z cyclic of order $q-1$, and there is a prime $r \leqslant n \leqslant d+2$ that divides $|s|$ but not $q-1$. Note that $S_n \times Z$ is (modulo scalars) self-dual and defined over the prime field. So this case only arises for certain orthogonal and symplectic groups over the prime field. Note that if s corresponds to a permutation with c cycles, then it have will have at least $2c-2$ distinct minimal invariant subspaces and will have an eigenspace of dimension $c-2$. As in the previous case, in essentially every case this forces $c \leqslant 2$, and so s has order less than $n^2/4$ (modulo scalars).

(iii) In [19, Ex. 2.4(a), Ex. 2.5, Ex. 2.6(b)–(c), Ex. 2.7, Ex. 2.8, and Ex. 2.9], the dimension e of the maximal irreducible subspace of the d-dimensional natural module satisfies $e \geqslant d-3$ or $e = d-3$ is even. Moreover, the centralizer of the element of prime order r in the maximal subgroup typically has small order, certainly much smaller than q^m.

Remark 5.2. In order to keep $|\mathcal{M}(G,s)|$ small we often try to choose a reducible element s having invariant subspaces whose dimensions are relatively prime or almost relatively prime. If this is not possible, then we can still avoid some obstacles by using the fact that orthogonal groups do not contain elements acting irreducibly on nondegenerate subspaces of odd dimension greater than 1 (Lemma 2.8).

5.2. The exceptional case $\mathrm{Sp}(2m,2)$

We first deal with $G = \mathrm{Sp}(2m,2)$, $m > 2$, since this family is an anomaly, as indicated in Theorem 1.1. Note that the outer automorphism group is trivial. We begin with a simple observation (where we will always assume that transvections are nontrivial):

Lemma 5.3. *Let* $G = \mathrm{Sp}(2m,q)$ *with* q *even.*

(a) *The number of transvections in* $\mathrm{Sp}(2m,q)$ *is* $q^{2m}-1$.
(b) *The number of transvections in* $\mathrm{O}^\epsilon(2m,q)$ *is* $q^{2m-1} - \epsilon q^{m-1}$.
(c) *The probability that a transvection of* G *lies in* $\mathrm{O}^\epsilon(2m,q)$ *is* $[1 - \epsilon/(q^m+\epsilon)]/q$.

We use this to prove that $\mathrm{Sp}(2m,2)$ does, indeed, provide exceptional situations in Theorem 1.1:

Proposition 5.4. *Let* $G = \mathrm{Sp}(2m,2)$, $m \geqslant 3$. *Let* $g \in G$ *be a transvection and* $s \in G$. *Set* $P_G(g)$ *to be the minimum of* $P(g,s)$ *for* $s \in G$. *Then* $1/2 < P_G(g) \leqslant 2^{m-1}/(2^m-1)$.

Proof. By [22], the only possible maximal subgroup containing a transvection g and an irreducible element h of order 2^m+1 is $\mathrm{O}^-(2m,2)$. Thus, the preceding lemma implies that $P(h,g) = 2^{m-1}/(2^m-1)$.

It remains to show that $P(g,s) > 1/2$ for any $s \in G$.

Any element s of G lies in an orthogonal subgroup $\mathrm{O}^{\pm}(2m,2)$ (this is well known and easy; cf. [28, Lemma 4.1]). If $s \in \mathrm{O}^{-}(2m,2)$ then $P(s,g)$ is at least the probability that a transvection lies in $\mathrm{O}^{-}(2m,2)$, which is $2^{m-1}/(2^m-1)$ by the preceding lemma.

It remains to consider the case in which s lies in an orthogonal group $\mathrm{O}^{+}(2m,2)$. Then s is reducible. If $m=3$, this is easily computed by a computer calculation. So we assume that $m>3$.

Case 1. *s leaves invariant a nondegenerate subspace of dimension $d \leqslant m$.* Then s is in the stabilizer X_d of this d-dimensional space and so is also in some orthogonal group O on V for which this d-dimensional space is nondegenerate. We may assume that $O \cong \mathrm{O}^{+}(2m,2)$.

Whether the d-dimensional space is of $+$ or $-$ type, the total number of transvections in $X_d \cup O$ is at least

$$\begin{aligned}&\left(2^d-1+2^{2m-d}-1\right)+\left(2^{2m-1}-2^{m-1}\right)\\&\quad-\left(2^{d-1}+2^{d/2-1}+2^{2m-d-1}+2^{m-d/2-1}\right)>\left(2^{2m}-1\right)/2.\end{aligned}$$

(The first two terms count the number of transvections in X_d, the next two count the number in O, and the subtracted terms estimate the number in $X_d \cap O$.)

Each of these transvections does not generate G together with s, as required.

Case 2. *s leaves invariant no proper nondegenerate subspace.* Then s also leaves invariant no proper nondegenerate subspace with respect to our chosen orthogonal group O containing s. Consequently, a nonzero s-invariant subspace W of minimal dimension is either totally singular or a nonsingular 1-space for O.

We claim that W can be chosen to be totally singular for O and hence also for G. This is clear if s is unipotent, since then it fixes some nonzero singular vector. If s is not unipotent and W is 1-dimensional then s is 1 on W. Moreover, s leaves invariant the nondegenerate subspace $[h,V]$, where h is the semisimple part of s. Then $[h,V]$ is a nondegenerate subspace of V not containing W, which contradicts the situation in Case 2.

Thus, s must leave invariant some totally singular subspace for both O and G of dimension $d \leqslant m$. Let X_d be the stabilizer in G of this d-dimensional totally singular subspace. Since O has type $+$, the same is true for a Levi factor of $(X_d \cap O)/O_2(X_d \cap O)$. The number of transvections in $X_d \cup O$ is at least

$$\left(2^{2m-1}-2^{m-1}\right)+\left(2^d-1\right)+\zeta \geqslant 2^{2m-1}+2^{m-1}-1,$$

where ζ is 0 if $d=m$ and $2^d\{(2^{2m-2d}-1)-(2^{2m-2d-1}-2^{m-d-1})\}$ otherwise. (Here the first two terms count the number of transvections in O, the next two count the number of transvections in $\mathrm{O}_2(X_d)$, none of which are in O, and ζ counts the number of transvections in $X_d \setminus \mathrm{O}_2(X_d)$ not in O. Note that the last two terms in ζ correspond to $\mathrm{O}^{+}(2m-2d,2)$ when $m-d>0$.)

Each of these transvections does not generate G together with s, as required. □

Remark 5.5. It has been shown in [20, Prop. 2.5] that the spread of $\mathrm{Sp}(2m,2)$, $m \geqslant 2$, is at most 2. Thus, these groups are really exceptions in Theorem 1.2.

5.3. The exceptional case $\Omega(2m+1,3)$, for even m

The family $G = \Omega(2m+1,3)$, for even m, is the second anomaly in Theorem 1.1. If we view $\mathrm{Sp}(2m,2)$ as $\Omega(2m+1,2)$, then the two exceptional infinite series concern odd-dimensional orthogonal groups, and [20, Section 3.2] already shows that the spread for these groups behaves differently than for other groups of Lie type.

As in the previous section, we begin with some simple observations. The following result will be used also for odd m (see Proposition 5.19), so m will be an arbitrary positive integer.

Lemma 5.6. *Let q denote the underlying quadratic form on the natural module V of G. We may fix $Q = \mathrm{diag}(-1,1,1,\ldots,1)$ as the matrix of q, i.e., $q(v) = vQv^{\mathrm{tr}}$ holds for all $v \in V$.*

(a) *G acts transitively on the 1-dimensional subspaces $\langle v\rangle$ of fixed norm $q(v)$. The orbit for $q(v)=0$ has length $(3^{2m}-1)/2$, and the orbit for $q(v)=\pm 1$ has length $3^m(3^m - (-1)^m q(v))/2$.*
(b) *If $q(v)=\pm 1$ then $\langle v\rangle^\perp$ contains $3^{m-1}(3^m+(-1)^m q(v))/2$ nonsingular 1-spaces of each of the norms ± 1, and $(3^{2m-1}-2(-1)^m q(v)3^{m-1}-1)/2$ singular 1-spaces.*
(c) *G has exactly five orbits on the subspaces of codimension 2 in V. For even m, the number of 1-spaces of norm 1 in each such subspace is $3^{m-1}(3^{m-1}\pm 1)/2$ or $3^m(3^{m-2}-1)/2$. For odd m, the number of singular 1-spaces in each such subspace is $(3^{2m-2}-1)/2$ or $(3^{2m-2}\pm 3^{m-1}2-1)/2$.*
(d) *Let U be a quadratic space over a finite field F of odd characteristic such that $U/\mathrm{rad}(U)$ is of $-$ type. Then U contains more than $|U|/|F|$ singular vectors.*

We now turn to the exceptional nature of these groups in Theorem 1.1. Part (d) of the next result states that these groups are, indeed, exceptional.

Proposition 5.7. *Assume that $m \geqslant 4$ is even. Let $g \in G$ with $-g$ a reflection in $\mathrm{GO}(2m+1,3)$, and let $s \in G$ have type $s : 1 \perp 2m^-$ and order $(3^m+1)/2$. Then the following hold.*

(a) *$\mathcal{M}(G,s) = \{M\}$ with $M = G_{2m^-} = N_G(\Omega^-(2m,3))$.*
(b) *$P(g,s) = 1/3$.*
(c) *If $1 \neq h \in G \setminus g^G$ then $P(h,s) < 1/3$.*
(d) *If $1 \neq h \in G$ then $P(g,h) \geqslant 1/3$.*
(e) *For any triple of nonidentity elements $(x,y,z) \in G$, some $s' \in s^G$ satisfies $\langle x,s'\rangle = \langle y,s'\rangle = \langle z,s'\rangle = G$.*

Proof. Let V, q, Q be as in Lemma 5.6, We may assume that $g = -Q$, and $C_V(g)$ is spanned by vectors of norm -1. Let $0 \neq v \in C_V(s)$. The natural module for the subgroup $\Omega^-(2m,3)$ of G can be embedded into the subspace of V spanned by the first $2m$ basis vectors, since the matrix of the quadratic form for $\Omega^-(2m,3)$ can be chosen as $\mathrm{diag}(-1,1,1,\ldots,1)$ if m is even. (If m is odd then the identity matrix can be chosen as the matrix of the quadratic form for $\Omega^-(2m,3)$; in this case, the natural module for the subgroup $\Omega^-(2m,3)$ of G can be embedded into the subspace of V spanned by the last $2m$ basis vectors.) So we have $q(v) = 1$.

Let $W_\pm(h)$ denote the eigenspace of $h \in G$ for the eigenvalue ± 1. Note that each h-invariant 1-space is either singular or lies in one of the subspaces $W_\pm(h)$. Let $\hat{U}$ denote the set of 1-spaces in any subspace U of V.

(a) This follows from [26, Theorem 1.1] since $m > 2$ (cf. Proposition 5.20 below).

(b) If $\mathcal{O} = \langle v\rangle^G$, then G/M and $\mathcal{O}$ are equivalent as G-sets, and $|\mathcal{O}| = 3^m(3^m - 1)/2$, by Lemma 5.6(a).

Clearly $\dim W_-(g) = 2m$ and $\dim W_+(g) = 1$. By Lemma 5.6(b), $P(g,s)|\mathcal{O}| = |\mathrm{Fix}_{\mathcal{O}}(g)| = |\hat{W}_-(g) \cap \mathcal{O}| + |\hat{W}_+(g) \cap \mathcal{O}| = 3^{m-1}(3^m - 1)/2 + 0$, which implies (b).

(c) Both $W_+(h)$ and $W_-(h)$ have codimension at least 2, while at least one of these has dimension at most m. By Lemma 5.6(c), $P(h,s)|\mathcal{O}| = |\hat{W}_+(h) \cap \mathcal{O}| + |\hat{W}_-(h) \cap \mathcal{O}| \leqslant (3^m - 1)/2 + 3^{m-1}(3^{m-1} + 1)/2 < |\mathcal{O}|/3$.

(d) Any $h \in G$ fixes some 1-space $U = \langle u\rangle$, so that

$$P(g,h) = \frac{|\{k \in G \mid \langle h^k, g\rangle < G\}|}{|G|} \geqslant \frac{|\{k \in G \mid U^k \subseteq W_-(g)\}|}{|G|} = \frac{|\hat{W}_-(g) \cap U^G|}{|U^G|}.$$

If $q(u) = 1$ then the right-hand side of this inequality is $(3^{m-1}(3^m - 1)/2)/(3^m(3^m - 1)/2) = 1/3$ (cf. part (b)); if $q(u) = 0$ then the right-hand side is $(3^{m-1}(3^m + 2) - 1)/(3^{2m} - 1) > 1/3$, by Lemma 5.6(b).

The case $q(u) = -1$ is more delicate. Here, we claim that

$$\left|\left\{g' \in g^G \;\middle|\; \langle g', h\rangle \text{ is reducible}\right\}\right| \geqslant \left|g^G\right|/3,$$

which implies (d). Note that $g' \mapsto W_+(g')$ is a bijection from g^G to the set of 1-spaces spanned by vectors of norm -1.

$W = \langle u\rangle^\perp$ is of $+$ type and hence is $\langle h\rangle$-reducible (by Lemma 2.8). A minimal $\langle h\rangle$-invariant subspace W_0 of W is either nondegenerate or totally singular. In either case we will estimate the number of $g' \in g^G$ such that $W_+(g') \subseteq W_0^\perp \cup W$; the group $\langle g', h\rangle$ is reducible for each such g'.

By Lemma 5.6(b), W contains $3^{2m-1} - 3^{m-1}$ norm -1 vectors. We will estimate the number of norm -1 vectors of the form $\pm u + y$ with $y \in W_0^\perp \cap W$ singular; clearly $\pm u + y \in W_0^\perp \setminus W$ and different vectors y produce different conjugates g'.

If W_0 is totally singular then it is contained in a totally singular m-space $\tilde{W} \subseteq W_0^\perp$, and $\pm u + \tilde{W} \subseteq W_0^\perp \setminus W$ consists of $2 \cdot 3^m$ norm -1 vectors.

Assume that W_0 is nondegenerate of dimension k. By Lemma 2.8, either $k = 1$ or W_0 is of $-$ type. If $k = 1$ then $W_0^\perp \cap W$ is a nondegenerate $2m - 1$-space and hence contains 3^{2m-2} singular vectors by Lemma 5.6. If W_0 is of $-$ type then $W_1 = W_0^\perp \cap W$ is also of $-$ type (since W is of $+$ type), and $W_0 \cup W_1$ contains $3^{k-1} + 3^{2m-k-1} \geqslant 2 \cdot 3^{m-1}$ singular vectors by Lemma 5.6.

In each case, we obtain at least $3^{2m-1} - 3^{m-1} + 2 \cdot 3^{m-1} = 2|g^G|/3$ vectors of norm -1 for which the associated group $\langle g', h\rangle$ is reducible, as claimed.

(e) By (b) and (c), it suffices to consider conjugates x, y, z of g. We will show that the sets of fixed points of these three conjugates cannot cover $\mathcal{O}$, since then some conjugate of s fixes a point moved by each of the three given elements, and behaves as required. Since each conjugate of g fixes exactly one third of the points in $\mathcal{O}$, it is enough to show that any two conjugates x, y of g fix a common point in $\mathcal{O}$. This holds by Lemma 5.6(c), because the intersection of the -1 eigenspaces of x and y has codimension 2 in V and thus contains vectors of norm 1. □

Remark. Since our choice of s has $|\mathcal{M}(G,s)| = 1$, Proposition 2.6 implies that $P'(g,s) < 1/2$ for any nontrivial $g \in \mathrm{Aut}(G)$, as required in Theorem 1.4.

5.4. $G = \mathrm{Sp}(2m,q)$, q even and $m \geqslant 2$

The next result is slightly more precise than Theorem 1.1 in this case:

Proposition 5.8. *If $G = \mathrm{Sp}(2m,q)$ with q even and $(m,q) \neq (2,2)$, choose s irreducible of order $q^m + 1$. Then, whenever $1 \neq g \in G$,*

(a) $P(g,s) < 1/3$ *if* $q \geqslant 4$;
(b) $P(g,s) < 1/3$ *if* $q = 2$, $m > 3$, *and g is not a transvection*; *and*
(c) *if* $1 \neq x, y \in G$ *then* $G = \langle s', x\rangle = \langle s', y\rangle$ *for some* $s' \in s^G$.

Proof. Given transvections $x, y \in G$ in the case $q = 2$, by [20, proof of Proposition 3.5] we have $G = \langle x, s'\rangle = \langle y, s'\rangle$ for some $s' \in s^G$. Thus part (c) follows from (a), (b), and Proposition 5.4 (aside from the case $\mathrm{Sp}(6,2)$ which we check directly, see Section 4).

If $(m,q) \neq (4,2)$ then, by [2] and Lemma 2.12, the only maximal overgroups of s are a single $\mathrm{O}^-(2m,q)$ along with one subgroup $M_b \cong \mathrm{Sp}(2m/b, q^b).b$ for each prime b dividing m. (Note that, for odd m, there is a unitary subgroup that contains an irreducible torus, but this subgroup is not maximal as it is contained in $\mathrm{O}^-(2m,q)$.) If g is a transvection then g is not contained in any M_b, so (a) (for transvections) follows by Lemma 5.3. So it suffices to assume that g is not a transvection in order to prove (a) and (b).

Case 1. $m \in \{2,3\}$. By Theorem 2.1, $P(g,s) \leqslant 2(4/3q) < 1/3$ if $q > 8$, or if $q = 8$ and g is contained in exactly one member of $\mathcal{M}(G,s)$. If $q = 8$ and g is contained in both members of $\mathcal{M}(G,s)$ then we apply Lemma 2.3, with $U = N_G(\mathrm{O}^-(2m,q))$ and $H = \mathrm{Sp}(2,q^m)$, and get $\sigma(g,s) \leqslant 4/3q + 4/3q^m + 1/[G:U] < 1/3$. If $q \leqslant 4$, we verify the result directly using GAP (Table 2).

Note that $\mathrm{Sp}(6,2)$ contains elements g of order 3 (with fixed space of dimension 4) with $P(g,s) = 5/14 > 1/3$, hence this group is really an exception in (b).

Case 2. $m \geqslant 4$. If $m = 4$ and $q = 2$, we verify (b) directly using GAP (Table 2). So assume that $q > 2$ or $m > 4$.

In order to complete the proof of Proposition 5.8, as above we have to prove that $(*)$ $P(g,s) < 1/3$ *for any $g \in G$ of prime order that is not a transvection.* By [16, Lemma 3.18], $\mu(g, G/\mathrm{O}^-(2m,q)) \leqslant 1/q^2 + 1/q^m$, so we are done if g is not contained in any M_b.

Let $B = \max\{b \mid g \in M_b\}$. If $B = 2$ then m is even and, by Lemma 3.4 and [16, Lemma 3.18],

$$P(g,s) \leqslant \begin{cases} (1/q^2 + 1/q^m) + 1/q^{2m-3} < 1/3 & \text{for } m > 4, \\ (1/q^2 + 1/q^4) + 1/(q-1)(q^3-1) < 1/8 & \text{for } m = 4 \end{cases}$$

(since $q \geqslant 4$ when $m = 4$), as required.

Thus we may assume that $B \geqslant 3$. Now $g \in \mathrm{Sp}(2m/B, q^B).B$ so that

$$\begin{aligned} \mu\big(g, G/\mathrm{O}^-(2m,q)\big) &= \mu\big(g, \big[\mathrm{Sp}\big(2m/B, q^B\big).B\big] \,/\, \big[\mathrm{O}^-\big(2m/B, q^B\big).B\big]\big) \\ &< 1/q^B + 1/q^m \end{aligned}$$

by [16, Lemma 3.18] (cf. Lemma 3.5); alternatively, apply Lemma 2.3.

Lemma 3.4 yields $\mu(g, G/M_2) \leqslant 1/q^{2m-3}$. We now apply Lemma 2.3 to conclude that $\mu(g, G/M_B) \leqslant 4/3q^B + 1/[G : M_B]$ (using $U = M_B$ and $H = \langle M'_B, g\rangle$) and $\mu(g, G/M_b) \leqslant 4/3q^B$ for all odd $b < B$ (using $U = M_b$ and $H = M_B$). Also note that $[G : M_B] > 2^{m^2/2-m}$.

If $B = 3$ it follows that $m \geqslant 6$ and

$$\begin{aligned} P(g,s) &\leqslant \left(1/q^B + 1/q^m\right) + 1/q^{2m-3} + \left(4/3q^B + 1/[G : M_B]\right) \\ &\leqslant 1/2^3 + 1/2^6 + 1/2^9 + 1/6 + 1/2^{12} < 1/3. \end{aligned}$$

If $B \geqslant 5$ then there are at most $B - 3$ additional summands $4/3q^B$, since there are at most $B - 3$ odd primes up to B. Hence, since $m \geqslant 5$,

$$\begin{aligned} P(g,s) &\leqslant \left(1/q^B + 1/q^m\right) + 1/q^{2m-3} + \left((B-3)4/3q^B + 1/[G : M_B]\right) \\ &\leqslant 1/2^5 + 1/2^5 + 1/2^7 + 8/\left(3 \cdot 2^5\right) + 1/2^7 < 1/3. \end{aligned}$$

This proves $(*)$. □

Remark. Theorem 1.1 for $\mathrm{Sp}(2m, 2)$ now follows by the previous result and Proposition 5.4 (and the computations for the small cases). Now consider the almost simple case: Theorem 1.4. If $q = 2$, then $G = \mathrm{Aut}(G)$ and there is nothing to do. In any case, no two members of $\mathcal{M}(G, s)$ are isomorphic, so we can compute fixed point ratios and the estimates above apply. The result for $\mathrm{Aut}(\mathrm{Sp}(4, 4))$ and $\mathrm{Aut}(\mathrm{Sp}(6, 4))$ is verified using GAP (Table 8).

5.5. $G = \mathrm{Sp}(2m, q)$, q odd

Lemma 5.9. *Let $s \in U = \mathrm{Sp}(m, q^2).2$ with $s : 4 \perp (2m-4)$ and $m > 2$ even. Then s is contained in precisely two G-conjugates of U.*

Proof. The group U is defined over a quadratic extension E of F. The two s-invariant F-subspaces X and Y of dimension 4 and $2m - 4$ are E-spaces of dimension 2 and $m - 2$, respectively. In their guise as E-spaces we will denote them X_E and Y_E.

The eigenvalues of s are a and a^{q^2} on X_E and $b, b^{q^2}, \ldots, b^{q^{2m-6}}$ on Y_E, for some a, b in an extension field L of E (each of these is a full set of Galois conjugates in L). Then the eigenvalues of s are a, a^q, a^{q^2}, a^{q^3} and $b, b^q, \ldots, b^{q^{2m-5}}$ on X and Y, respectively (this time these are full sets of Galois conjugates in L as an extension field of F). In particular, $C_G(s)$ is a maximal torus of order $(q^2 + 1)(q^{m-2} + 1)$ and hence lies in U.

We claim that $s^G \cap U$ splits into two U-classes. For, if $s_1 \in s^G \cap U$ then the eigenvalues of s_1 as an element of U are a Galois orbit of either a or a^q together with a Galois orbit of either b or b^q. This provides us with four possibilities for the eigenvalues of s_1 as an element of G. Moreover, by Proposition 2.9 each of the four possibilities provided by a, a^q and b, b^q gives rise to a U-class of $s^G \cap U$. Since the involutory field automorphism of L is also in U and fixes none of the four eigenvalue possibilities, $s^G \cap U$ consists of precisely two U-conjugacy classes.

Consequently, G has just two orbits on the pairs $(s_1, U_1) \in s^G \times U^G$ with $s_1 \in U_1$, so that $C_G(s) \leqslant U$ has two orbits on the members of U^G containing s, as required. □

Proposition 5.10. *If $m \geqslant 5$, let $\delta = \gcd(2, m)$ and use $s : 2\delta \perp (2m - 2\delta)$ of order $\operatorname{lcm}(q^\delta + 1, q^{m-\delta} + 1)$. Then $\mathcal{M}(G, s) = \{G_{2m-2}\}$ if m is odd, and $\mathcal{M}(G, s) = \{G_{2m-4}, \mathrm{Sp}(m, q^2).2, \mathrm{Sp}(m, q^2).2\}$ if m is even. In both cases, $\sigma(G, s) < 1/3$.*

Proof. Here $|s|$ is divisible by a p-primitive prime divisor of $q^e - 1$, where $e = 2m - 2\delta$. Now check [19, Ex. 2.1 to 2.9] to see that the only possible overgroups are conjugate in G to the ones described.

In particular, when m is even the only proper irreducible overgroups are extension field groups corresponding to quadratic extensions. By Lemma 5.9, there are exactly two possible extension field overgroups of s, as asserted in the proposition.

We will estimate the fixed point ratios. By [16, Proposition 3.16],

$$\mu(g, G/G_{2m-2\delta}) \leqslant 2/q^{m-2} + 1/q^m + 1/q^{k/2} + 1/q^{2m-k} < 1/3,$$

where $k = 2m - 2$ if m is odd and $k = 4$ if m is even. So the only remaining case is that m is even and both g and s are contained in a subgroup $U = \mathrm{Sp}(m, q^2).2$. Then

$$\sigma(g, s) \leqslant \mu(g, G/G_{2m-4}) + 2\mu\big(g, G/\mathrm{Sp}\big(m, q^2\big).2\big) < 1/3$$

by Lemma 3.4. □

Remark. We now deal with the almost simple case (Theorem 1.4) using the same s as in the proposition above. Let S be the socle of $G = \langle S, g\rangle$ with g of prime order. If m is odd, then $|\mathcal{M}(S, s)| = 1$, whence $P'(g, s) < 1/2$ by Proposition 2.6.

Assume that m is even, and let $J := \langle s^{\langle g\rangle}\rangle$ as in Lemma 2.4. We will use a variant of the following argument in several other instances and so we will give full details here. Let M_1 be the stabilizer of the 4-space fixed by s and let M_2 and M_3 denote the other two members of $\mathcal{M}(S, s)$ (see Proposition 5.10).

Lemma 5.11.

(a) $M_2 \cap M_3 \leqslant M_1$;
(b) *if $J < S$, then g normalizes at least one of the M_i; and*
(c) $P'(g, s) \leqslant \sum_{i=1}^{3} \mu(g, S/M_i) < 1/2$.

Proof. (a) For $j = 2, 3$, M_j' is irreducible but not absolutely irreducible, and hence is $C_G(z_j)$ for some $z_j \in \mathrm{GL}(2m, q)$. Clearly, $\langle z_2, z_3\rangle$ is not cyclic and so $U := M_2' \cap M_3'$ is reducible. Moreover, $s^2 \in U$ and s^2 has precisely two invariant subspaces (of distinct dimensions), and hence so does U. Since $M_2 \cap M_3$ normalizes U it preserves each of these subspaces, and hence $M_2 \cap M_3 \leqslant M_1$.

(b) Clearly $J \leqslant M_j$ for some j. Hence $J = J^g \leqslant M_j \cap M_j^g$. If $M_j^g = M_j$, then g normalizes M_j. If not, then $M_j^g = M_i$ for some $i \neq j$. The only possibility is that $\{i, j\} = \{2, 3\}$. Thus, $J \leqslant M_2 \cap M_3 \leqslant M_1$ and $J = J^g \leqslant M_1^g$, whence $M_1^g = M_1$.

(c) Now let x be any conjugate of g. By Lemma 2.4 $\langle s, x\rangle = G$ if and only if $\langle s^{\langle g\rangle}\rangle = S$. So by (b), x fails to generate with s if and only if x normalizes one of the M_i—i.e. x has a fixed

point on S/M_i for some i. Thus, $P'(g,s) \leqslant \sum \mu(g, S/M_i)$. The fact that this sum is less than $1/2$ follows precisely as in the proof of Proposition 5.10. □

This proves Theorem 1.4 for S as in the preceding proposition. We now return to the proof of Theorem 1.1.

Proposition 5.12. *If $2 \leqslant m \leqslant 4$ and $(m,q) \notin \{(2,3),(3,5),(3,7)\}$, let s be irreducible of order q^m+1. Then $\mathcal{M}(G,s) = \{\mathrm{Sp}(m,q^2).2\}$ if $m \in \{2,4\}$ and $\mathcal{M}(G,s) = \{N_G(\mathrm{SU}(3,q)), \mathrm{Sp}(2,q^3).3\}$ if $m=3$. In each case, $\sigma(G,s) < 1/3$.*

Proof. By [2, Main Theorem], every maximal subgroup containing s is of extension field type, and there is only one group of each type by Lemma 2.12. (Note that, for $m=4$, no subgroup of type $N_G(\mathrm{SU}(2,q))$ occurs because the order of that group is not divisible by $|s|$.)

The claim concerning $\sigma(G,s)$ follows from Theorem 2.1 when $m \in \{2,4\}$ and $q \geqslant 5$, and when $m=3$ and $q \geqslant 9$. When G is $\mathrm{Sp}(6,3)$ or $\mathrm{Sp}(8,3)$, we use GAP to show that $\sigma(G,s) < 1/3$ (Table 2). □

The remaining cases of Theorem 1.1 for the groups $\mathrm{Sp}(2m,q)$ are $\mathrm{Sp}(2,q)$, $\mathrm{Sp}(4,3)$, $\mathrm{Sp}(6,5)$, and $\mathrm{Sp}(6,7)$. The case $\mathrm{Sp}(2,q) \cong \mathrm{SL}(2,q)$ is handled below in Section 5.12, and $\mathrm{PSp}(4,3) \cong \mathrm{SU}(4,2)$ is handled below in Section 5.11. For $\mathrm{Sp}(6,5)$ and $\mathrm{Sp}(6,7)$, we choose $s : 2 \perp 4$ of order $\mathrm{lcm}(q+1, q^5+1)$; as in Proposition 5.10, we check [19, Ex. 2.1 to 2.9], and get $\mathcal{M}(G,s) = \{G_2\}$, so Theorem 1.1 holds for these groups by Theorem 2.1.

Remark. The same argument applies to Theorem 1.4. Only $\mathrm{Aut}(\mathrm{Sp}(6,3))$ needs a computational verification, see Table 8.

5.6. $G = \Omega^+(2m,q)$, $m > 4$

Proposition 5.13. *If m is odd, use $s : (m-1)^- \perp (m+1)^-$ of order $(q^{(m-1)/2}+1)(q^{(m+1)/2}+1)/\gcd(4,q-1)$. Then s is contained in a unique maximal overgroup, and $\sigma(G,s) < 1/3$.*

Proof. If $m > 5$ or $q > 2$, the statement about $\mathcal{M}(G,s)$ follows from [19], and [16, Proposition 3.16] (with $k = m+1$ and $l = (m-1)/2$) yields $\sigma(G,s) \leqslant 2/q^{m-2} + 1/q^{m-1} + 1/q^l + 1/q^{2m-k}$, which is less than $1/3$. In the excluded case $G = \Omega^+(10,2)$, we find that $\mathcal{M}(G,s) = \{(\Omega^-(4,2) \times \Omega^-(6,2)).2\}$ holds (for example, by [11, p. 146]), and then use GAP (Table 3). □

Remark. Since $|\mathcal{M}(G,s)| = 1$, Theorem 1.4 follows from Proposition 2.6.

Proposition 5.14. *If m is even, use $s : (m-2)^- \perp (m+2)^-$ of order $(q^{(m-2)/2}+1)(q^{(m+2)/2}+1)/\gcd(4,q-1)$. Then $\mathcal{M}(G,s)$ consists of the reducible subgroup G_{m+2} and precisely two extension field groups of the form $\mathrm{O}^+(m,q^2).2$. Moreover, $P(g,s) < 1/3$.*

Proof. By [32] $\langle s \rangle$ contains an element of prime order acting irreducibly on a subspace of dimension $m+2$. Once again a list of possible overgroups is given in [19], and since $m > 4$ the only possibilities are as stated. The assertion about the number of field extension subgroups containing s is proved exactly as in Lemma 5.9 using Proposition 2.11.

Now let $g \in G \setminus Z(G)$. If g is not contained in one of the extension field groups, then $P(g,s) = \mu(g, G/G_{m+2}) \leqslant 3/q^{m-2} + 1/q^{m-1} + 1/q^{m/2}$ [16, Proposition 3.16]. If $m > 6$ or $q > 2$ then this is smaller than $1/3$; the case $\Omega^+(12,2)$ is handled with GAP (Table 3).

If g is contained in a field extension subgroup, then by Theorem 2.1, together with Lemma 2.3 (with $U = \mathrm{O}^+(m,q^2).2$ and $H = \langle g^U \rangle = \langle g^H \rangle \leqslant U$, where $c = 1$), we have $\mu(g, G/U) \leqslant 4/3q^2 + |\mathrm{O}^+(m,q^2).2|/|G|$. Now $P(g,s) \leqslant 2\mu(g, G/U) + \mu(g, G/G_{m+2})$, and this is less than $1/3$ if either $q \geqslant 5$ or $m \geqslant 8$ and $q \geqslant 3$.

For $G = \Omega^+(12,3)$, we use GAP to compute that $\mu(g, G/N_G(\Omega^+(6,9))) \leqslant 2/88209$. The sum of twice this value and the above estimate for $\mu(g, G/G_{m+2})$ is smaller than $1/3$ (Table 3).

When $q = 2$ and $m > 6$, Lemma 3.5 implies that $\mu(g, G/\mathrm{O}^+(m,4).2) \leqslant 1/2^{13}$. By [16, Proposition 3.16], $\mu(G, G/G_{m+2}) < 1/8$. Thus $P(g,s) < 1/3$. □

Remark. In Theorem 1.4, consider the case $G = \langle g, S \rangle > S = \Omega^+(2m,q)$ with $m \geqslant 6$ even, and choose s as in the proposition.

Let $\mathcal{M}(S,s) = \{M_1, M_2, M_3\}$ with M_1 reducible. Arguing as in the symplectic case (Lemma 5.11), we see that $M_2 \cap M_3 \leqslant M_1$. Thus, $\langle g, s \rangle$ contains S if and only if g does not normalize one of the M_i (cf. Lemma 5.11(b)). Now we argue precisely as in the simple group case using the fixed point ratio estimates above.

The fixed point ratios are the same (with the same proof) for the almost simple group unless g is a reflection (or transvection if q is even). However, in that case g is not in any extension field group and so $P'(g,s) = \mu(g, G/M_1) < 1/2$ (see [18] or [16]).

While the estimates given in the simple group case when $S = \Omega^+(12,3)$ do not give the $1/3$ upper bound for G, they do give the required $1/2$ bound and hence we do not need computer calculations in this case.

So all that remains to consider is when $S = \Omega^+(12,2)$. In this case, we compute that the two extension field subgroups are not conjugate in S but are conjugate in G. It follows that $\mathcal{M}'(G,s) = \{N_G(M_1)\}$ (since $M_2 \cap M_3 \leqslant M_1$), and so $P'(g,s) < 1/2$ as above.

5.7. $G = \Omega^+(8,q)$

Let $G = \Omega^+(8,q) = \Omega^+(V)$ and $F = \mathbb{F}_q$. We deal with $q \leqslant 4$ using GAP computations (Section 4, Tables 3 and 8).

Assume that $q \geqslant 5$. We will use regular semisimple elements. We will need to be somewhat careful so as to avoid, in one situation, a problematic element of this sort.

Lemma 5.15. *There is an element s of order $(q^2+1)/\gcd(2, q-1)$ such that the following hold.*

(a) *$C_G(s)$ is abelian.*
(b) *If q is not a square, then $\mathcal{M}(G,s)$ consists of three subgroups, each with socle $\Omega^-(4,q) \times \Omega^-(4,q)$ modulo $\langle -1 \rangle$.*
(c) *If q is a square, then $\mathcal{M}(G,s)$ consists of the maximal subgroups in* (b)*, together with the normalizer of $\Omega^-(8, \sqrt{q})$.*
(d) *$\sigma(G,s) < 1/3$.*
(e) *The intersection of any two of the maximal subgroups in* (b) *is contained in the third.*

Proof. (a)–(c) Decompose $V = U \perp U^\perp$ using 4^--spaces $U, U^\perp$. We will choose s preserving this decomposition, and having eigenvalues $\alpha, \alpha^q, \alpha^{q^2} = \alpha^{-1}, \alpha^{q^3} = \alpha^{-q}$ on U and $\beta, \beta^q, \beta^{q^2} = \beta^{-1}, \beta^{q^3} = \beta^{-q}$ on $U^\perp$, where $\alpha, \beta \in \mathbb{F}_{q^4}$ have order dividing q^2+1. Namely, *choose α of order $(q^2+1)/\gcd(2, q-1)$ and $\beta \neq 1$ of order dividing $(q^2+1)/\gcd(2, q-1)$ and not the image of α under any automorphism of $\mathbb{F}_{q^4}$*. This is possible since we only have to exclude $1 + 4e$ elements when we choose β (where $q = p^e$), and this is less than $|\alpha|$ since $q > 3$. Then U and $U^\perp$ are not $F[s]$-isomorphic, so that these are the only proper s-invariant 4-spaces. Then $C_G(s)$ leaves each of them invariant and hence is abelian on each of them. Moreover, each element of G of order dividing $(q^2+1)/\gcd(2, q-1)$ lies in a conjugate of the maximal torus $C_G(s)$.

Note that, thus far all we have done is to observe that regular semisimple elements of order $(q^2+1)/\gcd(2, q-1)$ exist.

Clearly s is contained in the stabilizer of $\{U, U^\perp\}$. Triality sends this stabilizer to two further maximal subgroups containing conjugates of s. Thus, s is contained in the maximal subgroups listed in (b). The one in (c) is evident.

There are 75 conjugacy classes of maximal subgroups of (subgroups of $\mathrm{Aut}(G)$ containing) G listed in [23]. A straightforward check of their orders shows that only the above ones have order divisible by $(q^2+1)/\gcd(2, q-1)$, *unless* $q = 5$, s has order 13, and $M = N_G(\mathrm{Sz}(8))$. We avoid this subgroup M by choosing s with slightly more care: if $s' \in M$ has order 13 and agrees with s on U, then make a different choice of $s \neq s'$. This simply adds one additional choice of $\{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}\}$ we need to avoid, still leaving $13 - 1 - 2 \cdot 4$ possibilities for β.

(d) By Lemma 3.7, the subgroups in (b) contribute less than $3 \cdot 8/q^4$ to $\sigma(G, s)$. By Theorem 2.1, for M in (c) we have $\mu(G, M) \leqslant 4/3q$. Thus, $\sigma(G, s) < 24/5^4 + 4/15 < 1/3$.

(e) Let M_1, M_2 and M_3 denote the three subgroups described in (b) with M_1 reducible, and $M_i' = [M_i, M_i]$. Since s leaves precisely 2 invariant proper subspaces on the natural module, the only reducible subgroups containing s are contained in M_1. In particular, M_i' acts irreducibly for $i > 1$. Since M_i' is a central product of two copies of $\mathrm{SL}(2, q^2)$, it has no absolutely irreducible modules of dimension 8 defined over $\mathbb{F}_q$. Arguing as in Lemma 5.11(a) shows that $M_2 \cap M_3 \leqslant M_1$, and applying triality yields (e). □

Remark. Once again consider Theorem 1.4. Let $S = \mathrm{P}\Omega^+(8, q)$ with $q \geqslant 5$, and consider $G = \langle g, S\rangle$ with $g \in \mathrm{Aut}(S) \setminus S$ of prime order. Let $J = \langle s^{\langle g\rangle}\rangle$ as in Lemma 2.4.

It follows as in Proposition 2.6 that, since no two elements of $\mathcal{M}(S, s)$ are S-conjugate, $|\mathcal{M}'(G, s)| \leqslant |\mathcal{M}(S, s)| \leqslant 4$. Thus, by Theorem 2.1, $P'(s, g) \leqslant 4(4/3q) < 1/2$ for $q \geqslant 11$.

So we may assume that $q \leqslant 9$ and hence no prime greater than 3 divides the order of the outer automorphism group of S. In particular, $|g|$ is 2 or 3.

Consider the case $|g| = 3$. If g does not preserve the S-conjugacy classes of the three isomorphic elements of $\mathcal{M}(S, s)$, then $|\mathcal{M}'(G, s)| \leqslant 1$ for $q \neq 9$ and $|\mathcal{M}'(G, s)| \leqslant 2$ for $q = 9$. By Theorem 2.1, $P'(s, g) \leqslant 4/15$ or $2(4/27)$, and hence $P'(s, g) < 1/2$.

The remaining possibility is that $q = 8$ and g induces a field automorphism. By Theorem 2.1, $\mu(g, G/M) < 1/6$ for each $M \in \mathcal{M}'(G, s)$. Note that $N_S(\langle s\rangle)$ has order prime to 3 and that $\langle gsg^{-1}\rangle$ is S-conjugate to $\langle s\rangle$. Thus, 3 divides $|N_G(\langle s\rangle)|$. In the particular, there is an element of order 3 that normalizes s and is in gS. By Lang's Theorem, any such element is conjugate to g. In particular, $g^G \cap N_G(M_1) \cap N_G(M_2) \cap N_G(M_3) \neq \emptyset$, whence $P'(g, s) < \sum \mu(g, S/M_i) \leqslant 1/2$ as required.

Finally, suppose that g is involution. If g is a diagonal automorphism, the proof proceeds precisely as in the simple group case. So we may assume that either g is a graph automorphism or $q = 9$. If $q = 7$ or 8, then $|\mathcal{M}(G, s)| = 2$ and so $P'(g, s) \leqslant 2(4/21) < 1/2$ by Theorem 2.1.

Now consider the case where $q = 5$ or 9 and g is a graph automorphism. Let M_1, M_2, M_3 be the maximal subgroups in Lemma 5.15(b); when $q = 9$ let M_4 be the maximal subgroup in Lemma 5.15(c). After renumbering if needed, we may assume that M_1^g and M_1 are S-conjugate, and hence M_j^g and M_j are not S-conjugate for $j = 2, 3$. So if $J < S$, then J is either contained in M_1, $M_2 \cap M_3$ or M_4. By Lemma 5.15(d), $J \leqslant M_1$ or M_4. Consequently, as in Lemma 5.11(c), by Theorem 2.1 we have $P'(s, g) \leqslant \mu(g, S/M_1) < 1/21$ or $P'(s, g) \leqslant \mu(g, S/M_1) + \mu(g, S/M_4) \leqslant 2(4/27) < 1/3$.

The only remaining case is when $q = 9$ and g is a field automorphism. We may assume that g normalizes M_1. Then we observe that $|M_1| < 2 \cdot 81^6 = 2 \cdot 3^{24}$ and $|g^S| = |S : C_S(g)| > 3^{26}$. Let $T := \langle M_1, g\rangle$. We use the crude strict upper bound $|M_1|/2$ for the number of involutions in $T \setminus M_1$. (This can be seen in many ways. For example, we can use the fact that the total number of involutions in T is at most the sum of the degrees of the distinct irreducible characters of T; moreover, any irreducible character that is nontrivial on $F^*(T)$ has degree at least 9, and $|T/F^*(T)| = 8$, so that the number of involutions in T is less than $|T|/8 = |M_1|/4$. Alternatively, one can compute this in GAP.) Thus, $\mu(g, S/M_1) < 1/9$. By Theorem 2.1, $\mu(g, S/M_4) \leqslant 4/27$. So $P'(s, g) < 3(1/9) + 4/27 < 1/2$, as required.

5.8. $G = \Omega^-(2m, q)$

Proposition 5.16. *If $m \geqslant 11$, use $s : (2m-10)^- \perp 6^- \perp 4^-$ of order $\operatorname{lcm}(q^{m-5}+1, q^3+1, q^2+1)/\gcd(2, q-1)$. Then $\mathcal{M}(G, s) = \{G_{4^-}, G_{6^-}, G_{10^+}\}$, and $\sigma(G, s) < 1/3$.*

Proof. We will use $e = 2m - 10$ in [19, Ex. 2.1 to 2.9] (cf. Section 5.1).

Ex. 2.1 is excluded because $\Omega^-(2m, q_0)$ is impossible by the choice of $|s|$.

Ex. 2.3 and Ex. 2.6(a) are excluded using Remark 5.1. More precisely, s can involve at most 3 cycles and the cycle sizes are at most 1 larger than the dimensions of the irreducible constituents of s. Thus, $|s| \leqslant (q-1)(2m-10+1)(6+1)(4+1)$, which is not the case.

In Ex. 2.4(b), only $b = 2$ can occur since each irreducible constituent of s is defined over the field of size q^b, in particular b divides 4 and 6. This only leaves the possibilities for the normalizers of $\mathrm{SU}(m, q)$ and $\Omega(m, q^2)$, which cannot occur since orthogonal and unitary groups do not contain irreducible elements on both odd- and even-dimensional nondegenerate $\mathbb{F}_{q^2}$-spaces (dimensions 2 and 3 here, see Lemma 2.8 and Remark 5.2).

Ex. 2.6(b)–(c), Ex. 2.4(a), Ex. 2.5, Ex. 2.7, Ex. 2.8, and Ex. 2.9 are excluded by Remark 5.1(iii).

Finally, Ex. 2.2 yields the groups $G_{(2m-4)^+}$, $G_{(2m-6)^+}$, and G_{10^+}. By [16, Proposition 3.16], $\mu(G, G/G_{(2m-4)^+}) + \mu(G, G/G_{(2m-6)^+}) + \mu(G, G/G_{10^+}) \leqslant (2/q^{m-2} + 1/q^m + 1/q^{m-2} + 1/q^4) + (2/q^{m-2} + 1/q^m + 1/q^{m-3} + 1/q^6) + (2/q^{m-2} + 1/q^m + 1/q^{m-5} + 1/q^{10}) < 1/8$. □

Proposition 5.17. *Assume that $m \geqslant 7$ is odd.*

(i) *If $(m, q) \neq (7, 2)$, use $s : (m+1)^- \perp (m-5)^- \perp 4^-$ of order $\operatorname{lcm}(q^{(m+1)/2}+1, q^{(m-5)/2}+1, q^2+1)/\gcd(2, q-1)$. Then $\sigma(G, s) < 1/3$ and $\mathcal{M}(G, s) = \{G_{(m+1)^-}, G_{(m+5)^+}, G_{(2m-4)^+}\}$.*

(ii) *For $\Omega^-(14, 2)$ and an irreducible s of order $2^7 + 1$, $\sigma(G, s) < 1/3$.*

Proof. (i) Let $d = 2m$.

We will use $e = m + 1$ in [19, Ex. 2.1 to 2.9] (cf. Section 5.1).

Ex. 2.1 is excluded because $\Omega^-(2m, q_0)$ is impossible by the choice of $|s|$.

Ex. 2.3 and Ex. 2.6(a) are excluded using Remark 5.1, since $|s| > (q-1)m^2$, which is not the case.

In Ex. 2.4(b), only $b = 2$ can occur since each irreducible constituent of s is defined over the field of size q^b, in particular b divides 4 and 6. This only leaves the possibilities for the normalizers of $\mathrm{SU}(m, q)$ and $\Omega(m, q^2)$, which cannot occur since orthogonal and unitary groups do not contain irreducible elements on both odd- and even-dimensional nondegenerate $\mathbb{F}_{q^2}$-spaces (dimensions 2 and 3 here, see Lemma 2.8 and Remark 5.2).

Ex. 2.6(b)–(c), Ex. 2.4(a), Ex. 2.5, Ex. 2.7, Ex. 2.8, and Ex. 2.9 are excluded by Remark 5.1(iii).

Finally, Ex. 2.2 yields the groups $G_{(2m-4)^+}$, $G_{(m+1)^-}$, and $G_{(m+5)^+}$. By [16, Proposition 3.16], $\mu(G, G/G_{(2m-4)^+}) + \mu(G, G/G_{(m+1)^-}) + \mu(G, G/G_{(m+5)^+}) \leqslant (2/q^{m-2} + 1/q^m + 1/q^{m-2} + 1/q^4) + (2/q^{m-2} + 1/q^m + 1/q^{(m+1)/2} + 1/q^{m-1}) + (2/q^{m-2} + 1/q^m + 1/q^{(m+5)/2} + 1/q^{m-5})$, which is less than $1/3$ if $m \geqslant 9$ or if $m = 7$ and $q > 2$.

(ii) By [2], $\mathcal{M}(G, s) = \{\mathrm{GU}(7, 2)\}$, and then $\sigma(G, s) < 1/3$ (Table 3). □

Proposition 5.18. *If $m \in \{4, 5, 6, 8, 10\}$ and $s \in G$ is irreducible of order $(q^m + 1)/\gcd(2, q-1)$, then $\sigma(G, s) < 1/3$.*

Proof. By [2, Main Theorem] or [26, Theorem 1.1], $\mathcal{M}(G, s)$ consists of extension field type subgroups of G. If m is even then they are of the form $M_b = \Omega^-(2m, q) \cap \mathrm{GO}^-(2m/b, q^b) \trianglerighteq \Omega^-(2m/b, q^b)$, for prime divisors b of m (note that for even m, $\mathrm{GU}(m, q)$ is not an overgroup of s).

Since s acts irreducibly, $\mathcal{M}(G, s)$ contains at most one group for each extension field, by Lemma 2.12.

Let $g \in G \setminus Z(G)$, and set $B = \max\{b \mid g \in M_b\}$. By (2.4), $\sigma(g, s) = \sum_{b \leqslant B} \mu(g, G/M_b)$. Note that we can replace g by a conjugate in G in order to have $g \notin Z(M_B)$. (That is, if g is in this center then it can be viewed as a matrix of blocks, and one of those blocks can be conjugated to a nontrivial power of itself within G while leaving the remaining blocks unchanged, thereby moving g into $M_B \setminus Z(M_B)$.)

The cases $(m, q) \in \{(4, 2), (4, 3), (6, 2)\}$ are handled with GAP (Table 3).

Let $m = 4$, $q \geqslant 4$. Then $\mathcal{M}(G, s) = \{M_2\}$ with $M_2' = \mathrm{PSL}(2, q^4)$. We apply Lemma 2.3, with $U = M_2$ and $H = \langle g^U \rangle = \langle g^H \rangle$, together with elementary bounds [25, Theorem $1'$ and Table 1] on fixed point ratios for $\mathrm{PSL}(2, q^{2B})$, and obtain $\mu(g, G/M_B) \leqslant (q^B + 2)/(q^{2B} + 1) + |M_B|/|G| < 1/3$.

If $m = 6$ and $q \geqslant 3$ then $B \leqslant 3$ and $\mathcal{M}(G, s) = \{M_2, M_B\}$. By Lemma 2.3, again with $U = M_2$ and $H = \langle g^U \rangle = \langle g^H \rangle$, and Theorem 2.1, we get $\mu(g, G/M_2) \leqslant 4/3q^2 \leqslant 4/27$. As in the case $m = 4$, $M_3' \cong \mathrm{PSL}(2, q^6)$ and $\mu(g, G/M_3) \leqslant (q^3 + 2)/(q^6 + 1) + |M_3|/|G| < 5/27$. Thus, $\sigma(g, s) < 4/27 + 5/27 = 1/3$.

If $m = 8$ then $\mathcal{M}(G, s) = \{M_2\}$. Lemma 3.5 yields $\sigma(G, s) \leqslant 1/q^{2m-3} < 1/3$ if q is even, and Lemma 2.3 yields $\sigma(G, s) \leqslant 4/3q^2 < 1/3$ when $q \geqslant 3$.

If $m = 10$ then $B \in \{2, 5\}$ and $\mathcal{M}(G, s) = \{M_2, M_B\}$. As above, if $B = 2$ then $\mu(g, G/M_2)$ is bounded by $4/3q^2 \leqslant 4/27$ for $q \geqslant 3$ and by $1/2^{17} < 1/3$ for $q = 2$. If $B = 5$ then we argue as in the case $m = 6$, and get $\mu(g, G/M_5) \leqslant (q^5 + 2)/(q^{10} + 1) + |M_5|/|G| < 5/27$, which implies $\sigma(g, s) < 4/27 + 5/27 = 1/3$.

If $m = 5$ then $\mathcal{M}(G, s) = \{N_G(\mathrm{SU}(5, q))\}$, so we can use Theorem 2.1 if $q \geqslant 5$. The cases $q = 2$ and $q = 3$ are handled with GAP (Table 3). If $q = 4$ then $\mathcal{M}(G, s) = \{\mathrm{GU}(5, 4)\}$, and the proposition follows from Lemma 3.9. □

Remark. In all the cases above, the same proofs are valid for the almost simple case. Note that GAP computations are needed only for $\Omega^-(12, 2)$, see Table 8.

5.9. $G = \Omega(2m + 1, q)$

The case of even q was dealt with for the isomorphic group $\mathrm{Sp}(2m, q)$; the case $m = 2$ was dealt with for $\mathrm{Sp}(4, q)$; and the case $q = 3$ with even m was dealt with in Section 5.3. Thus, *we may assume that either* $q = 3$ *and* m *is odd, or* $q > 3$ *is odd and* $m \geqslant 3$.

Proposition 5.19. *Assume that* $q = 3$ *and* $m \geqslant 3$ *is odd.*

(a) *If* $m = 3$ *then* $G = \Omega(7, 3)$ *is an exception in Theorem* 1.1 *but has uniform spread at least* 3.
(b) *If* $m \geqslant 5$, *use* $s : [3] \perp (2m - 2)^-$ *of order* $q(q^{m-1} + 1)/2$, *where the invariant* 3*-space is indecomposable and* s *fixes a* (*singular*) 1*-space* L, *say. Then* $\mathcal{M}(G, s) = \{G_1, G_{(2m-2)^-}\}$, *where* G_1 *is the stabilizer of* L, *and* $P(G, s) < 1/3$.

Proof. (a) See Table 3.

(b) The statement about $\mathcal{M}(G, s)$ follows from [19]. Let $\mathcal{O} = L^G$, and let V, q, Q be as in Lemma 5.6.

Case 1. $g \in G$ with $-g$ is a reflection in $\mathrm{GO}(2m + 1, 3)$. We may choose $g = -Q$. Then g fixes a vector of norm -1.

Counting the number of singular 1-spaces in the hyperplane $C_V(-g)$ and using Lemma 5.6, we get

$$\mu(g, G/G_1) = \mu(g, \mathcal{O}) = \frac{3^{m-1}(3^m - 2) - 1}{3^{2m} - 1} < 1/3 - 1/3^{m+1}.$$

We claim that $P(g, s) - \mu(g, G/P_1) < 1/3^{m+1}$, so that $P(g, s) < 1/3$. Note that, in view of $\mathcal{M}(G, s)$, $\{g' \in g^G \mid \langle s, g' \rangle \neq G\}$ is the disjoint union of $g^G \cap G_1$ and $\{g' \in g^G \mid g' \in G_{(2m-2)^-} \setminus G_1\}$. Hence, if V_1 denotes the invariant 3-space of s, then $P(s, g) - \mu(g, G/G_1)$ is the proportion of conjugates g' of g that fix V_1 but not L, and that V_1 must contain the fixed space of any such g'. (The generator of L must involve components v_1, v_{-1} from the ± 1 eigenspaces of g'; the image of $v_1 + v_{-1} \in L$ is $v_1 - v_{-1}$, so v_1 lies in V_1.) Since V_1 contains only six 1-spaces of norm -1 and $-g$ is a reflection, there are at most six possibilities for g'. The claim follows from the fact that $6/|g^G| = 12/(3^m(3^m - 1)) < 1/3^{m+1}$.

Case 2. $1 \neq h \in G \setminus g^G$. Arguing as in the proof of Proposition 5.7(c), we get

$$\mu(h, G/G_1) = \mu(h, \mathcal{O}) \leqslant \frac{(3^m - 1) + 3^{m-1}(3^{m-1} + 2)}{3^{2m} - 1} < 1/9 + 1/3^4.$$

By [16, Proposition 3.16] with $k = 2m-2$ and $l = m-1$,

$$\mu(h, G/G_{(2m-2)^-}) \leqslant 2/q^{m-1} + 1/q^m + 1/q^{m-1} + 1/q^3 \leqslant 2/3^3 + 1/3^5.$$

Thus, $\sigma(h, s) < 2/9$. □

Proposition 5.20. *For $q > 3$, use $s : 1 \perp 2m^-$ of order $(q^m+1)/2$. Then $\mathcal{M}(G, s) = \{G_{2m^-}\}$, and $\sigma(G, s) < 1/3$.*

Proof. The statement about $\mathcal{M}(G, s)$ follows from [26, Theorem 1.1], and [16, Proposition 3.16] yields $\mu(G, G/G_{2m^-}) \leqslant 1/q + 3/q^{m-1} + 1/q^m$, which is less than $1/3$ if $q > 3$. □

Remark. For the almost simple case (Theorem 1.4), we can argue as we did for the simple group. Alternatively, we can argue as in the previous proposition but allow $g \in \mathrm{Aut}(G)$ and also allow $q = 3$ for $m > 3$. This time $|\mathcal{M}(G, s)| = 1$ and so $P'(g, s) < 1/2$.

Only $\Omega(7, 3)$ needs computational verification, see Table 8.

5.10. $G = \mathrm{SU}(2m+1, q)$

Proposition 5.21. *Suppose that $(m, q) \notin \{(1, 3), (1, 5), (2, 2)\}$. If s is irreducible of order $(q^{2m+1}+1)/(q+1)$, then $\mathcal{M}(G, s)$ consists of extension field type subgroups of G of the form $M_b = N_G(\mathrm{SU}(2m+1/b, q^b))$, for prime divisors b of $2m+1$, one overgroup per b. Moreover, $\sigma(G, s) < 1/3$.*

Proof. The statement about the structure of the groups in $\mathcal{M}(G, s)$ follows from [2, Main Theorem], and Lemma 2.12 yields the statement about their number.

Let $g \in G \setminus Z(G)$, and set $B = \max\{b \mid g \in M_b\}$. As usual, we have

$$\sigma(g, s) = \sum_{b \leqslant B} \mu(g, G/M_b).$$

As in the proof of Proposition 5.18, if necessary we can modify g in order to assume that the normal closure H of g in M_B contains M_B'.

Clearly $H = \langle g^H \rangle$ has no fixed points on G/M_b for $b \neq B$ and exactly one fixed point on G/M_B. Thus, by Theorem 2.1 and Lemma 2.3 (with $U = M_b$), $\mu(g, G/M_b) \leqslant 4/3q^B$ if $b \neq B$ and $\mu(g, G/M_B) \leqslant 4/3q^B + 1/[G : M_B]$, so that $\sigma(g, G) \leqslant (B-2) \cdot 4/(3q^B) + 1/[G : M_B] < 1/3$. (As in the proof of Proposition 5.18, the term $B-2$ is a crude upper bound on the number of prime divisors of $2m+1$.) □

The remaining cases for (m, q) are $(1, 3)$, $(1, 5)$, and $(2, 2)$. They are handled using GAP (Table 4).

Remark. The proof of the bound in the proposition for the almost simple case goes through verbatim. The three remaining cases are in Table 8.

5.11. $G = \mathrm{SU}(2m, q)$, $m \geqslant 2$

Proposition 5.22. *Suppose that* $m > 1$ *and* $(m, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. *Take* $s : 1 \perp (2m-1)$ *of order* $q^{2m-1}+1$, *then* $\mathcal{M}(G, s) = \{G_1\}$, *and* $\sigma(G, s) < 1/3$.

Proof. The statement about $\mathcal{M}(G, s)$ follows from [26, Theorem 1.1], and Theorem 2.1 implies the statement about $\sigma(G, s)$ for $q \geqslant 5$. For $m \geqslant 3$, [16, Proposition 3.16] yields $\mu(G, G/G_1) \leqslant 2/q^{2(m-2)} + 1/q^{2m-1} + 1/q^{2l} + 1/q^2$, with $l = m$, which is smaller than $1/3$ if $m > 4$ or $(m, q) \in \{(3, 4), (4, 3), (4, 4)\}$ holds. The cases $(m, q) \in \{(2, 4), (3, 3), (4, 2)\}$ are treated with GAP (Table 4). □

The remaining cases are SU(4, 2), SU(4, 3), and SU(6, 2). They are handled by GAP computations (Table 4); for SU(4, 2), they show that this group is an exception for Theorem 1.1 but not for Theorem 1.2.

Remark. In the almost simple case, Proposition 2.6 yields the result.

5.12. $G = \mathrm{SL}(d, q)$

We begin with large dimensions:

Proposition 5.23. *If* $d \geqslant 8$ *and* $d \neq 11$ *and* $(d, q) \notin \{(8, 2), (10, 2)\}$, *use* $s : e \oplus (d-e)$ *of order* $\mathrm{lcm}(q^e - 1, q^{d-e} - 1)/(q-1)$, *where*

$$e = \begin{cases} (d+1)/2 & \text{if } d \text{ is odd}, \\ d/2 + 2 & \text{if } d \equiv 2 \bmod 4, \\ d/2 + 1 & \text{if } d \equiv 0 \bmod 4. \end{cases}$$

Then $\mathcal{M}(G, s) = \{G_e, G_{d-e}\}$, *and* $\sigma(G, s) < 1/4$.

Proof. We have $d/2 < e \leqslant d-3$. In Ex. 2.1, clearly no $\mathrm{SL}(d, q_0)$ can occur, $\mathrm{Sp}(d, q_0)$ is excluded because e is odd if d is even, and $\Omega(d, q_0)$ is excluded because at least one of e, $d-e$ is odd and $\mathrm{O}(2m+1, q_0)$ does not contain irreducible elements.

Ex. 2.2 yields $\mathcal{M}(G, s) = \{G_e, G_{d-e}\}$, where $\mu(G, G/G_e) = \mu(G, G/G_{d-e}) < 2/q^{d-e} \leqslant 1/8$ by [16, Proposition 3.1(i)]. (N.B.—We are using the fact that our choice of e implies that $\gcd(e, d-e) = 1$, which eliminates the possibility of a unitary overgroup. Note that $d - e \geqslant 4$ holds except if $d \in \{8, 10\}$, so we have $q \geqslant 3$ if $d - e = 3$.)

Ex. 2.3 and Ex. 2.6(a) are excluded by Remark 5.1, since our choice of s satisfies $|s| \geqslant (q-1)(d+2)^2/4$.

All possibilities in Ex. 2.4(a), Ex. 2.5, Ex. 2.6(b) and (c), Ex. 2.7, Ex. 2.8 and Ex. 2.9 are excluded by the fact that either $e \leqslant d-3$ or $e = d-3$ is odd, see Remark 5.1(iii). □

Proposition 5.24. *For* $d = 2$ *and* $q \notin \{4, 5, 7, 9\}$, *or* $d = 3$ *and* $q \neq 4$, *or* $d \in \{4, 5, 7, 11\}$, *let* s *be irreducible of order* $(q^d - 1)/(q-1)$. *Then* $|\mathcal{M}(G, s)| = 1$, *and* $\sigma(G, s) < 1/3$.

Proof. By [2, Main Theorem], any maximal subgroup containing s is of extension field type. If $d \neq 4$ then $\mathcal{M}(G, s) = \{N_G(\langle s \rangle)\}$, while if $d = 4$ then $\mathcal{M}(G, s) = \{N_G(\mathrm{SL}(2, q^2))\}$. Now the result follows from Theorem 2.1 if $q \geqslant 5$. For $d \in \{5, 7, 11\}$ and $q \in \{2, 3, 4\}$, we apply Lemma 3.8,

and get $\sigma(G,s) < 1/2^d < 1/3$. In the cases $(d,q) \in \{(3,2),(3,3),(4,2),(4,3),(4,4)\}$, we compute $\sigma(G,s)$ (Table 5). □

Proposition 5.25. *If $d = 6$ and $q \geqslant 7$, use $s : 5 \oplus 1$ of order $q^5 - 1$. Then $\mathcal{M}(G,s) = \{G_1, G_5\}$, and $\sigma(G,s) < 1/3$.*

Proof. The fact that e is odd excludes Ex. 2.3, Ex. 2.4(a), Ex. 2.5, and Ex. 2.6(a).

Ex. 2.6(b) and (c) are excluded because Tables 2 to 4 in [19] contain no entry with $e = 5$.

Ex. 2.1(b) and (d) cannot occur because e is odd, and (a) (for $q_0 < q$) and (c) cannot occur because $|s|$ is too large.

Ex. 2.2 yields $\mathcal{M}(G,s) = \{G_1, G_5\}$. By [16, Proposition 3.1(ii)], $\mu(G, G/G_1) = \mu(G, G/G_5) < 1/q + 1/q^5$, which is smaller than $1/6$ for $q \geqslant 7$.

Ex. 2.4(b) is excluded because $\gcd(d,e) = 1$.

Ex. 2.7 is excluded because the only cases in [19, Table 5] where $e = 5$ and $d = 6$ are $2.M_{12}$ or $3.M_{22}$, but $|s|$ is too large for these when $q \geqslant 3$.

Ex. 2.8 is excluded because [19, Table 6] contains no entry for e odd.

Ex. 2.9 is excluded because [19, Table 7] contains no entry for $e = 5$, and the only entry for odd e in [19, Table 8] has $\mathrm{PSL}(2,t)$ for $t = 2e + 1 = 11$; but the maximal element order in this group is 11, whereas $|s| \geqslant 1023$. □

In order to complete the proof of Theorem 1.1 for the groups $\mathrm{SL}(d,q)$, it remains to consider the cases $(d,q) \in \{(2,4),(2,5),(2,9),(2,7),(3,4),(6,2),(6,3),(6,4),(6,5),(8,2),(10,2)\}$. The first three are handled below in Section 6 using alternating groups, Proposition 5.24 handles $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$, and the last seven groups are in Table 5.

Remark. The proof of the result in the almost simple case goes through with no changes, including the computational cases (see Section 4.8).

6. The remaining simple groups

In this section we complete the proof Theorem 1.1 by considering the sporadic simple groups, the simple exceptional groups of Lie type, and the simple alternating groups.

Lemma 6.1. *If G is a sporadic simple group different from M_{11} and M_{12} then there exists $s \in G$ such that $\sigma(G,s) < 1/3$. If $G = M_{12}$, $P(G,s) < 1/3$ holds with s of order 12. The group $G = M_{11}$ satisfies $P_G = 1/3$ and has uniform spread at least 3 (with s of order 11).*

If $S = F^*(G)$ is a sporadic simple group with $G \neq S$, then $[G:S] = 2$, and $\sigma'(G,s) < 1/7$ using the same s chosen for the simple group. In particular, sporadic simple groups yield no exceptions in Theorem 1.4.

Proof. See Section 4, Tables 7 and 9. □

The next lemma deals with the exceptional group case of Theorem 1.4.

Lemma 6.2. *If $F^*(G) = S$ is an exceptional simple group of Lie type, there exists $s \in S$ such that $P'(g,s) < 1/3$ whenever $1 \neq g \in G$.*

Proof. For $G_2(4)$, ${}^2F_4(2)'$ and $G_2(3)$, use [16, Proposition 6.2]. In the remaining cases, by [16, Propositions 6.1 and 6.2] we can choose s with $|\mathcal{M}(G,s)| \leqslant 2$, and [24, Theorem 1] yields $\sigma(G,s) \leqslant 2/13$. □

Now we turn to the alternating groups. As in [16, Section 7], these are not as easy to deal with as one might expect. However, even degree is straightforward:

Proposition 6.3. *Each alternating group $G = A_{2m}$, $m \geqslant 4$, contains an element s such that $\sigma(G,s) < 1/3$.*

Proof. Let s be a product of two cycles of relatively prime lengths $m_1 = m - \gcd(2, m-1)$ and $m_2 = m + \gcd(2, m-1)$, as in [6]. Then s lies in a unique maximal subgroup M of A_{2m}: the stabilizer of an m_1-subset (cf. [16, p. 776]). The action on the cosets of M is equivalent to that on the set $\mathbf{X}$ of m_1-subsets of $\{1, 2, \ldots, n\}$. We estimate $\mu(g, G/M)$, for an element $g \in G$ of prime order p, say, using arguments appearing in the proof of [16, Lemma 7.4]. Without loss of generality, let $g = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p)\cdots$.

If p is odd then $\mathrm{Fix}_{\mathbf{X}}(g)$ is contained in $\mathrm{Fix}_{\mathbf{X}}((1, 2, \ldots, p))$, so assume $g = (1, 2, \ldots, p)$. Each fixed point of g is an m_1-set that either contains or is disjoint from $\{1, 2, \ldots, p\}$. Thus, $|\mathrm{Fix}_{\mathbf{X}}(g)| = \binom{2m-p}{m_1} + \binom{2m-p}{m_2} \leqslant \binom{2m-3}{m_1} + \binom{2m-3}{m_2}$, so we may assume that g is a 3-cycle and

$$\mu(g,\mathbf{X}) = \frac{|g^G \cap M|}{|g^G|} = \frac{m_2(m_2-1)(m_2-2) + m_1(m_1-1)(m_1-2)}{2m(2m-1)(2m-2)}$$
$$= \begin{cases} \frac{(2m-2)(m^2-2m+3)}{2m(2m-1)(2m-2)} < 1/4 & \text{if } m \text{ is even,} \\ \frac{(2m-2)(m^2-2m+12)}{2m(2m-1)(2m-2)} < 1/3 & \text{if } m \text{ is odd.} \end{cases}$$

If $p = 2$ then $\mathrm{Fix}_{\mathbf{X}}(g) \subseteq \mathrm{Fix}_{\mathbf{X}}((1,2)(3,4))$, so assume that $g = (1,2)(3,4)$. Each fixed point of g either contains or is disjoint from $\{1, 2, 3, 4\}$, or else contains exactly one of the pairs $\{1, 2\}, \{3, 4\}$. Then $|\mathrm{Fix}_{\mathbf{X}}(g)| = \binom{2m-4}{m_1} + \binom{2m-4}{m_2} + 2\binom{2m-4}{m_1-2}$, and this time we obtain

$$\mu(g,\mathbf{X}) \leqslant \big\{m_2(m_2-1)(m_2-2)(m_2-3) + m_1(m_1-1)(m_1-2)(m_1-3)$$
$$+ 2m_1(m_1-1)m_2(m_2-1)\big\} \,/\, \big(3m(2m-1)(2m-2)(2m-3)\big)$$
$$= \begin{cases} \frac{4(m-1)(m-2)(m^2-m+3)}{3m(2m-1)(2m-2)(2m-3)} < 1/4 & \text{if } m \text{ is even,} \\ \frac{4(m^4-4m^3+14m^2-35m+36)}{3m(2m-1)(2m-2)(2m-3)} < 1/3 & \text{if } m \text{ is odd.} \end{cases} \quad \square$$

In fact, by [6], for $m \geqslant 4$, A_{2m} has uniform spread exactly 4, and the above proof shows that $\mu(g,\mathbf{X}) < 1/4$ also for odd $m \geqslant 9$.

For symmetric groups, we get a similar result:

Lemma 6.4. *Let $G = S_{2m}$ with $m > 3$. Let $s \in A_{2m}$ be a product of two disjoint cycles of length $m+1$ and $m-1$ if m is even or $m \leqslant 7$. If $m > 7$ is odd, let s be a product of two disjoint cycles of lengths $m+2$ and $m-2$. Then $P'(g,s) < 1/2$ for every nontrivial $g \in G$.*

Proof. We may assume that g has prime order p. If $m > 7$ or m is even, the proof above gives the result unless g is a transposition. If g is a transposition, then $1 - P'(g, s) = (m^2 - a)/m(2m - 1)$, where $a = 1$ when m is even and $a = 4$ when m is odd. This gives the result.

If $m = 5$ or 7, then s is contained in precisely two maximal subgroups: the stabilizer of an orbit of $\langle s \rangle$ and the stabilizer of a partition into blocks of size 2; each orbit of $\langle s \rangle$ is a union of blocks. If g is a transposition, then g preserving the partition implies that g preserves each orbit of s (for if g moves a block, it will move at least 4 elements—indeed, the same holds for any cycle of prime length). The probability that a random transposition fixes the orbits of s is $21/45 < 1/2$ (and is even less for a cycle).

So assume that g has more than one orbit. It is straightforward to compute that $\sum |g^G \cap M|/|g^G| < 1/2$ where the sum is over the two elements of $\mathcal{M}(A_{2m}, s)$. □

The case of odd degree is more complicated because no element of A_n has precisely two orbits. We are forced to deal with n-cycles, which can live in several maximal subgroups.

However, there is no problem if we work in S_n:

Lemma 6.5. *Let $n = 2m + 1 > 6$ and $G = S_n$. Let s be the product of two disjoint cycles of length m and $m + 1$. Then s is contained in a unique maximal subgroup, namely $S_m \times S_{m+1}$, and $P'(g, s) < 1/2$ for any nontrivial $g \in G$.*

Proof. Clearly there are no transitive imprimitive groups containing s. Since no primitive group other than A_n or S_n contains a cycle of length less than $n/2$ [30], there are no proper primitive overgroups of s, whence the statement about maximal overgroups of s. As in Lemma 6.3, we reduce to the case where g is a p-cycle for some prime p and then to the case where g is a transposition. Then $1 - P'(g, s) = (m^2 + m)/(m(2m + 1)) > 1/2$. □

It is not hard to show that, if g is a transposition, s is an n-cycle and n is divisible by many small primes, then $1 - P'(g, s)$ can be arbitrarily small (this is already observed in [16, pp. 786–787]). We will see in Proposition 6.8 that $P'(g, s) < 1/3$ when s is an n-cycle and g is not a transposition (in S_n for odd $n \geqslant 9$).

We begin by using Stirling's formula to estimate sizes of conjugacy classes:

Lemma 6.6. *Let $G = A_n$, $n > 24$. Let $x \in S_n$ have prime order p. and assume that x fixes at most $n/2$ of the n points, then $|x^G| \geqslant 2^{3n/4}(n/e)^{n/4}/8\sqrt{\pi n}$.*

Proof. Let x have $t \leqslant n/2$ fixed points. Note that $x^G = x^{S_n}$ except when x is an n or $n - 1$ cycle in which case the result is obviously true. So we assume that this is not the case. If $r = |x|$, then $|C_G(x)| = f(r, t) := t! r^d d!$, where $d = (n - t)/r$. Since we need to estimate the maximum value of $|C_G(x)|$, it follows easily that we may assume that $r = 2$.

First we deal with the case $n = 4m$. It is also straightforward to compute $f(2, t)/f(2, t + 2)$ to see that $f(2, t)$ decreases from $t = 0$ to its minimum and then increases again (note that we must retain the requirement that $n - t$ is even here). Thus, it suffices to prove the inequality when t is 0 or $2m$.

We obtain an estimate when $t = 2m$; it is not difficult to see that this gives the larger centralizer. By Stirling's formula (using upper and lower bounds [27]),

$$\begin{aligned}\left|x^G\right| &= \frac{n!}{2^m m!(2m)!} \\ &\geqslant \frac{\sqrt{2\pi n}(n/e)^n}{2^{n/4}\sqrt{2\pi m}(m/e)^m e^{1/12m}\cdot\sqrt{2\pi 2m}(2m/e)^{2m}e^{1/24m}} \\ &= \frac{\sqrt{2\pi n}(n/e)^n}{\pi(n/2)\sqrt{2}(n/2e)^{3n/4}e^{1/2n}} = \frac{2^{3n/4+1}(n/e)^{n/4}}{\sqrt{\pi n}e^{1/2n}}.\end{aligned}$$

If n is not divisible by 4, choose $1 \leqslant a \leqslant 3$ with $m = n + a$ divisible by 4. We need to estimate the class size of x^G where x is an involution moving at least $m/2$ points. Consider the worst case: $a = 3$. We have an estimate for $|x^{S_m}|$. Note that $|x^{S_{m-3}}| = (m/2-3)(m/2-2)(m/2-1)/m(m-1)(m-2)|x^{S_m}| > |x^{S_m}|/12$. Using the estimate above for $|x^{S_m}|$ shows that

$$\left|x^{S_m}\right| \geqslant \frac{2^{3(n+3)/4+1}(n/e)^{(n+3)/4}}{\sqrt{\pi(n+3)}e^{1/2(n+3)}} > 12\frac{2^{3n/4+1}(n/e)^{n/4}}{\sqrt{\pi n}e^{1/2n}},$$

which yields the result. □

Proposition 6.7. *Each alternating group $G = A_{2m+1}$, $m \geqslant 4$, contains an element s such that $\sigma(G, s) < 1/3$.*

Proof. Let $n = 2m + 1$, and let s be an n-cycle. Table 6 implies the proposition when $4 \leqslant m \leqslant 11$.

Now assume that $n \geqslant 25$. As noted in [16, Proposition 7.6], each group $M \in \mathcal{M}(G, s)$ is of one of the following types:

(a) $N_G(\langle s\rangle)$; this occurs only if n is prime, and there is clearly a unique such group.
(b) $\mathrm{P\Gamma L}(d, q) \cap A_n$, for $n = (q^d - 1)/(q - 1)$, where q is a prime power and $d \geqslant 2$; there are at most $\log_2 n$ possibilities for the pair (q, d) (since clearly $d \leqslant \log_2 n$). For a given d, q with $n = (q^d - 1)/(q - 1)$, we note that there is a single conjugacy class of subgroups in A_n. If the n-cycle s is in $H \cong \mathrm{P\Gamma L}(d, q)$, then the number of conjugates of H containing s is $|N_G(\langle s\rangle) : N_H(\langle s\rangle)| \leqslant (n-1)/d \leqslant (n-1)/2$.
(c) $(S_{n/l} \wr S_l) \cap A_n$ for divisors l of n such that $1 < l < n$; for each l there is a unique such group containing s.

We now estimate the fixed point ratio for each of these cases.

Case (a). By [16, Proposition 7.6], $\mu(g, G/M) \leqslant 2 \cdot (4/(n+1))^{(n-3)/2} < 10^{-8}$.

Case (b). If $M = \mathrm{P\Gamma L}(d, q) \cap A_n$ then we first note that any $g \in M$ fixes less than $n/2$ points (no nontrivial element fixes more than the number of 1-spaces in a hyperplane). We use the very crude bound $\mu(g, G/M) < |M|/|g^G|$.

Note that $|M| < n^{\log_2 n+1}$. Combining this with Lemma 6.6 yields

$$\mu(g, G/M) < 8n^{\log_2 n+1}\sqrt{\pi n}/2^{3n/4}(n/e)^{n/4}.$$

In order to sum over all possibilities for such subgroups M containing a given s, we multiply the right-hand side by $(n-1)(\log_2 n)/2$.

Thus, the probability that g and s are contained in such an M is less than $4n^3 n^{\log_2 n}\sqrt{\pi n}/2^{3n/4}(n/e)^{n/4}$. If $n > 64$, this shows that the sum of the fixed point ratios is less than $(n/e)^{-5} < 20^{-5} < 10^{-6}$.

Suppose that $25 \leqslant n < 64$. The only possible pairs with $d = 2$ have q a power of 2 (since n is odd). So $q = 32$ and $n = 33$ is the only case that occurs (and there will be precisely two such subgroups containing a given n-cycle). Arguing as above (but using the fact that there are only two maximal subgroups in this case and using the explicit formula for $|M|$), we see that the upper bound 10^{-6} is still valid. If $d > 2$, the only possible n and pairs (q, d) are $n = 31$ (for $(q, d) = (2, 5)$ or $(5, 3)$) and $n = 57$ (for $(q, d) = (7, 3)$). For $n = 31$, there are 16 different choices for M and for $n = 57$, there are 12 choices. Again, in each case, we use the above inequality to verify that the bound 10^{-6} is still valid.

Case (c). More work is needed when $M = (S_{n/l} \wr S_l) \cap A_n$. Here l is odd since it is a factor of n. We may assume that $|g| = p$ is prime, that we are permuting $\{1, \ldots, n\}$, and that

$$g = (1, 2, \ldots, p)(p + 1, \ldots, 2p)\cdots,$$

where of course there may only be one nontrivial cycle; we will read mod p within each nontrivial cycle of g. We will use arguments and notation appearing in the proof of [16, Lemma 7.4], cf. the proof of Proposition 6.3.

Subcase (c1). If p is *odd* we will show that

$$\mu(g, G/M) \leqslant \mu\big((1, 2, 3), G/M\big) < 1/l^2. \tag{6.8}$$

Namely, for the first of these inequalities we construct an injection $\theta : \mathrm{Fix}_{G/M}(g) \to \mathrm{Fix}_{G/M}((1, 2, 3))$, as follows. Identify G/M with the set of block systems on $\{1, \ldots, n\}$ with blocks of length n/l, and let $\pi \in \mathrm{Fix}_{G/M}(g)$; this is a partition of our n-set. If $\pi \in \mathrm{Fix}_{G/M}((1, 2, 3))$ then set $\pi\theta = \pi$; otherwise the points $1, 2, 3$ are in three different blocks of π, so π is a partition of the form $(1, i, j, */2, i + 1, j + 1, */3, i + 1, j + 2, */\ldots)$, and we define $\pi\theta = (1, 2, 3, */i, i + 1, j + 2, */j, j + 1, i + 2, */\ldots)$. Then $\pi\theta \in \mathrm{Fix}_{G/M}((1, 2, 3)) \setminus \mathrm{Fix}_{G/M}(g)$, and π can be recovered from $\pi\theta$ because i and j are determined by the fact that $\pi\theta$ has exactly two blocks meeting cycles of g in exactly two points. (Other cycles of g lie either inside blocks of π or meet blocks of π in at most one point.)

For the second part of (6.8), note that $|G/M| = n!/[(n/l)!^l l!]$ and $|\mathrm{Fix}_{G/M}((1, 2, 3))| = (n - 3)!/[(n/l - 3)!(n/l)!^{l-1}(l - 1)!]$ (since each fixed point of $(1, 2, 3)$ has one distinguished block containing $\{1, 2, 3\}$). Thus,

$$\mu\big((1, 2, 3), G/M\big) = (n/l - 1)(n/l - 2)/\big[(n - 1)(n - 2)\big] < 1/l^2,$$

as claimed.

Subcase (c2). Now let $p = 2$. We will show that

$$\mu(g, G/M) < \begin{cases} 8/(n - 1)(n - 2) < 1/69 & \text{if } n/l = 3, \\ (l + 1)/l^3 & \text{otherwise.} \end{cases} \tag{6.9}$$

For that, we will first compute $|\mathrm{Fix}_{G/M}((1, 2)(3, 4))|$, and then compare this with $|\mathrm{Fix}_{G/M}(g)|$.

Each element in $\mathrm{Fix}_{G/M}((1,2)(3,4))$ is of the form $(1,2,*/3,4,*/\ldots)$ or $(1,2,3,4,*/\ldots)$, the latter occurring only for $n/l > 3$. There are $(n-4)!/[(n/l-2)^2 \cdot (n/l)!^{l-2} \cdot (l-2)!]$ fixed points of the first form, and $(n-4)!/[(n/l-4) \cdot (n/l)!^{l-1} \cdot (l-1)!]$ of the second form when $n/l > 3$. The corresponding fixed point ratios are $n/l \cdot (n/l-1)^2 \cdot (l-1)/((n-1) \cdot (n-2) \cdot (n-3)) < (l-1)/l^3$ and $(n/l-1) \cdot (n/l-2) \cdot (n/l-3)/[(n-1) \cdot (n-2) \cdot (n-3)] < 1/l^3$, respectively.

Now we define a map θ from $\mathrm{Fix}_{G/M}(g)$ to $\mathrm{Fix}_{G/M}((1,2)(3,4))$, as follows. Let $\pi \in \mathrm{Fix}_{G/M}(g)$. If $\pi \in \mathrm{Fix}_{G/M}((1,2)(3,4))$ then set $\pi\theta = \pi$. Otherwise π is of the form $(1,3,*/2,4,*/\ldots)$ or $(1,*/2,*/3,*/4,*/\ldots)$. For fixed points of the first kind, we set $\pi\theta = (1,2,*/3,4,*/\ldots)$; this is injective because just the points 2 and 3 are exchanged, and the image clearly does not lie in $\mathrm{Fix}_{G/M}(g)$. For fixed points π of the second kind, if $n/l > 3$ write $\pi = (1,i,j,k,*/2,q,r,s,*/3,*/4,*/\ldots)$, with $i < j < k$, and set $\pi\theta = (1,2,3,4,*/i,q,r,s,*/j,*/k,*/\ldots)$; the image is not fixed by g, and the map is 2 to 1 on the fixed points of this type (because we cannot distinguish i and q). For fixed points of the second kind when $n/l = 3$, we map $\pi = (1,i,j/2,q,r/3,s,t/4,u,v/\ldots)$ to

$$\pi\theta = (1,2,q/3,4,r/i,s,t/j,u,v/\ldots) = (1,3,q/2,4,r/i,s,t/j,u,v/\ldots)\theta.$$

This image is not fixed by g, and θ restricted to the fixed points of the second kind is injective. Thus, each element of $\mathrm{Im}\,\theta$ has at most 2 preimages.

Putting the pieces together, we obtain (6.9): $\mu(g, G/M) < (l-1)/l^3 + 2/l^3$ for $n/l \neq 3$, and $\mu(g, G/M) < 2\mu((1,2)(3,4), G/M) = 2 \cdot 3 \cdot 2^2(n/3-1)/(n-1)(n-2)(n-3) < 1/69$ when $n/l = 3$ (since $n \geqslant 27$).

Completion of the proof of Proposition 6.7. The total contribution of Case (c) subgroups to $\sigma(G,s)$ is thus less than $1/69 + \sum_{k=1}^{\infty}(1/(2k+1)^2 + 1/(2k+1)^3) < 1/69 + (\pi^2/8 - 1) + 6/100 < 1/3 - 10^{-6} - 10^{-8}$.

When combined with our estimates in (a) and (b), this proves the proposition. □

This completes the proof of Theorem 1.1 *for alternating groups other than* A_5, A_6, *and* A_7. The latter groups are handled computationally (Section 4, Table 6).

Proof of Theorem 1.4. We have included Remarks in each section in order to deal with this variation of Theorem 1.1. If $F^*(G) = A_5$ or A_6, the result follows by our computational results. When $G = S_m$, $m > 6$, the result follows from Lemmas 6.4 and 6.5. This completes the proof of Theorem 1.4. □

We conclude with some observations concerning symmetric groups.

Proposition 6.8. *Let* $G = S_{2m+1}$ *with* $m \geqslant 4$. *If* s *is a cycle of length* $2m+1$ (*so* $s \in A_{2m+1}$) *and* g *is neither trivial nor a transposition, then* $P'(g,s) < 1/3$.

Proof. By Lemma 6.7, $P(g,s) < 1/3$ for $g \in A_{2m+1}$ and hence also for any g whose order is greater than 2 (since g^2 will be in A_{2m+1}). So we only need consider the case where g is an involution but not a transposition. In that case the argument used in Lemma 6.7 for elements of

A_{2m+1} applies (for primitive overgroups, there is no difference; for imprimitive overgroups M, we saw that $\mu(g, G/M)$ is largest when g is a product of two disjoint transpositions). □

Finally, we sketch a proof that, when $G = S_{2m+1}$ in Corollary 1.5, we can choose $s \in A_{2m+1}$:

Proposition 6.9. *Let $G = S_n$ with $n \geqslant 5$ odd. If x and y are nontrivial elements of G, then there is an n-cycle s such that $\langle s, x\rangle$ and $\langle s, y\rangle$ both contain A_n.*

Proof. We must find a conjugate of $s' = (1, 2, \ldots, n)$. We may assume that x and y have prime orders p and q, respectively. If neither x nor y is a transposition, the result follows from the previous proposition. So we may assume that $x = (12)$ and hence $G = \langle s', x\rangle$. If y is also a transposition, then we may assume that $y = (13)$ or (34) (by conjugating by an element of $C_G(x)$); in the either case, s' behaves as required. Thus, from now on we assume that *y is not a transposition.*

Note that $P'(s', x) = 1 - \varphi(n)/(n-1)$, since $G = \langle s', w\rangle$ for a transposition $w = (ij)$ if and only if $\gcd(j-i, n) = 1$. As n is odd, for $n \leqslant 100$ we deduce that $P'(s', x) < 1/2$; but $P'(s, y) < 1/3$ by the previous proposition, so the result holds. Hence we may assume that $n > 100$.

We now construct a conjugate $y' = y^g$, $g \in C_G(x)$, such that, among other things, $\langle s', y'\rangle$ *is primitive.* Let $u_1, \ldots, u_m$ be all of the distinct nontrivial divisors of n. Note that even a poor estimate gives $m < \sqrt{n}$ (since $n > 3$ is odd). We choose $g \in C_G(x)$ such that

$$y' = y^g : \begin{cases} 3 \mapsto 4, \\ 3 + u_i \mapsto 5 + 2u_i \quad \text{for } 1 \leqslant i \leqslant m. \end{cases}$$

This can be done since m is small compared to n and there are no coincidences among the numbers $3, 4, 3 + u_i$ and $5 + 2u_j$ (since $3 + u_i$ is even and $5 + 2u_j$ is odd). Observe that $\langle s', y'\rangle$ is primitive. For if not, a nontrivial block system is the set of congruence classes modulo u_i for some i. The block containing 3 is moved by s' to the block containing 4; but 3 and $3 + u_i$ are in the same block, whereas 4 and $(3 + u_i)^y = 5 + 2u_i$ are not. This proves primitivity.

If $\langle s', y'\rangle \geqslant S$ then $s := s'^{g^{-1}}$ behaves as required. Hence, we may assume that $\langle s', y'\rangle$ lies in some maximal overgroup of s' other than S. In Proposition 6.7 we listed the possible such overgroups; there are at most $(n-1)\log_2 n$ of them. Moreover, if f denotes the number of fixed points of y' other than 1, 2, 3, 4 (these points may or may not be fixed), then a glance at these overgroups shows that $f < n/2 - 4$.

Claim. *There is a transposition $t = (k, l)$, $k, l > 2$, such that $\langle s', y'^t\rangle \geqslant S$.*

Once we prove this, clearly $s := s'^{(gt)^{-1}}$ will behave as required since t commutes with x. We restrict k and l as follows:

- $k, l \notin \{1, 2, 3, 4, 3 + u_i, 5 + 2u_j \mid 1 \leqslant i \leqslant m\}$;
- k is moved by y'; and
- if $q = 2$ or 3, then $l \notin k^{\langle y'\rangle}$.

Since $n > 100$, at least $(n - f - 2m - 4)(n - 2m - 6)/2 > (n-1)\log_2 n$ transpositions t meet these conditions. For each of them, y'^t satisfies the same requirements as y' did, and hence $W_t := \langle s', y'^t\rangle$ is primitive.

Suppose that $y'^t = y'^u$ for two distinct such transpositions t, u. Then tu commutes with y', is either a product of two disjoint transpositions or a 3-cycle, and moves a point k, say, moved by y'. This implies that $k^{\langle tu\rangle}$ is an orbit of y', whence $q = 2$ or 3; and we have explicitly excluded this possibility in the construction of our transpositions. Consequently, we obtain more than $(n-1)\log_2 n$ distinct elements y'^t.

If no W_t contains S, then, by the pigeonhole principle, $\langle W_t, W_u\rangle$ is contained in a primitive maximal subgroup M of S (if $y \in S$) or G (if not) for distinct transpositions t, u. Then $y^t(y^u)^{-1}$ is a nontrivial element in M, is a product of at most 4 transpositions, and so moves at most $8 < n/2$ points. However, we already noted that no such overgroup of s' exists. This finally proves our claim, and hence also the proposition. □

It would be preferable to have an elementary proof of the preceding proposition.

References

[1] Á. Bereczky, On the density of generating pairs in projective special linear groups and projective symplectic groups in odd characteristic, PhD thesis, University of Florida, 1999.
[2] Á. Bereczky, Maximal overgroups of Singer elements in classical groups, J. Algebra 234 (2000) 187–206.
[3] G. Binder, The bases of the symmetric group, Izv. Vyssh. Uchebn. Zaved. Mat. 78 (1968) 19–25.
[4] G. Binder, The two-element bases of the symmetric group, Izv. Vyssh. Uchebn. Zaved. Mat. 90 (1970) 9–11.
[5] J.L. Brenner, R.M. Guralnick, J. Wiegold, Two-generator groups. III, in: Contemp. Math., vol. 33, 1984, pp. 82–89.
[6] J.L. Brenner, J. Wiegold, Two-generator groups. I, Michigan Math. J. 22 (1975) 53–64.
[7] J.L. Brenner, J. Wiegold, Two-generator groups. II, Bull. Austral. Math. Soc. 22 (1980) 113–124.
[8] T. Breuer, GAP computations concerning probabilistic generation of finite simple groups, arXiv:0710.3267.
[9] T. Breuer, G. Pfeiffer, Finding possible permutation characters, J. Symbolic Comput. 26 (1998) 343–354.
[10] W.S. Burnside, Theory of Groups of Finite Order, Dover Publications, New York, 1955, unabridged republication of the second edition, published in 1911.
[11] J.H. Conway, R.S. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, An Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
[12] M. Evans, T-systems of certain finite simple groups, Math. Proc. Cambridge Philos. Soc. 113 (1993) 9–22.
[13] S. Ganief, J. Moori, On the spread of the sporadic simple groups, Comm. Algebra 29 (2001) 3239–3255.
[14] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.4, 2004, http://www.gap-system.org.
[15] D. Gorenstein, R. Lyons, R. Solomon, The Classification of the Finite Simple Groups. Number 3, Part I. Chapter A. Almost simple K-groups, Math. Surveys Monogr., vol. 40.3, American Mathematical Society, Providence, RI, 1998.
[16] R.M. Guralnick, W.M. Kantor, Probabilistic generation of finite simple groups, J. Algebra 234 (2000) 743–792.
[17] R. Guralnick, B. Kunyavskii, E. Plotkin, A. Shalev, Thompson-like characterization of the solvable radical, J. Algebra 300 (2006) 363–375.
[18] R.M. Guralnick, K. Magaard, On the minimal degree of a primitive permutation group, J. Algebra 207 (1998) 127–145.
[19] R.M. Guralnick, T. Penttila, C.E. Praeger, J. Saxl, Linear groups with orders having certain primitive prime divisors, Proc. London Math. Soc. 78 (1999) 167–214.
[20] R.M. Guralnick, A. Shalev, On the spread of finite simple groups, Combinatorica 23 (2003) 73–87.
[21] P.E. Holmes, R.A. Wilson, $L_2(59)$ is a subgroup of M, J. London Math. Soc. 69 (2004) 141–152.
[22] W.M. Kantor, Subgroups of classical groups generated by long root elements, Trans. Amer. Math. Soc. 248 (1979) 347–379.
[23] P.B. Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups, J. Algebra 110 (1987) 173–242.
[24] R. Lawther, M. Liebeck, G. Seitz, Fixed point ratios in actions of finite exceptional groups of Lie type, Pacific J. Math. 205 (2002) 393–464.
[25] M.W. Liebeck, J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of Riemann surfaces, Proc. London Math. Soc. (3) 63 (1991) 266–314.
[26] G. Malle, J. Saxl, T. Weigel, Generation of classical groups, Geom. Dedicata 49 (1994) 85–116.
[27] H. Robbins, A remark on Stirling's formula, Amer. Math. Monthly 62 (1955) 26–29.

[28] J. Saxl, G. Seitz, Subgroups of algebraic groups containing regular unipotent elements, J. London Math. Soc. 55 (1997) 370–386.
[29] A. Wagner, Determination of the finite primitive reflection groups over an arbitrary field of characteristic not two. I, Geom. Dedicata 9 (1981) 229–253.
[30] A. Williamson, On primitive permutation groups containing a cycle, Math. Z. 130 (1973) 159–162.
[31] R.A. Wilson, The maximal subgroups of the Baby Monster, I, J. Algebra 211 (1999) 1–14.
[32] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys. 3 (1892) 265–284.

Further reading

[33] P.B. Kleidman, M.W. Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Ser., vol. 129, Cambridge University Press, 1990.
[34] T.A. Springer, R. Steinberg, Conjugacy classes, in: Seminar on Algebraic Groups and Related Finite Groups, The Institute for Advanced Study, Princeton, NJ, 1968/1969, in: Lecture Notes in Math., vol. 131, Springer, Berlin, 1970, pp. 167–266.