Journal of Algebra **234,** 743–792 (2000)
doi:10.1006/jabr.2000.8357, available online at http://www.idealibrary.com on IDEAL®

Probabilistic Generation of Finite Simple Groups[1]

Robert M. Guralnick

Department of Mathematics, University of Southern California, Los Angeles, California 90089-1113
E-mail: guralnic@math.usc.edu

and

William M. Kantor

Department of Mathematics, University of Oregon, Eugene, Oregon 97403-1222
E-mail: kantor@math.uoregon.edu

Communicated by Alexander Lubotzky

Received January 10, 1997

FOR HELMUT WIELANDT ON HIS 90TH BIRTHDAY

For each finite simple group G there is a conjugacy class C_G such that each nontrivial element of G generates G together with any of more than $1/10$ of the members of C_G. Precise asymptotic results are obtained for the probability implicit in this assertion. Similar results are obtained for almost simple groups.

1. INTRODUCTION

It is well known that any finite simple group G can be generated by two elements. In fact, the probability that two elements generate G approaches 1 as $|G| \to \infty$ [Di,KaLu,LiSh2]. In [KaLu] it was asked whether one could obtain an analogous result by using any given nontrivial element

[1] This research was supported in part by the NSF.

0021-8693/00 $35.00

of G together with a random element and still generate G with probability $\to 1$ as $|G| \to \infty$; however, this is not the case [GKS] (for example, a 3-cycle in A_n does not generate A_n together with each element in a large proportion of the group).

This paper has the same theme, but we restrict our random elements to a fixed conjugacy class C_G, chosen so that each element in C_G is contained in very few maximal subgroups. Using estimates for numbers of fixed points of elements on the cosets of these maximal subgroups (which have turned out to be of independent interest), we deduce estimates, whenever $1 \neq g \in G$, for the probability that a random element of C_G together with g generate G. We obtain an absolute lower bound for this probability, as well as asymptotic bounds as the simple group gets large. In particular, if G is a group of Lie type over a field of q elements and $q \to \infty$, then this probability usually tends to 1 (a similar but slightly different result for classical groups is given in [GKS]). We also prove an analogous result for almost simple groups.

In order to state our results more precisely, we introduce some notation. For any finite group G, let $O_\infty(G)$ denote the last term in the derived series for G. Let $\mathrm{PC}(G)$ denote the following conditional probability:

$$\mathrm{PC}(G) = \max_{1 \neq s \in G} \min_{1 \neq g \in G} \Pr\left\{\langle g, s' \rangle \geq O_\infty(G) \mid s' \in s^G\right\}.$$

Note that, for an almost simple group G with socle S, $\mathrm{PC}(G) = \max_{1 \neq s \in G} \min_{1 \neq g \in G} \Pr\{\langle g, s' \rangle \geq S \mid s' \in s^G\}$. (A group is called *almost simple* if it lies between S and $\mathrm{Aut}(S)$ for some nonabelian finite simple group S.)

Thus, for at least one conjugacy class $C_G = s^G$, $\mathrm{PC}(G)$ is a lower bound for the proportion of members of C_G each of which generates a subgroup containing $O_\infty(G)$ together with any given nontrivial $g \in G$. Using this notation we will prove the following two theorems:

THEOREM I. *If G is a finite almost simple group then* $\mathrm{PC}(G) > 1/10$.

THEOREM II. $\liminf\{\mathrm{PC}(G)$ *for G almost simple*$\} = \liminf\{\mathrm{PC}(G)$ *for G simple*$\} = 1/2$.

We will obtain more than just the stated lim infs. If (G_i) is any sequence of pairwise nonisomorphic groups of Lie type then $\lim \mathrm{PC}(G_i) = 1$ unless (G_i) contains a subsequence (G_{i_j}) with $G_{i_j} \trianglerighteq \Omega(2m_{i_j} + 1, q)$ for a fixed prime power q, in which case $\lim \mathrm{PC}(G_{i_j}) = 1 - 1/q$. The value of $\mathrm{PC}(A_n)$ is related to arithmetical properties of n; we find that $\liminf \mathrm{PC}(A_{2l+1}) = 8/\pi^2 \approx 0.811$ and $\liminf \mathrm{PC}(A_{2l}) = 3/4$. Moreover, $\liminf \mathrm{PC}(A_{n_i}) = 1$ if and only if the smallest prime dividing n_i tends to infinity. More precise information concerning $\mathrm{PC}(A_n)$ is obtained in Section 7 (cf. Remark 2 at the end of the section), where it is also shown that $[1/2, 1]$ is the set of limit points of $(\mathrm{PC}(S_n))$. One surprising fact is that, for infinitely many n, $\mathrm{PC}(S_n)$ is not attained when C_G consists of n-cycles; instead it is attained by elements s having two cycles of length approximately $n/2$. Somewhat similarly, for many of the classical groups we use elements s having two irreducible constituents on the underlying vector space, of approximately the same degrees. In some of these cases there is in general no single optimal choice for the set of conjugates of $\langle s \rangle$.

It is natural to ask whether the requirement $\langle g, s' \rangle \geq O_\infty(G)$ in the definition of $\mathrm{PC}(G)$ is too weak: perhaps we should have required that $\langle g, s' \rangle = G$ provided that G is cyclic modulo its socle S (if G/S is not cyclic, then taking $g \in S$ shows that not every element has a mate such that the pair generate). However, this stronger notion would not give the desired type of lim inf even when G is a symmetric group (cf. Remark 1 at the end of Section 7).

The above theorems do not imply the results in [Di,KaLu,LiSh2]. On the other hand, Theorem I implies, in particular, the following property of simple groups, called "$1\frac{1}{2}$ generation" (cf. [DT, Wo]). The property was first conjectured by Steinberg [Ste] in 1962, who observed that his conjecture, "if true, would quite likely require methods much more detailed than those used here."

COROLLARY. *Any nontrivial element of a finite almost simple group G belongs to a pair of elements generating at least the socle of G.*

This can be proved using less effort than we employ here for Theorem I. In particular, if x is an element contained in at most 2 maximal subgroups of a simple group G, then $G = \langle g, x^{y(g)} \rangle$ for any nontrivial element g and some $y(g) \in G$ (see [G2, 2.2]). In most cases one can produce such an element x.

The proofs of the theorems rest on the classification of finite simple groups. However, when G is alternating or classical, a more elementary proof of Theorem I is possible (but with a poorer bound); the case $\mathrm{PSL}(d, q)$ is contained in [Ka3], using very elementary methods, while the alternating groups are dealt with in (7.1) below. All proofs of this type of result follow similar patterns: bounding the number of ways *not* to generate G by using information concerning maximal subgroups of G.

For any $a, b \in G$ write $P_a(b) = \Pr\{\langle a', b \rangle \not\geq O_\infty(G) \mid a' \in a^G\}$. Then $P_a(b) = P_b(a) = \Pr\{\langle a', b' \rangle \not\geq O_\infty(G) \mid a' \in a^G, b' \in b^G\}$ and $\mathrm{PC}(G) = \max_{1 \neq s \in G} \min_{1 \neq g \in G}(1 - P_s(g))$. Thus, we focus on estimating $P_s(g)$ for carefully chosen s as indicated above and for all $g \neq 1$. This is discussed from a general viewpoint in Section 2, relating our task to estimating fixed point ratios of elements of permutation groups. Section 3 provides some such estimates for the classical groups, leading to a proof of the theorems for these groups in Sections 4 and 5. Exceptional and sporadic groups are dealt with in Section 6, while the alternating and symmetric groups are considered in Section 7. We have already mentioned that the latter cases lead to many of the situations we encounter in which a subsequence of a sequence in Theorem II converges to a limit other than 1; hence they require more effort than might be expected.

Our results on simple groups were presented at the Groups and Geometries Conference in Siena in September 1996 shortly before the present paper was submitted. Later some of the results were stated in [GH] and a proof of the corollary for simple groups was given in [St]. We are grateful to T. Breuer and G. Malle for providing us with GAP computations, and to J. Buhler, Z. Reichstein, and A. Shalev for helpful comments. Finally, we thank the referee for his helpful comments, including the suggestion that we should extend our earlier results to almost simple groups.

2. FIXED POINT RATIOS; NOTATION

All groups will be finite, as will the sets on which they act. For any action of a group 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, and the *fixed point ratios*

$$\mu(g, \mathbf{X}) = |\mathrm{Fix}_{\mathbf{X}}(g)|/|\mathbf{X}| \qquad \text{and}$$

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

These are related to $P_s(g)$ and hence to $\mathrm{PC}(G)$ as follows. Let $s \in G$ be such that the conjugacy class $s^{O_\infty(G)}$ generates a subgroup containing $O_\infty(G)$. If $g \in G$, then $P_s(g) = P_g(s) \le \Sigma_{M \in \mathscr{M}(s)} |g^G \cap M|/|g^G|$, where $\mathscr{M}(s)$ is the set of all subgroups M of G containing s and maximal with respect to not containing $O_\infty(G)$ (in particular, if G is simple, then $\mathscr{M}(s)$ is precisely the collection of maximal *overgroups* of s in G). If M^G denotes the conjugacy class of $M \in \mathscr{M}(s)$, then

$$\mu(g, M^G) = |g^G \cap M|/|g^G| \le |M|/|g^G| \tag{2.1}$$

(we use the fact that $M = \mathrm{N}_G(M)$, which follows from the maximality of M together with our hypothesis $O_\infty(G) \le \langle s^{O_\infty(G)} \rangle \le \langle M^{O_\infty(G)} \rangle$). In particular,

$$P_s(g) \le \sum_{M \in \mathscr{M}(s)} \mu(g, M^G). \tag{2.2}$$

Thus, it suffices to estimate $\mu(G, \mathbf{X})$ for suitable choices of $\mathbf{X}$. Note, however, that (2.2) is a crude estimate, since it ignores the overlaps of members of $\mathscr{M}(s)$.

For any group G, let $\mu(G) = \max\{\, \mu(G, \mathbf{X}) \mid G$ is nontrivial and primitive on $\mathbf{X}\}$. Also, let $F^*(G)$ denote the generalized Fitting subgroup of

G—we will not define this here, but note that if G is almost simple then $F^*(G)$ is the socle of G. The proof of Theorem II for classical groups over fields of size $q \to \infty$ uses (2.2) together with a difficult general upper bound for $\mu(G)$ obtained by Liebeck and Saxl:

THEOREM 2.3 [LiSa]. *Suppose that $S = F^*(G)$ is a simple group of Lie type over $\mathbb{F}_q$ not isomorphic to any 2-dimensional linear group, alternating group or* PSp(4, 3). *Then $\mu(G, M^G) \leq 4/3q < 9/10$ for any maximal subgroup M of G. In particular, $\mu(G, M^G) \to 0$ as $q \to \infty$.*

In order to use this for Theorem II we merely need to choose s so that $|\mathscr{M}(s)|$ stays bounded as $q \to \infty$. This theorem also shows that Theorem I holds for groups of Lie type provided that $|\mathscr{M}(s)| = 1$.

The next section provides some more precise bounds for $\mu(G, \mathbf{X})$ in the case of classical groups in natural permutation actions. Exceptional groups of Lie type will be dealt with in Section 6.

We will use (2.2) in conjunction with another simple observation:

LEMMA 2.4. *Let $A < B < G$. If all G-conjugates of A lying in B are B-conjugate, then A lies in $|\mathrm{N}_G(A) : \mathrm{N}_G(B) \cap \mathrm{N}_G(A)|$ conjugates of B. In particular, if also B is self-normalizing, then A lies in $|\mathrm{N}_G(A) : \mathrm{N}_B(A)|$ conjugates of B.*

Another well-known and elementary result about fixed points is the following:

LEMMA 2.5. *If G acts transitively on a set $\mathbf{X}$ and $g \in G$, then*

$$|\mathrm{Fix}_{\mathbf{X}}(g)| = \sum_i |\mathrm{C}_G(g_i) : \mathrm{C}_H(g_i)|,$$

where H is the stabilizer of a point in $\mathbf{X}$ and the g_i are a set of representatives for the H-conjugacy classes that intersect the G-conjugacy class of g.

3. SOME FIXED POINT RATIOS FOR CLASSICAL GROUPS

Recall that a group is called *quasisimple* if it is perfect and simple modulo its center. Let S be a quasisimple classical (linear) group defined on a d-dimensional vector space V over $\mathbb{F}_q$ (or $\mathbb{F}_{q^2}$ in the unitary case). In this section we will consider groups G such that $S \leq G \leq \mathrm{N}_{\Gamma\mathrm{L}(V)}(S)$: for each type of group we need to consider the number of fixed points of an r-element $g \in G$ whose order modulo scalars is the prime r. More precisely, we will provide bounds on $\mu(g, M^G)$ for various subgroups M of G. On occasion we will replace G by $G/Z(S)$, which will not effect any of our estimates (since $Z(S)$ always acts trivially in the permutation representations we consider).

Some unpublished results are known for the groups $\mathrm{PSL}(d,q)$ [Sh]; for the remaining classical groups [Pu] contains related estimates when q is sufficiently large.

3.1. $\mathrm{SL}(d,q)$

PROPOSITION 3.1. *Let $G = \Gamma\mathrm{L}(V) = \Gamma\mathrm{L}(d,q)$, and let $\mathbf{S}_k$ denote the set of all k-spaces of V, where $1 \le k \le d/2$. Then*

(i) $\mu(G,\mathbf{S}_k) < 2/q^k$, *and*

(ii) $\mu(G,\mathbf{S}_1) < \min\{1/2, 1/q + 1/q^{d-1}\}$.

Proof. Let $g \in G$ act nontrivially on $\mathbf{S}_k$. We may assume that g has prime order modulo $Z(G)$ and is semisimple, unipotent, or a field automorphism. There are four cases to consider:

Case A. *g is semisimple and acts homogeneously on V* with each irreducible submodule having dimension e, where $1 < e \mid k$ and $e \mid d$.

Case B. *g is semisimple and does not act homogeneously on V*. Then $V = V_1 \oplus V_2$ for nonzero g-invariant subspaces V_i having no common $\langle g \rangle$-irreducible constituent, and $\dim V_1 = e$ where $1 \le e \le d/2$.

Case C. *g is unipotent.*

Case D. *g is a field automorphism of prime order.*

As usual, write $[{d \atop k}]_q = |\mathbf{S}_k|$ (a "Gaussian coefficient"), or just $[{d \atop k}]$ when the field is evident.

LEMMA 3.2. *If Case* A *holds, then* $\mu(g,\mathbf{S}_k) < 1/q^k$.

Proof. In this case g preserves an $\mathbb{F}_{q^e}$-linear structure on V and indeed with respect to this structure acts as a scalar that generates $\mathbb{F}_{q^e}/\mathbb{F}_q$. Note that if g has any k-dimensional invariant subspace, then $e \mid k$ and $\mathrm{Fix}_{\mathbf{S}_k}(g)$ is the set of k/e-spaces of V viewed as a d/e-dimensional $\mathbb{F}_{q^e}$-space. So

$$\mu(g,\mathbf{S}_k) = \begin{bmatrix} d/e \\ k/e \end{bmatrix}_{q^e} \Bigg/ \begin{bmatrix} d \\ k \end{bmatrix}_q < (q^e)^{(k/e)(d/e)-(k/e)^2+(k/e)}/q^{k(d-k)} \le 1/q^k.$$

∎

LEMMA 3.3. *Assume Case* B *holds. Then*

(a) $\mu(g,\mathbf{S}_k) < 2/q^k$;

(b) *if* $k = 1$, *then* $\mu(g,\mathbf{S}_k) < 1/q + 1/q^{d-1}$; *and*

(c) *if* $q = 2$, *then* $\mu(g,\mathbf{S}_k) < 1/4$.

Proof. (a), (b) Note that $\mathrm{Fix}_{\mathbf{S}_k}(g)$ is contained in the set Γ of k-spaces of the form $X_1 \oplus X_2$ with $X_i \subseteq V_i$, where

$$|\Gamma| = S(e \oplus (d-e); k) := \sum_{j=0}^{\min\{e,k\}} \begin{bmatrix} e \\ j \end{bmatrix}_q \begin{bmatrix} d-e \\ k-j \end{bmatrix}_q. \qquad (3.4)$$

Thus, we may apply (3.7) below in order to conclude that (a) and (b) hold.

(c) Suppose that $q = 2$ and $k \le 2$. If g has no fixed points on V, then the argument of the previous lemma yields the result. Thus, we may assume that g is trivial on V_1 or V_2 and has no invariant 1-spaces on the other subspace. Let $d_1 = \dim \mathrm{C}_V(g)$ and $d_2 = \dim[g, V]$ (one of these is e).

If $k = 1$, the number of invariant k-spaces is $2^{d_1} - 1 \le 2^{d-2} - 1$ and so (c) holds.

If $k = 2$, then the number of 2-dimensional g-invariant subspaces of V is the number of 2-dimensional g-invariant subspaces of $\mathrm{C}_V(g)$ plus the number of 2-dimensional g-invariant subspaces of $[g, V]$. It is easily seen that an upper bound for the latter is $4^{d_2/2}/3$ where d_2 is the dimension of the subspace generated by the 2-dimensional $\langle g \rangle$-irreducible subspaces. Thus, the total number of invariant 2-spaces is at most $(2^{d_1} - 1)(2^{d_1 - 1} - 1)/3 + 4^{d_2/2}/3$. This quantity is largest when $d_1 = d - 2$ and $d_2 = 2$, and the result follows.

If $k > 2$, the result follows from (a). ∎

LEMMA 3.5. *Assume Case* C *holds. Then*

(a) $\mu(g, \mathbf{S}_k) < 2/q^k$; *and*

(b) *if* $k = 1$, *then* $\mu(g, \mathbf{S}_k) < 1/q$.

Proof. We may replace g by a polynomial in g and hence assume that the minimal polynomial of g is $(T-1)^2$. Let $W = [g, V]$ and $e = \dim W$. Then $W \subseteq \mathrm{C}_V(g)$ and hence $e \le d/2$.

Given a j-space J of W with $j \le k$, we will count the number of g-invariant k-spaces U of V such that $U \cap W = J$. Here U/J is an g-invariant subspace of V/J such that $0 = (U/J) \cap (W/J) \supseteq [U/J, g]$, so that U/J is a $(k-j)$-space of $\mathrm{C}_{V/J}(g)$. Clearly $\dim \mathrm{C}_{V/J}(g) = (d-j) - \dim[V/J, g] = (d-j) - (e-j) = d - e$. Thus, J produces at most $\left[{d-e \atop k-j}\right]$ choices for U. It follows that the number of g-invariant k-spaces of V that intersect W in a j-space is at most $\left[{e \atop j}\right]\left[{d-e \atop k-j}\right]$. Then $|\mathrm{Fix}_{\mathbf{S}_k}(g)|$ is bounded above by the quantity $S(e \oplus (d-e); k)$ in (3.4), and (a) follows from (3.7) below.

If H is any g-invariant hyperplane containing $\mathrm{C}_V(g)$, then every g-invariant 1-space is contained in H. Thus, if $k = 1$, then $\mu(g, \mathbf{S}_k) < 1/q$, which proves (b). ∎

LEMMA 3.6. *Assume Case* D *holds. Then* $\mu(g, \mathbf{S}_k) < 2/q^{k(d-k)/2} \le 2/q^k$ *for* $d \ge 3$ *and* $\mu(g, \mathbf{S}_1) \le 1/(q+1)$.

Proof. Let g be a field automorphism of prime order r. Let $D = \mathrm{PGL}(V)$. There is a unique conjugacy class of elements of order r in the coset gD (cf. [GL, 7.2]), so we may take g to be the standard field automorphism. Indeed the same argument shows that there is also a unique such class in gK where K is the stabilizer of a point in $\mathbf{S}_k$. From (2.5) it follows that the number of fixed points of g is precisely $|\mathrm{C}_G(g) : \mathrm{C}_K(g)|$, i.e., the number of k-subspaces over the fixed field of g. A straightforward computation now yields the result. ∎

We now turn to a combinatorial observation that is crucial for the above arguments. Recall that $S(e \oplus (d-e); k)$ was defined in (3.4) for $1 \le k \le d/2$ and $1 \le e \le d/2$.

LEMMA 3.7. (a) $S(e \oplus (d-e); k)/|\mathbf{S}_k| < 2/q^k$.

(b) *If* $k = 1$, *then* $S(e \oplus (d-e); k)/|\mathbf{S}_k| < 1/q + 1/q^{d-1}$.

Proof. Recall that $S(e \oplus (d-e); k)$ counts a set of k-spaces of a d-dimensional $\mathbb{F}_q$-space V. Namely, write $V = V_1 \oplus V_2$ where $\dim V_1 = e$. Then $S(e \oplus (d-e); k)$ is the size of the set Γ of all pairs (X_1, X_2) of subspaces X_i of V such that each $X_i \subseteq V_i$ and $\dim X_1 + \dim X_2 = k$.

We begin by disposing of two special cases of the lemma. If $k = 1$, then

$$|\Gamma|/|\mathbf{S}_k| = \{(q^e - 1) + (q^{d-e} - 1)\}/(q^d - 1)$$
$$\le \{(q-1) + (q^{d-1} - 1)\}/(q^d - 1),$$

so that (a) and (b) are clear. If $e = 2$ and $d = 2k$, then

$$|\Gamma|/|\mathbf{S}_k| = \{2(q^k - 1)(q^{k-1} - 1) + (q+1)(q^k - 1)^2\}/(q^{2k} - 1)$$
$$\times (q^{2k-1} - 1) < 2/q^k.$$

Consequently, for the remainder of the proof, assume that

$$k \ge 2; \qquad \text{if } e = 2 \text{ then } d > 2k. \tag{3.8}$$

Let π_i denote the projection onto V_i compatible with the decomposition $V = V_1 \oplus V_2$. Define $\varphi_i : \mathbf{S}_k \to \Gamma$ by $\varphi_1(W) = (W \cap V_1, \pi_2(W))$ and $\varphi_2(W) = (\pi_1(W), W \cap V_2)$.

Let $\mathbf{S}_k^1$ and $\mathbf{S}_k^2$ be disjoint copies of $\mathbf{S}_k$ and define $\tau : \mathbf{S}_k^1 \cup \mathbf{S}_k^2 \to \Gamma$ by $\tau(W_i) = \varphi_i(W_i)$ whenever $W_i \in \mathbf{S}_k^i$ for $i = 1, 2$. We claim that

$$|\tau^{-1}(X_1, X_2)| > q^k \qquad \text{for each } (X_1, X_2) \in \Gamma, \tag{3.9}$$

from which it follows that $|\Gamma|/|\mathbf{S}_k| < 2/q^k$, as desired.

Fix $(X_1, X_2) \in \Gamma$ with $\dim X_1 = j \leq e$. First note that

$$|\varphi_1^{-1}(X_1, X_2)| = |\mathrm{Hom}(X_2, V_1/X_1)| = q^{(e-j)(k-j)}$$
$$|\varphi_2^{-1}(X_1, X_2)| = |\mathrm{Hom}(X_1, V_2/X_2)| = q^{j(d-e-k+j)}.$$

Namely, if $\alpha \in \mathrm{Hom}(X_2, V_1/X_1)$ and elements of V_1/X_1 are viewed as subsets of V, then $\{\alpha(x_2) + x_2 \mid x_2 \in X_2\}$ lies in $\varphi_1^{-1}(X_1, X_2)$; and this construction easily reverses.

Then $|\varphi_i^{-1}(X_1, X_2)| \geq 1$ for $i = 1, 2$, and we will prove the following, which implies (3.9):

$$|\varphi_i^{-1}(X_1, X_2)| \geq q^k \qquad \text{for } i = 1 \textit{ or } 2. \tag{3.10}$$

If $j = 0$ or k then $(e-j)(k-j) \geq ek \geq k$ or $j(d-e-k+j) \geq k(d-e) \geq k$, respectively, and (3.10) holds. We now assume that $0 < j < k$, and divide the remainder of the proof of (3.10) into various cases:

Case 1. $e < k$ and $j < e/2$. Here $(e-j)(k-j) > (e/2)(k-e/2) > (e/2)(k/2) \geq k$ provided that $e \geq 4$. Since $0 < j < e/2$, the only remaining possibility is $(e, j) = (3, 1)$, in which case $(e-j)(k-j) = 2(k-1) \geq k$ by (3.8).

Case 2. $e < k$ and $j \geq e/2$. Here $j(d-e-k+j) \geq (e/2)(d-e-k+e/2) \geq (e/2)(k-e/2) \geq k$ for $e \geq 4$. This leaves the possibilities $e = j \leq 3$ or $(e, j) = (3, 2)$, $(2, 1)$.

If $e = j$, then $j(d-e-k+j) \geq j(d-k) \geq k$. If $(e, j) = (3, 2)$, then $j(d-e-k+j) = 2(d-k-1) \geq 2(k-1) \geq k$. If $(e, j) = (2, 1)$, then $j(d-e-k+j) = d-k-1 \geq k$ by (3.8).

Case 3. $e \geq k$ and $j \leq k/2$. Here $(e-j)(k-j) \geq (e-k/2)(k/2) \geq (e/2)(k/2) \geq k$ if $e \geq 4$. By (3.8), the only remaining possibility is $(e, j) = (3, 1)$, and then $(e-j)(k-j) = 2(k-1) \geq k$.

Case 4. $e \geq k$ and $j > k/2$. Since $d \geq 2e$, and $j > k/2 \geq 1$ by (3.8), we have $j(d-e-k+j) \geq j(e-k+j) \geq j(k/2) \geq k$. ∎

The next lemma deals with graph and field-graph automorphisms of order 2. This is needed for Theorem 8.2 as well for the general almost simple case.

LEMMA 3.11. *Let G be an almost simple group with socle* $\mathrm{PSL}(d, q) = \mathrm{PSL}(V)$ *with $d \geq 3$. Fix a positive integer $k \leq d/2$. Let $\mathbf{X}_1$ be the G-set consisting of complementary pairs of subspaces one of which has dimension k. Let $\mathbf{X}_2$ be the G-set of flags of type $(k, d-k)$ (here $k < d/2$). If $g \in G$ is* *an involution inducing a graph or field-graph automorphism, then, for $i = 1, 2$,*

(a) $\mu(g, \mathbf{X}_i) < 2/q^k$;

(b) *if $k = 1$, then* $\mu(g, \mathbf{X}_i) < 1/q + 1/q^{d-1}$;

(c) $\mu(g, \mathbf{X}_i) < 1/2$; *and*

(d) *if $d = 2k$, then* $\mu(g, \mathbf{S}_k) < 2/q^k$.

Proof. We may take $G = \operatorname{Aut}\operatorname{PSL}(V)$. First suppose that g induces a field-graph automorphism. There is a unique such class in G (see [GL, 7.2]), so we may assume that g corresponds to the standard hermitian form on V.

Then g fixes $(U_1, U_2) \in \mathbf{X}_i$ if and only if $U_2 = U_1^{\perp}$. Thus, the number of fixed points of g is either the number of totally singular k-spaces (on $\mathbf{X}_2$) or the number of nondegenerate k-spaces (on $\mathbf{X}_1$). A straightforward computation now yields much better estimates than claimed.

Similarly, if $d = 2k$ then g fixes an element of $\mathbf{S}_k$ if and only if the subspace is a maximal totally singular subspace, and the desired estimates hold.

Now assume that g induces a graph automorphism. Since g is an involution, there is a nondegenerate bilinear form associated to g and the fixed points of g can be identified as above. Again, a straightforward computation yields much better estimates than claimed. ▮

LEMMA 3.12. *Let G be an almost simple group with socle* $\operatorname{PSL}(d, q) = \operatorname{PSL}(V)$, $d \geq 3$. *Let $1 \leq k \leq d/2$, and let $\mathbf{X}_i$ denote the G-set in the previous lemma. If $1 \neq g \in G$ then, for $i = 1, 2$,*

(a) $\mu(g, \mathbf{X}_i) < 2/q^k$;

(b) *if $k = 1$, then* $\mu(g, \mathbf{X}_i) < 1/q + 1/q^{d-1}$; *and*

(c) $\mu(g, \mathbf{X}_i) < 1/2$.

Proof. We may assume that g has prime order. If g is a graph or field-graph automorphism, the previous lemma applies. Otherwise, we can simply use (3.1) (since $\mathbf{X}_i$ maps onto the G-set $\mathbf{S}_k$) except in the case $d = 2k$ and $\mathbf{X}_i = \mathbf{X}_1$. We now assume that $d = 2k$ and that g arises from a semilinear transformation.

If g has odd order, then fixing (U_1, U_2) is equivalent to fixing both U_1 and U_2 and again the result follows from (3.1).

The remaining case is when g is an involution. If g is a field automorphism, then argue precisely as in (3.6).

If g cannot interchange two complementary subspaces, then the estimate for the action on $\mathbf{S}_k$ again applies. Thus, we may assume that g arises modulo scalars from

$$\begin{pmatrix} 0 & sI \\ I & 0 \end{pmatrix}$$

for some scalar s. So we see that one of the following holds:

(a) g is diagonalizable with 2 distinct eigenvalues, both of multiplicity k;

(b) the natural module is a direct sum of isomorphic 2-dimensional irreducible $\langle g \rangle$-modules; or

(c) q is even and the Jordan form for g has all of its blocks of size 2.

In general, the fixed points of g are either of pairs of fixed k-subspaces or pairs of g-conjugate subspaces. Suppose that U_1 is a g-invariant k-space and that g fixes some complement U_2. Let Q be the radical of the maximal parabolic subgroup leaving U_1 invariant. Then Q acts regularly on the set of complements to U_1. Thus, the number of g-invariant pairs of complementary subspaces with first term U_1 is precisely $|\mathrm{C}_Q(g)|$. Considering each of the three cases above, we see that $|\mathrm{C}_Q(g)| \le q^{k^2/2}$ (note that Q, considered as a $\langle g \rangle$-module, is just $U_1 \otimes U_2^*$, where U_2^* denotes the adjoint of U_2).

Let t denote the number of elements of $\mathbf{S}_k$ fixed by g. The number of pairs of complementary k-spaces interchanged by g is certainly at most $(1/2)(|\mathbf{S}_k| - t)$. Thus, if g fixes s pairs of complementary k-spaces, then $s \le tq^{k^2/2} + (1/2)(|\mathbf{S}_k| - t)$. The number of pairs of complementary k-spaces is $|\mathbf{S}_k|\ |Q| = |\mathbf{S}_k| q^{k^2}$, whence the result follows.

3.2. *The Remaining Classical Groups*

Let S be a classical group $\mathrm{Sp}(V)$, $\Omega(V)$ or $\mathrm{SU}(V)$ on a d-dimensional vector space V of Witt index $m \ge 2$ over the field $\mathbb{F} = \mathbb{F}_q$ (or $\mathbb{F}_{q^2}$ in the unitary case). We will need to consider the action of S on totally singular subspaces and on nonsingular spaces. (We use the term "totally singular" instead of separating into "totally isotropic or totally singular" subspaces according to the type of space V. We use "nonsingular" to mean having 0 radical.)

Let $S \le G \le \mathrm{N}_{\Gamma\mathrm{L}(V)}(S)$. Let $\mathbf{TS}_k$ and $\mathbf{NS}_k$ denote G-orbits on the set of totally singular or nonsingular k-spaces, respectively. These are S-orbits except in some orthogonal settings where they can be unions of two S-orbits: when $S = \Omega^+(V)$ and the action is on $\mathbf{TS}_{d/2}$, or when $S = \Omega^{\pm}(V)$ with both q and k odd and the action is on $\mathbf{NS}_k$. In all of the latter cases any element either preserves the two orbits or else interchanges them and hence has no fixed points.

In our results on orthogonal groups, we also include the case $S = \Omega_4^+(q)$ (because inductively we need results about all such groups with Witt index at least 2). The fact that S is not quasisimple will make no difference in the computations.

In the next section we will prove Theorem I except in the case of very small-dimensional spaces. In order to minimize the number of special arguments needed in small dimensions, in this section we will be somewhat careful about bounds—leading to relatively ugly-looking estimates. In this direction, we introduce additional parameters $m^{\#}$, m^* for S, as follows:

S	$\mathrm{Sp}(2m,q)$	$\Omega^+(2m,q)$	$\Omega^-(2m+2,q)$	$\Omega(2m+1,q)$	$SU(2m,q)$	$SU(2m+1,q)$
$m^{\#}$	m	$m-1$	$m+1$	m	$m-1/2$	$m+1/2$
m^*	$m-1$	$m-2$	m	$m-1$	$m-1$	m

Note that $m^{\#} \geq m - 1$. If x is any singular 1-space, then $x^{\perp}/x$ has exactly $|\mathbf{TS}_m|/(|\mathbb{F}|^{m^{\#}} + 1)$ totally singular $m - 1$-spaces. The meaning of m^* will appear within the proof of (3.13). Both of these quantities will be carried along during various fixed point estimates.

We will require an important and useful subgroup. Let Q denote the centralizer of a given totally singular m-space W. Then Q has the following structure, with each indicated module a natural one for $\mathrm{GL}(W)$, where we also use a $\mathrm{GL}(W)$-invariant subgroup Z of Q:

$\mathrm{Sp}(2m,q)$. $Z = Q$ can be viewed as the space $S^2(W)$ of symmetric 2-tensors. If q is even, this is an indecomposable module with composition factors $W \wedge W$ and a Frobenius twist of W.

$\Omega^+(2m,q)$. $Z = Q \cong W \wedge W$.

$\Omega(2m+1,q)$. $Z \cong W \wedge W$ and $Q/Z \cong W$, where $Z = Z(Q)$ if q is odd.

$\Omega^-(2m+2,q)$. $Z = Z(Q) \cong W \wedge W$ and $Q/Z(Q) \cong W'$, where $W' = W \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$.

$\mathrm{SU}(2m,q)$. Q can be viewed as the $\mathbb{F}_q$-subspace $W \blacktriangle W$ of $W \otimes W$ spanned by all $v \blacktriangle w := v \otimes w - \overline{w} \otimes \overline{v}$ with $v, w \in W$.

$\mathrm{SU}(2m+1,q)$. $Z = Z(Q) \cong W \blacktriangle W$ and $Q/Z(Q) \cong W$.

LEMMA 3.13. *Let S be an orthogonal, unitary, or symplectic group acting on its natural module. If g is a nonscalar element of* $\mathrm{N}_{\mathrm{GL}(V)}(S)$ *acting nontrivially on the g-invariant totally singular m-space W, then* $|\mathrm{C}_Q(g)| \leq |Q|/|\mathbb{F}|^{m^*}$.

Proof. Let h denote the linear transformation of W induced by g, so $h \neq 1$. We will obtain a lower bound for $\dim[h, Z]$ (and so an upper bound for $\dim \mathrm{C}_Z(h)$).

Case A: *S is not unitary*

Subcase: *h is unipotent.* Decompose $W = W_1 \oplus W_2$ where h acts nontrivially and indecomposably on W_1, so that $[h, W_1]$ is a hyperplane of W_1. Then Z contains the submodule $W_1 \otimes W_2$. If $S = \mathrm{Sp}(2m,q)$, then Z even contains $(W_1 \otimes W_2) \oplus S^2(W_1)$, where $S^2(W_1)$ is the symmetric square of W_1.

By considering a maximal h-invariant flag on W_2, we obtain an h-invariant flag on $W_1 \otimes W_2$ all of whose quotients are $\langle h \rangle$-isomorphic to W_1. Thus,

$$\dim[h, Z] \geq \dim[h, W_1 \otimes W_2] \geq (\dim W_1 - 1)(\dim W_2) \geq m - 2.$$

This shows that the dimension of the centralizer of h in Z has codimension at least $m - 2$, which is m^* when $S = \Omega^+(2m, q)$. In the symplectic case, h is also nontrivial on $S^2(W_1)$ and so the codimension of the centralizer is at least $m - 1 = m^*$.

This proves the desired estimate except when S is $\Omega^-(2m + 2, q)$ or $\Omega(2m + 1, q)$, where m^* is m or $m - 1$, respectively. If $S = \Omega^-(2m + 2, q)$, then $Q/Z \cong W \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$ and hence $\dim_{\mathbb{F}_q}[h, Q/Z] \geq 2$, whence $|Q|/|\mathrm{C}_Q(h)| \geq q^{(m-2)+2} = q^{m^*}$. If $S = \Omega(2m + 1, q)$ then $Q/Z \cong W$ and $\dim_{\mathbb{F}_q}[h, Q/Z] \geq 1$, which yields the desired result.

Subcase: *h is semisimple*. We will abuse notation and consider the modules W and Z over the algebraic closure: the dimensions and codimensions of centralizers will be the same whether we consider Z over $\mathbb{F}_q$ (its field of definition) or over the algebraic closure.

First suppose that h induces a scalar on W. If the scalar is not -1, then $Z = [h, Z]$ and the result follows easily. If h acts as $-I$ on W, then $Q \neq Z$ (since h is not a scalar on V). Then $[h, Q/Z] = Q/Z$ and the result follows in this case.

So we assume that h has at least 2 distinct eigenvalues on W. *We will show that* $[h, Z]$ *has dimension at least* $m - 1$ *unless* $m = 3$ and h has exactly 2 eigenvalues whose product is 1.

Let the eigenvalues of h (over the algebraic closure) on W be $a_1, \dots, a_m$. Then $\dim \mathrm{C}_Z(h)$ is the number of ordered pairs (i, j) such that

(i) $a_i a_j = 1$ for $i < j$ if S is orthogonal; or

(ii) $a_i a_j = 1$ for $i \leq j$ if S is symplectic.

Suppose that h has 2 distinct eigenvalues a and b with $ab \neq 1$ (there may be further eigenvalues). Decompose $W = W_1 \oplus W_2$ for $\langle h \rangle$-modules W_i such that $\dim W_1 = e$ with $1 \leq e < m$ and if a_i is any eigenvalue on W_i, then $a_1 a_2 \neq 1$. Since $W_1 \otimes W_2$ is isomorphic to an $\langle h \rangle$-submodule of Z and h has no fixed points on this submodule, it follows that $\dim[h, Z] \geq e(m - e) \geq m - 1$.

So assume that h has exactly 2 eigenvalues a and a^{-1} with multiplicities e and $m - e$. Let W_1 and W_2 denote the eigenspaces of h. Then $\wedge^2(W_i)$ (or $S^2(W_i)$ in the symplectic case) are subspaces of Z, having 0 intersection, such that h has no fixed points on either. If G is orthogonal then $\dim[h, Z] \geq e(e - 1)/2 + (m - e)(m - e - 1)/2 \geq m - 1$ unless $m \leq 3$, in which case $\dim[h, Z] \geq m - 2$. If $S = \mathrm{Sp}(2m, q)$ then $\dim[h, Z] \geq e(e+1)/2 + (m-e)(m-e+1)/2 \geq m - 1$.

Now complete the argument as in the unipotent case (considering $[h, Q/Z]$).

Case B: *S is unitary*

We again abuse notation and consider the modules W and Z over the algebraic closure: the dimensions and codimensions of centralizers will be the same whether we consider Z over $\mathbb{F}_q$ (its field of definition) or over the algebraic closure. Since the result is stated over $\mathbb{F} = \mathbb{F}_{q^2}$ rather than over $\mathbb{F}_q$, we must divide our estimate of $\dim[h, W_1 \otimes W_2]$ by 2.

Subcase: *h is unipotent*. We decompose $W = W_1 \oplus W_2$ as above. Then Z is isomorphic to a direct sum of the 4 terms $W_i \otimes W_j$ (since $W_i^{\sigma} \cong W_i$ as $\langle h \rangle$-modules for $i = 1, 2$). The argument in Case A shows that $\dim[h, W_1 \otimes W_2]$ and $\dim[h, W_2 \otimes W_1]$ are at least $m - 2$. Similarly, $\dim[h, W_1 \otimes W_1] \geq 2$. Thus, $\dim[h, Z] \geq 2m - 2$.

This yields the result when $d = 2m$ (recall that we must divide by 2). When $d = 2m + 1$, $Q/Z \cong W$, $|Q/Z : \mathrm{C}_{Q/Z}(h)| \geq q^2$ and so $|Q : \mathrm{C}_Q(h)| \geq q^{2m}$, as required.

Subcase: *h is semisimple*. If h has eigenvalues $a_1, \dots, a_m$, then $\dim \mathrm{C}_Z(h)$ is the number of pairs (i, j) so that $a_i a_j^q = 1$. Arguing as above, we see that the result is true if h induces a scalar on W or has 2 eigenvalues a, b with $ab^q \neq 1$. So assume that h has eigenvalues a and b with $ab^q = 1$, and let e be the multiplicity of a. Then $\dim[h, Z] = e^2 + (m - e)^2 \geq 2(m - 1)$.

This yields the result when $d = 2m$, while for $d = 2m + 1$ we proceed exactly as in the unipotent case. ∎

LEMMA 3.14. $\mu(G, \mathbf{TS}_m) < 2/|\mathbb{F}|^{m^*} + 1/|\mathbb{F}|^{m^\#} \leq 5/2|\mathbb{F}|^{m^*}$ *if* $m \geq 3$.

Proof. It suffices to assume that g has prime order e and is not a scalar. Let $g \in G$ act nontrivially on $\mathbf{TS}_m$. Write $C = \mathrm{C}_V(g)$. We consider various cases which may overlap but contain all possibilities. In Cases A and B, we assume that g acts linearly on V.

Case A. *g is semisimple and has a* 1-*dimensional invariant subspace on* V. Suppose first that $V = V_1 \perp V_2$ is a nontrivial orthogonal decomposition of V, that there are no nontrivial $\langle g \rangle$-homomorphisms from V_1 to V_2, and that $\dim V_1 = k \geq \dim V_2$. Note that in particular this holds if $C \neq 0$ (with $\{V_1, V_2\} = \{C, [g, V]\}$). In particular, every maximal totally singular g-invariant subspace of V is spanned by ones of V_1 and V_2. Then $\mathrm{Fix}_{\mathbf{TS}_m}(g)$ is bounded above by the product of the number of maximal totally singular subspaces of a nonsingular subspace of dimension k and the number of maximal totally singular subspaces of a nonsingular space of dimension $d-k$ for some $k \geq 1$. If $k = d-1$, then $\mu(g, \mathbf{TS}_m) \leq 2/(|\mathbb{F}|^m + 1)$, and otherwise $\mu(g, \mathbf{TS}_m)$ is smaller than this.

This handles all possibilities except when $V = V_1 \oplus V_2$ for maximal totally singular subspaces V_1 and V_2 on each of which g induces a scalar. Then V must be a unitary space. Any g-invariant maximal totally singular subspace X must have the form $X = (X \cap V_1) \oplus (X \cap V_2)$ where $X \cap (X \cap V_1)^{\perp} = X \cap V_2$. Thus, the number of such X is the total number of subspaces of V_1, so that $\mu(G, \mathbf{TS}_m) < 2|\mathbb{F}|^{(m/2)^2}/|\mathbf{TS}_m| < 2/|\mathbb{F}|^{m^*}$.

Case B. *g is unipotent, or g is semisimple and has no* 1*-dimensional invariant subspace*. We may assume that g does stabilize some $W \in \mathbf{TS}_m$.

If every g-invariant element of $\mathbf{TS}_m$ lies in $C = \mathrm{C}_V(g)$, then $\operatorname{rad} C \neq 0$, so that $|\mathrm{Fix}_{\mathbf{TS}_m}(g)|$ is at most the number of maximal totally singular subspaces of $x^{\perp}/x$ for a singular 1-space x of $\operatorname{rad} C$, and hence is at most $|\mathbf{TS}_m|/(|\mathbb{F}|^{m^{\#}} + 1)$. Hence, we may assume that g acts nontrivially on our g-invariant subspace $W \in \mathbf{TS}_m$. Let $S_m(i)$ denote the set of members of $\mathbf{TS}_m$ whose intersection with W is an i-space. Since Q acts regularly on $S_m(0)$, $|\mathrm{Fix}_{S_m(0)}(g)|$ is either 0 or $|\mathrm{C}_Q(g)|$. By (3.13), since g is nontrivial on W we have $|\mathrm{Fix}_{S_m(0)}(g)| \leq |Q|/|\mathbb{F}|^{m^*} = |S_m(0)|/|\mathbb{F}|^{m^*}$.

Now consider $S_m(i)$, $0 < i \leq m$. Since $S_m(m) = \{W\}$ we will focus on the case $i \leq m-1$. If $U \in S(i)$ is g-invariant then $I = U \cap W$ is a g-invariant i-space; the number of such U for a given I is the number of g-invariant totally singular complements to W/I in $I^{\perp}/I$. Conversely, if we start with a g-invariant i-space $I \subset W$, we wish to count the number of g-invariant $U \in S_m(i)$ such that $U \cap W = I$.

First consider those I for which g is nontrivial on W/I. Then $m - i = \dim W/I \geq 2$ since we have assumed that g has no eigenvalue in $\mathbb{F} - \{1\}$. In particular, the Witt index of $I^{\perp}/I$ is $m - i \geq 2$, as required to apply (3.13): g fixes at most $|S_m(i)|/|\mathbb{F}|^{m^*-i}$ members of $S_m(i)$. By (3.1), there are fewer than $2|\mathbf{S}_i(W)|/|\mathbb{F}|^i$ choices for a g-invariant i-space I of W. Thus, the number of g-invariant $U \in \mathbf{TS}_m$ such that either $U = W$ or x is nontrivial on $W/(U \cap W)$ is at most

$$1 + \sum_{1}^{m-2} \frac{2|\mathbf{S}_i(W)|}{|\mathbb{F}|^i} \frac{|S_m(i)|}{|\mathbb{F}|^{m^*-i}} + \frac{|S_m(0)|}{|\mathbb{F}|^{m^*}} \leq \sum_{0}^{m} \frac{2|\mathbf{S}_i(W)|\,|S_m(i)|}{|\mathbb{F}|^{m^*}} = \frac{2|\mathbf{TS}_m|}{|\mathbb{F}|^{m^*}}.$$

Next consider those $I \in S_m(i)$ for which g is trivial on W/I, i.e., such that $[g, W] \subseteq I$. The number of totally singular m-spaces of V containing $[g, W]$ is just the number of maximal totally singular subspaces of $[g, W]^{\perp}/[g, W]$, which is at most $|\mathbf{TS}_m|/(q^{m^{\#}} + 1) < |\mathbf{TS}_m|/q^{m^{\#}}$.

Consequently, g fixes fewer than $2|\mathbf{TS}_m|/|\mathbb{F}|^{m^*} + |\mathbf{TS}_m|/q^{m^\#}$ members of $\mathbf{TS}_m$, as required.

We now consider the cases where g acts semilinearly but not linearly on V. These are elements which involve field automorphisms of the split group. We note two instances. If S is a unitary group, then there are involutory automorphisms which are a product of an involutory field automorphism and a graph automorphism of the corresponding linear overgroup; these are handled below in Case D. On the other hand, when S is of type ${}^2D_m$ the involutory field automorphism of the split group acts linearly on the natural orthogonal S-module and so was dealt with previously.

Case C. *g is a field automorphism of prime order e (with e odd if S is unitary or of type ${}^2D_m$), or g is a field-graph automorphism of order 2 for S of type D_m*. Argue as in the proof of (3.6) to conclude that the number of fixed points is the number of totally singular subspaces of dimension m defined over the fixed field of the field automorphism. A straightforward computation now yields a much better estimate than claimed.

Case D. *S is a unitary group and g is a nonlinear involution*. Let h denote the standard field automorphism of order 2 on $\mathrm{GU}(d,q)$, so $gS = hS$. The conjugacy classes of such involutions g are given in [LiSa]. In particular, if d is odd, there is a unique class. If d is even, then there are two classes of involutions if q is even and three if q is odd.

Note that by [GL, 7.2], g is conjugate to h in $\mathrm{GL}(d,q^2){:}\langle h\rangle$. In particular, $W = C_V(g)$ is a d-dimensional $\mathbb{F}_q$-subspace and each d-dimensional g-invariant subspace of V is generated over $\mathbb{F}$ by $V \cap W$, a d-dimensional subspace over $\mathbb{F}_q$.

The description of the conjugacy classes mentioned above shows that the restriction of the Hermitian form on V to W is an nondegenerate bilinear form over $\mathbb{F}_q$. (For example, if d is even and q is odd, the three conjugacy classes correspond to the cases where this restriction is alternating or either of the two classes of symmetric bilinear forms.) Thus, the number of fixed points of g is the number of totally singular m-spaces of U. A straightforward computation now yields a much better estimate than claimed. ∎

PROPOSITION 3.15. *$\mu(G, \mathbf{TS}_k) < 2/|\mathbb{F}|^{m^*} + 1/q^{m^\#} + 1/|\mathbb{F}|^k$ whenever $1 \le k \le m$ and $m \ge 3$.*

Proof. Let $g \in G$ act nontrivially on $\mathbf{TS}_k$. By the preceding lemma we may assume that $k \le m - 1$. The proof here, and in the remaining estimates in the section, can be viewed as elementary conditional probability estimates. Take any totally singular m-space $U \ne U^g$, and then choose one of at least $\left[{m \atop k}\right] - \left[{m-1 \atop k}\right] = \{1 - (|\mathbb{F}|^{m-k} - 1)/(|\mathbb{F}|^{m} - 1)\}\left[{m \atop k}\right]$ of the k-spaces in U not in U^g. By (3.14),

$$\begin{aligned}1 - \mu(g, \mathbf{TS}_k) &\geq \{1 - \mu(g, \mathbf{TS}_m)\}\{1 - (|\mathbb{F}|^{m-k} - 1)/(|\mathbb{F}|^{m} - 1)\}\\ &> \left(1 - \left\{2/|\mathbb{F}|^{m^*} + 1/q^{m^\#}\right\}\right)\left(1 - 1/|\mathbb{F}|^{k}\right)\\ &> 1 - \left\{2/|\mathbb{F}|^{m^*} + 1/q^{m^\#}\right\} - 1/|\mathbb{F}|^{k}.\end{aligned}$$

∎

We now consider actions on nonsingular k-spaces N, where $1 \leq k \leq d - 1$. We do *not* restrict k to be at most $d/2$. In fact, we will apply the following estimate either to N or to $N^{\perp}$, depending in part on the Witt index requirement in the proposition.

PROPOSITION 3.16. *If $m \geq 3$ and if $l \geq 1$ is the Witt index of the members of $\mathbf{NS}_k$, then $\mu(G, \mathbf{NS}_k)$ is bounded as follows:*

S	$\mu(G, \mathbf{NS}_k) <$
$\mathrm{Sp}(2m, q)$, q odd	$2/q^{m-2} + 1/q^{m} + 1/q^{k/2} + 1/q^{d-k}$
$\mathrm{Sp}(2m, q)$, q even	$2/q^{m-1} + 1/q^{m} + 1/q^{k/2} + 1/q^{d-k}$
$\Omega^{+}(2m, q)$	$2/q^{m-2} + 1/q^{m-1} + 1/q^{l} + 1/q^{d-k}$
$\Omega(2m+1, q)$, q odd	$2/q^{m-1} + 1/q^{m} + 1/q^{l} + 1/q^{d-k}$
$\Omega^{-}(2n, q)$	$2/q^{n-2} + 1/q^{n} + 1/q^{l} + 1/q^{d-k}$
$\mathrm{SU}(2m, q)$	$2/q^{2(m-2)} + 1/q^{2m-1} + 1/q^{2l} + 1/q^{2(d-k)}$
$\mathrm{SU}(2m+1, q)$	$2/q^{2(m-1)} + 1/q^{2m+1} + 1/q^{2l} + 1/q^{2(d-k)}$

Proof. Let $g \in G$ act nontrivially on $\mathbf{NS}_k$. As in the proof of (3.15), take any $L \neq L^g$ in $\mathbf{TS}_l$; then g moves any $N \supset L$ in $\mathbf{NS}_k$ such that $N \not\supset L^g$, so that

$$\begin{aligned}&1 - \mu(g, \mathbf{NS}_k)\\ &\quad\geq (1 - \mu(g, \mathbf{TS}_l))\left(1 - \max_{\substack{L, L' \in \mathbf{TS}_l\\ L \neq L'}} \Pr\{L' \subseteq N \mid L \subseteq N \in \mathbf{NS}_k\}\right).\end{aligned} \tag{3.17}$$

We only need to consider those distinct L, $L' \in \mathbf{TS}_l$ that lie in some $N \in \mathbf{NS}_k$. Since l is the Witt index of N, if $i = \dim L \cap L'$ for such a pair L, L' then $\langle L, L' \rangle = (L \cap L') \perp Z$ for a nonsingular $2(l-i)$-space Z of Witt index $l - i$. Here, $i \leq l - 1$ since $L \neq L'$. Moreover, the set-stabilizer G_L of L is transitive on the set $S_l(i)$ of all $L' \in \mathbf{TS}_l$ such that $\dim L \cap L' = i$ and $\langle L, L' \rangle/(L \cap L')$ is nonsingular.

For any such given L, $L' \in \mathbf{TS}_l$ for which $i = \dim L \cap L' = \dim \operatorname{rad}\langle L, L'\rangle \leq l - 1$, consider the probability $P(i) = \Pr\{L' \subseteq N \mid L \subseteq N \in \mathbf{NS}_k\}$ on the right side of (3.17). For given $I \subset L \subset N \in \mathbf{NS}_k$ such that $i = \dim I$ we also have

$$P(i) = \Pr\{L' \subseteq N \mid L' \in \mathbf{TS}_l, L \cap L' = I = \operatorname{rad}\langle L, L'\rangle\}.$$

Write $\delta = k - 2l$. Table I lists $|S_l(0)|$, as well as the size of the set $S_l(0) \cap N$ of members of $S_l(0)$ lying in N. (Here, p is the characteristic of $\mathbb{F}$ and $O_p(S_L)$ is regular on $S_l(i)$.)

Here $P(0) = |S_l(0) \cap N|/|S_l(0)|$, and $P(i)$ is obtained by replacing d, k, m, n, and l by $d - 2i$, $k - 2i$, $m - i$, $n - i$, and $l - i$, respectively (namely, we pass to $I^{\perp}/I$). Then $P(i)$ is given in the last column of Table I, including a bound that is achieved when $l = i - 1$.

Now (3.16) follows immediately from the table, since $1 - \mu(G, \mathbf{NS}_k) > 1 - \{2/|\mathbb{F}|^{m^*} + 1/|\mathbb{F}|^{m^\#}\} - \max_{0 \leq i < l} P(i) = 1 - \{2/|\mathbb{F}|^{m^*} + 1/|\mathbb{F}|^{m^\#}\} - P(l - 1)$ by (3.15) and (3.17). ▮

Note that the previous result also handles cases of Witt index 0. For example, when G is orthogonal and $\mathbf{NS}_2$ consists of anisotropic 2-spaces we can apply the proposition with $k = d - 2$. A similar remark holds for nonsingular 1-spaces, but here it is convenient to prove slightly more precise estimates than in the preceding result:

LEMMA 3.18. *Let $S = F^*(G) = \Omega(2m + 1, q)$, and let $\mathbf{NS}_{2m}^{\pm}$ denote the S-orbit of nonsingular hyperplanes of V of type $\Omega^{\pm}(2m, q)$, where $m \geq 4$. Let $1 \neq g \in G$.*

(i) *If q is even and g is a transvection, then $1/q - 1/q^m \leq \mu(g, \mathbf{NS}_{2m}^{\pm}) \leq 1/q + 1/q^m$, $\mu(g, \mathbf{NS}_{2m}^{+}) < 1/q$, and $1/q - 1/q^m \leq \mu(g, \mathbf{TS}_1)$.*

(ii) *If q is even and g is not a transvection then $\mu(g, \mathbf{NS}_{2m}^{\pm}) \leq 1/q^2 + 1/q^m$.*

(iii) *If q is odd and $-g$ is a reflection, then $1/q - 1/q^{m-1} \leq \mu(g, \mathbf{X})$ for $\mathbf{X} \in \{\mathbf{NS}_{2m}^{\pm}, \mathbf{TS}_1\}$.*

TABLE I

S	$\lvert O_p(S_L)\rvert = \lvert S_l(0)\rvert$	$\lvert S_l(0) \cap N\rvert$	$P(i)$
$\mathrm{Sp}(2m, q)$	$q^{m^2-(m-l)^2-\binom{l}{2}}$	$q^{\binom{l+1}{2}}$	$1/q^{(l-i)(2m-k)} \leq 1/q^{2m-k}$
$\Omega(2m + 1, q)$	$q^{m^2-(m-l)^2-\binom{l}{2}}$	$q^{\binom{l}{2}+\delta l}$	$1/q^{(l-i)(2m+1-k)} \leq 1/q^{2m+1-k}$
$\Omega^{\pm}(2n, q)$	$q^{(n^2-n)-\{(n-l)^2-(n-l)\}-\binom{l}{2}}$	$q^{\binom{l}{2}+\delta l}$	$1/q^{(l-i)(2n-k)} \leq 1/q^{2n-k}$
$\mathrm{SU}(d, q)$	$q^{\binom{d}{2}-\binom{d-2l}{2}-2\binom{l}{2}}$	$q^{l^2+2\delta l}$	$1/q^{2(l-i)(d-k)} \leq 1/q^{2(d-k)}$

Proof. (i) $\mu(g, \mathbf{NS}_{2m}^{\pm}) = \frac{1}{2}q^{2m-1}/\frac{1}{2}q^m(q^m \mp 1)$ and $\mu(g, \mathbf{TS}_1) = (q^{2m-1} - 1)/(q^{2m} - 1)$.

(ii) We may assume that g has prime order e and fixes some member of $\mathbf{NS}_{2m}^{\pm}$.

If $e \neq 2$ and g acts linearly on V, then $V = C_V(g) \perp [V, g]$, and the fixed hyperplanes not containing the radical $V^{\perp}$ are $V_0 \perp [V, g]$ for the hyperplanes V_0 of $C_V(S)$ not containing $V^{\perp}$. Here, $\dim[V, g]$ is even (as eigenvalues occur in inverse pairs). If $\dim C_V(g) = 2k + 1$, then $k \leq m - 1$ and hence $\mu(g, \mathbf{NS}_{2m}^{\pm}) = \frac{1}{2}q^k(q^k \pm 1)/\frac{1}{2}q^m(q^m \pm 1) \leq 1/q^2 + 1/q^m$ (note that the signs $\pm$ need not match up here).

Suppose that $e = 2$ and g acts linearly on V. Since $[V, g]$ is the intersection of the fixed hyperplanes of g it does not contain $V^{\perp}$. By considering $V/V^{\perp}$ we see that $[V, g]$ has a nonzero radical. Also, $\dim[V, g] \geq 2$ since g is not a transvection. Thus, $[V, g]$ contains a totally singular 2-space $\langle x, y\rangle$. Clearly, $\mu(g, \mathbf{NS}_{2m}^{\pm}) \leq \Pr\{H^{\pm} \supseteq \langle x, y\rangle \mid H^{\pm} \in \mathbf{NS}_{2m}^{\pm}\}$. Then, for $H^{\pm} \in \mathbf{NS}_{2m}^{\pm}$,

$$\begin{aligned}\mu\left(g, \mathbf{NS}_{2m}^{\pm}\right) &\leq \Pr\left\{\langle x', y'\rangle \subseteq H^{\pm} \mid \langle x', y'\rangle \text{ is a totally singular 2-space}\right\}\\ &= (q^m \mp 1)(q^{m-1} \pm 1)(q^{m-1} \mp 1)(q^{m-2} \pm 1)/\\ &\quad (q^{2m} - 1)(q^{2m-2} - 1)\\ &\leq 1/q^2 + 1/q^m.\end{aligned}$$

Suppose that g does not act linearly on V. As usual, by [GL], we may assume that g is the standard field automorphism and hence has a fixed point; let J denote the stabilizer of this point. If e is odd, then again by [GL], $g^G \cap J = g^J$ and so g has exactly $|G(q_0) : J(q_0)|$ fixed points where $q = q_0^e$. The result follows easily. If $e = 2$, then using [GL] again we see that every g-invariant hyperplane has a basis over $\mathbb{F}_{q_0}$. Thus, the total number of g-invariant hyperplanes is at most $(q_0^{2m+1} - 1)/(q_0 - 1)$. The total number of points is $(1/2)q^m(q^m + 1)$, so the fixed point ratio is at most $2(q_0^{2m+1} - 1)/(q_0 - 1)q^m(q^m + 1)$ and the result follows.

(iii) $\mu(g, \mathbf{NS}_{2m}^{-}) = (\alpha + \frac{1}{2}q^{m-1}(q^m + \delta))/\frac{1}{2}q^m(q^m + \varepsilon)$ for δ, $\varepsilon = \pm 1$ and $\alpha = 0$ or 1, and $\mu(g, \mathbf{TS}_1) = (q^m \pm 1)(q^{m-1} \mp 1)/(q^{2m} - 1)$. ∎

4. PROOF OF THEOREMS I AND II FOR CLASSICAL GROUPS WHOSE DIMENSION IS NOT SMALL

Before starting the proof of Theorems I and II for classical groups, we indicate our general approach using primitive prime divisors. Let G be a group such that $S = F^*(G)$ is classical group with natural module V of dimension d. We will assume that S is quasisimple and linear rather than simple, since this makes no difference for our estimates. We choose an element s of S and determine the set $\mathscr{M}(s)$ of overgroups of s maximal with respect to not containing S. The reducible maximal subgroups containing s are obvious: they are just the stabilizers of the nonsingular or totally singular subspaces left invariant by s. Thus, we need only classify the maximal irreducible subgroups of S containing s (or in the case of $\Omega(2m+1, q)$ with q even, those that act irreducibly modulo the radical $V^{\perp}$). In most cases, the normalizers of these maximal subgroups will be the maximal subgroups of G containing s but not S. In a few cases, an outer automorphism will fuse 2 elements of $\mathscr{M}(s)$; this only makes the arguments easier.

In all cases s acts irreducibly on a subspace of dimension e with $e > d/2$. Moreover, by Zsigmondy's Theorem [Zs], some prime order subgroup of $\langle s \rangle$ will act irreducibly on this space as well unless either $(q, e) = (2, 6)$ or $e = 2$ and q is a Mersenne prime. If $e = 2$, then $d \leq 3$ and all maximal subgroups are known. Whenever the case $(q, e) = (2, 6)$ comes up in our proof it is handled individually.

So we consider the case when some prime order element of $\langle s \rangle$ acts irreducibly on a subspace of dimension $e > d/2$ and apply [GPPS], which classifies all subgroups H of $\mathrm{GL}(d, q)$ containing such an element of prime order. The examples fall into several families. The most natural are other classical groups of the same dimension over subfields (not necessarily proper) and smaller classical groups over extension fields (this includes the important case of $\mathrm{SU}(d/2, q)$ in orthogonal and symplectic groups of even dimension d). The remaining subgroups H are usually in small dimension or have some other special properties which allow us easily to see that they do not contain our element s. Indeed, in most cases the element of H of prime order which acts irreducibly on the subspace of dimension e has small order (usually comparable in magnitude to d or at worst $2d$) and its centralizer in H is quite small (in particular, smaller than $|s|$).

With this in mind we will prove the following (where m always denotes the Witt index):

Proposition 4.1. *Theorems* I *and* II *hold for the classical groups in Table II*.

Proof. The action of s on V is given in Table II, including all irreducible constituents in the fourth column. On the first constituent s induces a linear transformation whose order is the first indicated factor (divided by a small number so as to have determinant and spinor norm 1). Similar statements hold for the remaining constituents.

The set $\mathscr{M}(s)$ is obtained using [GPPS]. When $S = \mathrm{SL}(d, q)$ the irreducible constituents have relatively prime dimensions, thereby eliminating the possibility $\mathrm{SL}(de, q^{1/e}) \trianglelefteq M \in \mathscr{M}(s)$ for some $e > 1$. Moreover, if

TABLE II

S	$\lvert s\rvert$ divides		$\mathscr{M}(s)$ and decomposition of V
$\mathrm{SL}(2m, q)$	excluding $\mathrm{SL}(4,2)$, where $m \geq 2$ satisfies:		
	odd	$(q^{m+2}-1)(q^{m-2}-1)$	$(m+2) \oplus (m-2)$
	even	$(q^{m+1}-1)(q^{m-1}-1)$	$(m+1) \oplus (m-1)$
$\mathrm{SL}(2m+1, q)$	excluding $\mathrm{SL}(11,2)$, where		
	$m \geq 2$	$(q^{m+1}-1)(q^{m}-1)$	$(m+1) \oplus m$
$\mathrm{Sp}(2m, q)$	$m \geq 4$ and also $m \neq 4, 5, 6, 8, 10$ if q is even, and m also satisfies:		
	odd	$(q^{\frac{1}{2}(m+1)}+1)(q^{\frac{1}{2}(m-1)}+1)$	$(m+1) \perp (m-1)$ &**O**
	0 mod 4	$(q^{\frac{1}{2}(m+2)}+1)(q^{\frac{1}{4}m}+1)(q^{\frac{1}{4}(m-4)}+1)$	$(m+2) \perp \frac{1}{2}m \perp \frac{1}{2}(m-4)$ &**O**
	2 mod 4	$(q^{\frac{1}{2}(m+4)}+1)(q^{\frac{1}{4}(m-2)}+1)(q^{\frac{1}{4}(m-6)}+1)$	$(m+4) \perp \frac{1}{2}(m-2) \perp \frac{1}{2}(m-6)$ &**O**
$\mathrm{SU}(2m, q)$	$m \geq 4$		
	odd	$(q^{m+2}+1)(q^{m-2}+1)$	$(m+2) \perp (m-2)$
	even	$(q^{m+1}+1)(q^{m-1}+1)$	$(m+1) \perp (m-1)$
$\mathrm{SU}(2m+1, q)$	$m \geq 4$		
	odd	$(q^{m+2}+1)(q^{m-1}-1)$	$(m+2) \perp [\frac{1}{2}(m-1) \oplus \frac{1}{2}(m-1)]$
	even	$(q^{m+1}+1)(q^{m}-1)$	$(m+1) \perp [\frac{1}{2}m \oplus \frac{1}{2}m]$

$\Omega^+(2m,q)$	$m \neq 2, 3, 4, 6, 8, 10$ and $(m,q) \neq (5,2)$, and m also satisfies:		
	odd	$(q^{\frac{1}{2}(m+1)}+1)(q^{\frac{1}{2}(m-1)}+1)$	$(m+1)^- \perp (m-1)^-$
	0 mod 8	$(q^{\frac{1}{2}(m+2)}+1)(q^{\frac{1}{4}m}+1)(q^{\frac{1}{4}m-1}-1)$	$(m+2)^- \perp \frac{1}{2}m^- \perp [\frac{1}{4}(m-4) \oplus \frac{1}{4}(m-4)]$
	4 mod 8	$(q^{\frac{1}{2}(m+2)}+1)(q^{\frac{1}{4}m}-1)(q^{\frac{1}{4}m-1}+1)$	$(m+2)^- \perp [\frac{1}{4}m \oplus \frac{1}{4}m] \perp \frac{1}{2}(m-4)^-$
	2 mod 8	$(q^{\frac{1}{2}(m+4)}+1)(q^{\frac{1}{4}(m-2)}+1)(q^{\frac{1}{4}(m-6)}-1)$	$(m+4)^- \perp \frac{1}{2}(m-2)^- \perp [\frac{1}{4}(m-6) \oplus \frac{1}{4}(m-6)]$
	6 mod 8	$(q^{\frac{1}{2}(m+4)}+1)(q^{\frac{1}{4}(m-2)}-1)(q^{\frac{1}{4}(m-6)}+1)$	$(m+4)^- \perp [\frac{1}{4}(m-2) \oplus \frac{1}{4}(m-2)] \perp \frac{1}{2}(m-6)^-$
$\Omega^-(2n,q)$	(and $n = m+1$) where $n \geq 7$ also satisfies:		
	1 mod 4	$(q^{\frac{1}{2}+(n+3)}+1)(q^{\frac{1}{4}(n-1)}+1)(q^{\frac{1}{4}(n-5)}+1)$	$(n+3)^- \perp \frac{1}{2}(n-1)^- \perp \frac{1}{2}(n-5)^-$
	3 mod 4	$(q^{\frac{1}{2}(n+1)}+1)(q^{\frac{1}{2}(n-1)}-1)$	$(n+1)^- \perp [\frac{1}{2}(n-1) \oplus \frac{1}{2}(n-1)]$
	0 mod 4	$(q^{\frac{1}{2}(n+2)}+1)(q^{\frac{1}{4}n}+1)(q^{\frac{1}{4}(n-4)}+1)$	$(n+2)^- \perp \frac{1}{2}n^- \perp \frac{1}{2}(n-4)^-$
	2 mod 4	$(q^{\frac{1}{2}(n+4)}+1)(q^{\frac{1}{4}(n-2)}+1)(q^{\frac{1}{4}(n-6)}+1)$	$(n+4)^- \perp \frac{1}{2}(n-2)^- \perp \frac{1}{2}(n-6)^-$
$\Omega(2m+1,q)$	excluding $\Omega(5,3)$ and $\Omega(7,q)$, where q is odd and		
	$m \geq 2$	q^m+1	$2m^- \perp 1$

$g \in G$ induces a graph automorphism, we see that $|\mathscr{M}(s)| = 1$. Then the result follows by (2.3).

In all other cases, by [GPPS] the only possible *irreducible* maximal overgroups M of s are the normalizers of naturally embedded subgroups of the following sorts: $\Omega^{\pm}(2m, q) < \mathrm{Sp}(2m, q)$ when q is even (denoted **O** in Table II), $\mathrm{SU}(m, q) < \mathrm{Sp}(2m, q)$, $\mathrm{SU}(m, q) < \Omega^{\pm}(2m, q)$, $\mathrm{Sp}(2m/t, q^t) < \mathrm{Sp}(2m, q)$, and $\Omega^{\pm}(2m/t, q^t) < \Omega^{\pm}(2m, q)$, where $t \mid m$. However, except for the cases **O** none of these can occur because of the following simple conditions we have imposed on the nonsingular constituents: in all cases two of their dimensions differ by 2, so $\mathrm{Sp}(2m/t, q^t) < \mathrm{Sp}(2m, q)$ and $\Omega^{\pm}(2m/t, q^t) < \Omega^{\pm}(2m, q)$ are ruled out; and unitary subgroups are ruled out because for one of the dimensions k in Table II the corresponding factor in column 3 is of the form $q^k + (-1)^k$.

Following (2.3) we noted that, if $q \to \infty$, then Theorem II holds. In particular, to prove Theorem II we may assume that q is fixed and d is large.

Case 1. *S is not $\Omega(2m + 1, q)$ for q of any parity*. The last column of Table II gives dimensions k to use in the estimates obtained in Section 3; there is some choice here, so we will choose to have the Witt index of a nonsingular subspace as large as possible. By (3.1, 3.15, 3.16), $\mu(G, M^G) < 4/q^{(d-12)/8}$ for any $M \in \mathscr{M}(s)$. Thus, by (2.2), $1 - \mathrm{PC}(G) \leq \Sigma_M \, \mu(G, M^G) < 20/q^{(d-12)/8} \to 0$ as $d \to \infty$.

This proves Theorem II for these classical groups. Slightly more care with these same estimates shows that $1 - \mathrm{PC}(G) < 9/10$ in every case within Table II, as required in Theorem I. We will give an example of this verification in Case 2 below. In many of the situations excluded in Table II only the cases $q = 2$ and possibly $q = 3$ still need to be considered, but in the next section we will not bother to make this restriction.

Case 2. *$S \cong \Omega(2m + 1, q)$ for q of any parity*. Here $\mathscr{M}(s)$ contains the stabilizer of a nonsingular hyperplane U, and $\mu(g, U^G) < 1/q + 1/q^m$ by (3.18). Then $1 - \mathrm{PC}(G) < 1/q + 1/q^m$ when q is odd. When q is even $S \cong \mathrm{Sp}(2m, q)$ and $\mathscr{M}(s)$ contains further subgroups, but proceeding as above we see that $1 - \mathrm{PC}(G) < 1/q + 13/q^{(d-12)/8} \to 0$ as $q \to \infty$, provided that $d \geq 13$. (We have used very different s for q odd and even so as to avoid dealing in the latter case with symplectic groups over extension fields.)

On the other hand, for *any* choice of $s \in G$, there is some s-invariant hyperplane (since $d = 2m + 1$ is odd and eigenvalues other than ± 1 must come in inverse pairs), and hence $1 - \mathrm{PC}(G) \geq P_s(g) > 1/q - 1/q^m$ when $\pm g$ is a reflection or a transvection, by (3.18(i), (iii)). Now for any q we have $1/q + 13/q^{(d-12)/8} > 1 - \mathrm{PC}(G) \geq P_s(g) > 1/q - 1/q^m$, and hence $\lim_{d \to \infty} \mathrm{PC}(G) = 1 - 1/q$ for fixed q.

It follows that, in order to determine $\liminf \mathrm{PC}(G)$ for classical G, it suffices to consider only the present odd-dimensional case and sequences (G_i) for which q is bounded. By passing to a subsequence we may assume that q is fixed, and then $\lim_{d\to\infty}\mathrm{PC}(G) = 1 - 1/q$ is smallest when $q = 2$, in which case this limit is $1/2$. This completes the proof of Theorem II for the groups considered in this section.

Once again, more care with these same estimates yields $1 - \mathrm{PC}(G) < 9/10$ in every case within Table II. For example, if $m \equiv 2 \pmod 4$ with $m > 10$ and if q is even, then $\mathscr{M}(s)$ consists of the stabilizers of the three indicated subspaces, together with a subgroup $\mathrm{O}^-(2m, q)$. Use (3.18), and the g-invariant nonsingular subspaces of dimensions $m + 4$, $(3m + 2)/2$, and $(3m + 6)/2$ in (3.16), in order to obtain $P_s(g) \le 3(2/q^{m-1} + 1/q^m) + (1/q^{(m+4)/2} + 1/q^{m-4}) + (1/q^{(m-2)/4} + 1/q^{(3m+2)/2}) + (1/q^{(m-6)/4} + 1/q^{(3m+6)/2}) + (1/q + 1/q^m) < 9/10$. ▮

Remark. We decomposed V as the orthogonal direct sum of nonsingular subspaces whose dimensions were approximately $(\dim V)/2$ or $(\dim V)/4$. Other choices would have produced the same results. This flexibility means that, at least asymptotically, the class $\langle s\rangle^G$ is not at all uniquely determined.

On the other hand, if we ignore asymptotic results and wish for a precise optimal $\mathrm{PC}(G)$, presumably an irreducible s will produce the "best" possible bound. However, there are groups where no irreducible element s exists, such as $\Omega^+(2m, q)$; and in that case we could not use s of order $q^m - 1$, since a list of all maximal overgroups of such an element is not presently known.

5. CLASSICAL GROUPS: ADDITIONAL CASES

We exclude those groups that are already (central extensions of) alternating groups. There are a number of cases omitted in the preceding section, all in dimension at most 20. Here we will settle most of those, postponing until (6.3) the following groups: $\Omega(5,3)$, $\mathrm{PSU}(4,2)$, $\mathrm{PSU}(5,2)$, $\mathrm{PSU}(6,2)$, $\mathrm{PSU}(3,3)$, $\mathrm{PSU}(4,3)$, $\Omega^+(8,2)$, $\mathrm{P}\Omega^+(8,3)$, $\mathrm{Sp}(6,2)$, $\mathrm{Sp}(8,2)$, $\mathrm{P}\Omega^\pm(10,2)$, $\mathrm{Sp}(10,2)$, and $\mathrm{PSL}(11,2)$. In each case we will see that $1 - \mathrm{PC}(G) < 9/10$, and that $1 - \mathrm{PC}(G) \to 0$ as $q \to \infty$. The latter fact follows again by noting that $|\mathscr{M}(s)|$ is bounded independently of q. We will list groups, bound the order of a torus in which s lies, and list $\mathscr{M}(s)$. The arguments used to show that Theorem I holds are essentially identical for the almost simple case. By the remark after (2.3), no further justification is needed for the cases for which $|\mathscr{M}(s)| = 1$.

All assertions concerning $\mathscr{M}(s)$ follow from [GPPS].

PSL$(2,q)$, $q = 7$ or $q > 9$; $|s| = (q+1)/(2,q+1)$; $\mathscr{M}(s) = \{\mathrm{N}_G(\langle s \rangle)\}$, and (2.3) applies.

PSL$(3,q)$, $q > 2$. Let $|s| = (q^2+q+1)/(3,q-1)$; $\mathscr{M}(s)$ is $\{\mathrm{N}_G(\langle s \rangle)\}$ if $q \neq 4$ and $\{\mathrm{SL}(3,2)\}$ if $q = 4$, and (2.3) applies.

PSU$(4,q)$, $q > 3$, and PSU$(6,q)$, $q > 2$; s preserves a decomposition $1 \perp 2m-1$ as in Section 4 (below we will use abbreviations such as $s : 1 \perp 2m-1$); $\mathscr{M}(s)$ consists of the stabilizer of a 1-space, and (2.3) applies.

PSU$(3,q)$, $5 \neq q > 3$, PSU$(5,q)$, $q > 2$, and PSU$(7,q)$; $|s| = (q^d + 1)/(q+1)(d,q+1)$; $\mathscr{M}(s) = \{\mathrm{N}_G(\langle s \rangle)\}$; and (2.3) applies.

P$\Omega^-(8,q)$; $|s|\ |q^4+1$; $\mathscr{M}(s) = \{\mathrm{N}_G(\Omega^-(4,q^2))\}$; and (2.3) applies.

P$\Omega^-(10,q)$; $|s|\ |q^5+1$; $\mathscr{M}(s) = \{\mathrm{N}_G(\mathrm{SU}(5,q))\}$; and (2.3) applies.

P$\Omega^-(12,q)$; $|s|\ |q^6+1$; $\mathscr{M}(s) = \{\mathrm{N}_G(\Omega^-(4,q^3)), \mathrm{N}_G(\mathrm{P}\Omega^-(6,q^2))\}$; and (2.3) gives $1 - \mathrm{PC}(G) \le 4/3q^2 + 4/3q^3$.

P$\Omega^+(8,q)$, $q \ge 4$; $s : 2^- \perp 6^-$; $\mathscr{M}(s)$ consists of the stabilizer of a nonsingular 2-space, together with two subgroups obtained from it by applying triality; and if g does not induce a triality, then (3.16) gives

$$1 - \mathrm{PC}(G) \le 3\big(3/q^2 + 1/q^3 + 1/q^6\big).$$

If g does induce a triality outer automorphism, then $|\mathscr{M}(s)| = 1$ and (2.3) applies.

P$\Omega^+(2m,q)$, $2m = 12$, 16, 20; $s : 4^- \perp (2m-4)^-$; $\mathscr{M}(s)$ consists of $\mathrm{N}_G(\mathrm{P}\Omega^+(m,q^2))$ and the stabilizer of a nonsingular 4-space; (3.16) and (2.3) give the desired bounds.

$\Omega(7,q)$, $q \ge 5$ odd; $|s| = (q^3+1)/2$ (so $s : 1 \perp 6^-$); $\mathscr{M}(s)$ consists of the stabilizer of a nonsingular 1-space; and (2.3) applies. (Note that $G_2(q)$ does not occur because $|s| > q^2 - q + 1$.)

PSp$(4,q)$, $q \ge 4$; $|s| = q^2 + 1$; if q is even, then $\mathscr{M}(s)$ consists of $\mathrm{O}^-(4,q)$ and $\mathrm{PSp}(2,q^2).2$ (note that these subgroups are isomorphic and are interchanged by a graph automorphism); the results follow by (2.3). If q is odd, then only the group $\mathrm{PSp}(2,q^2).2$ occurs and (2.3) yields the result.

PSp$(6,q)$, $q \ge 4$; $s : 2 \perp 4$; $\mathscr{M}(s)$ consists of the stabilizer of a nonsingular 2-space and, if q is even, also a subgroup $\mathrm{O}^+(6,q)$; $1 - \mathrm{PC}(G)$ is at most $2/q + 1/q^3 + 1/q^2 + 1/q^2 < 9/10$ for odd $q \ge 5$ and $(2/q^2 + 1/q^3 + 1/q^2 + 1/q^2) + (1/q + 1/q^3) < 9/10$ for even $q \ge 4$, by (3.16) and (3.18).

Sp$(8,q)$, $q \ge 4$ even; $|s| = q^4 + 1$; $\mathscr{M}(s) = \{\mathrm{Sp}(4,q^2).2, \mathrm{O}^-(8,q)\}$; $1 - \mathrm{PC}(G) \le 4/3q + 1/q < 9/10$ by (2.3) and (3.18).

Sp$(10,q)$, $q > 2$ even; $s : 2 \perp 8$; $\mathscr{M}(s)$ consists of the stabilizer of a nonsingular 2-space and a subgroup $\mathrm{O}^+(10,q)$; $1 - \mathrm{PC}(G) \le (2/q^3 + 1/q^5 + 1/q^4 + 1/q^2) + (1/q + 1/q^5) < 9/10$ for even $q \ge 4$, by (3.16) and (3.18).

$\mathrm{Sp}(4k, q)$, q even, $k = 3$ or 5; $|s| = q^{2k} + 1$; $\mathscr{M}(s) = \{\mathrm{Sp}(2, q^k).k, \mathrm{Sp}(2k, q^2).2, \mathrm{O}^-(4k, q)\}$; $1 - \mathrm{PC}(G) \leq 4/3q^2 + 1/|G : \mathrm{Sp}(2, q^k).k| + 4/3q^2 + 1/|G : \mathrm{Sp}(2k, q^2).2| + 1/q < 9/10$ by (2.3) and (3.18).

$\mathrm{Sp}(16, q)$, q even; $|s| = q^8 + 1$; $\mathscr{M}(s) = \{\mathrm{Sp}(8, q^2).2, \mathrm{O}^-(16, q)\}$; $1 - \mathrm{PC}(G) \leq 4/3q^2 + 1/|G : \mathrm{Sp}(8, q^2).2| + 1/q < 9/10$ by (2.3) and (3.18).

6. EXCEPTIONAL GROUPS AND SPORADIC GROUPS

We next consider the exceptional and the sporadic simple groups, as well as the few classical groups not dealt with in the preceding section.

PROPOSITION 6.1. *Let G be an almost simple exceptional group of Lie type other than ${}^2G_2(3)' \cong \mathrm{PSL}(2,8)$, $G_2(2)' \cong \mathrm{PSU}(3,3)$, $G_2(3)$, $G_2(4)$, ${}^2F_4(2)'$, $F_4(q)$, $q \leq 3$, ${}^2E_6(q)$, $q \leq 3$, and $E_7(q)$, $q \leq 3$. Let $\langle s \rangle$ be a cyclic maximal torus of $F^*(G)$ whose order is given in Table III. Then $P_s(g) \leq \nu(G) \leq 2/3$, where $\nu(G)$ is given in the table. Moreover, for such groups G, Theorem* I *holds and* $\lim_{|G| \to \infty} \mathrm{PC}(G) = 1$.

Proof. By (2.3) we have $\mu(G) \leq 4/3q$.

It follows from [We] that an upper bound for $|\mathscr{M}(s)|$ is as given in Table III. The result in [We] is only for the case G simple. If $|\mathscr{M}(s)| = 1$ in the simple case, then clearly this is true as well for G (recall that we are excluding maximal subgroups which contain $F^*(G)$). In the remaining cases, it is easy to compute that the bound for $|\mathscr{M}(s)|$ is still valid for G. The result follows by using $\nu(G) := |\mathscr{M}(s)|\,\mu(G)$. ∎

We have excluded ${}^2G_2(3)' \cong \mathrm{PSL}(2,8)$, $G_2(2)' \cong \mathrm{PSU}(3,3)$, $G_2(3)$, $G_2(4)$, ${}^2F_4(2)'$; and also, for $q \leq 3$, $F_4(q)$, ${}^2E_6(q)$, and $E_7(q)$, because these groups are excluded in [We]. We now consider these excluded groups as well as the sporadic groups.

PROPOSITION 6.2. *Let $F^*(G)$ be a simple sporadic group or $G_2(3)$, $G_2(4)$, ${}^2F_4(2)'$, $F_4(q)$, $q \leq 3$, ${}^2E_6(q)$, $q \leq 3$ or $E_7(q)$, $q \leq 3$. Let $s \in F^*(G)$ be an element whose order is given in Table IV. Then $P_s(g) \leq \nu(G) < 9/10$, where $\nu(G)$ is given in the table.*

Proof. The values for $\mu(G)$ are given in [Ma] for the sporadic groups. We use the weak bound $4/3q$ in (2.3) for the larger exceptional groups (noting that $\mu(G) < 1/2$ also holds [GM]). The bounds for the smaller exceptional groups can be computed from the character tables. So our entire proof amounts to defining s and $T = \langle s \rangle$ so that $\mathscr{M}(s)$ is small.

First consider the case that $F^*(G)$ is a sporadic simple group other than B and M. Then the conjugacy classes of all maximal subgroups H are known (cf. [CCNPW, JLPW]). If $T \leq H$ then, since T is a Sylow subgroup

TABLE III

$F^*(G)$	$\lvert s\rvert$	$\lvert\mathscr{M}(s)\rvert$	$\nu(G)$
${}^2B_2(q)$, $q = 2^{2k+1} = q_0^2$, $k \geq 1$	$q_0^2 + \sqrt{2}q_0 + 1$	1	$4/3q$
${}^2G_2(q)$, $q = 3^{2k+1} = q_0^2$, $k \geq 1$	$q_0^2 + \sqrt{3}q_0 + 1$	1	$4/3q$
${}^2F_4(q)$, $q = 2^{2k+1} = q_0^2$, $k \geq 1$	$q_0^4 + \sqrt{2}q_0^3 + q_0^2 + \sqrt{2}q_0 + 1$	1	$4/3q$
$G_2(q)$, $q \geq 5$	$q^2 - q + 1$	≤ 2, 1 if $3 \nmid q$	$8/3q$
${}^3D_4(q)$	$q^4 - q^2 + 1$	1	$4/3q$
$F_4(q)$, $q \geq 4$	$q^4 - q^2 + 1$	≤ 2, 1 if $2 \nmid q$	$8/3q$
${}^2E_6(q)$, $q \geq 4$	$q^6 - q^3 + 1$	1	$4/3q$
$E_6(q)$	$q^6 + q^3 + 1$	1	$4/3q$
$E_7(q)$, $q \geq 4$	$(q + 1)(q^6 - q^3 + 1)$	1	$4/3q$
$E_8(q)$	$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$	1	$4/3q$

of G, by (2.4) the number of members of H^G containing T is $[\mathrm{N}_G(T) : \mathrm{N}_N(T)]$. This leads us to our computation of $\mathscr{M}(s)$. In Table IV we have listed the maximal subgroups in the simple case. In the almost simple case, $|\mathscr{M}(s)|$ either decreases or is unchanged. We can almost always take $\nu(G) := \mu(G)|\mathscr{M}(s)|$.

There are two special cases. If $G = HS$, then we note from [CCNPW] that $|\chi(x)/\chi(1)| \leq 1/4$ for every nontrivial $x \in G$ and any character $\chi \neq 1$ of G with $\langle \chi, 1 \rangle \leq 1$. In particular, $\mu(G) \leq 1/4$ (this is slightly better than the estimate in [Ma]: the element appearing there and requiring a larger estimate is an outer involution and hence does not concern us in the simple case). If $[G : HS] = 2$, then it follows from [CCNPW] that $|\mathscr{M}(s)| = 1$, whence the result follows. The second special case is $F^*(G) = M_{12}$. If $G = M_{12}$, one computes (using the permutation characters of the three maximal subgroups as given in [CCNPW]) that we may take $\nu(G) = 5/9$. If $G = \mathrm{Aut}\, M_{12}$, then by [CCNPW], it follows that $|\mathscr{M}(s)| = 2$ and so we may take $\nu(G) = 2/3$.

If $G = B$ or M, then enough is known about the maximal subgroups to show that the only possible maximal overgroups of T are either $\mathrm{N}_G(T)$ or almost simple groups (cf. [CCNPW, JLPW]). The only possible almost simple groups containing an element of order 47 and whose order divides $|B|$ have socle PSL(2, 47); however, PSL(2, 47) is not a subgroup of B since B contains no dihedral group of order 46. This shows that $\mathrm{N}_G(T)$ is the unique maximal overgroup of T when $G = B$, as we have claimed in Table IV.

If $G = M$, the only possible simple subgroup of order dividing that of M and containing an element s of order 59 is $H = \mathrm{PSL}(2, 59)$. Let E be a subgroup of order 29 in $\mathrm{N}_G(T)$, so $\mathrm{N}_G(E) = (29{:}\ 14 \times 3) \cdot 2$. Then H contains all involutions in $\mathrm{N}_G(E)$. Let U be the dihedral subgroup of order

TABLE IV

$F^*(G)$	$\lvert T\rvert = \lvert s\rvert$	$\mathscr{M}(T)$ in $F^*(G)$	$\mu(G)$	$\nu(G)$
M_{11}	11	PSL(2, 11)	$3/11$	$3/11$
M_{12}	11	PSL(2, 11), M_{11}, M_{11}	$1/3$	$2/3$
M_{22}	11	PSL(2, 11)	$3/11$	$3/11$
M_{23}	23	$\mathrm{N}_G(T)$	$7/23$	$7/23$
M_{24}	23	M_{23}, PSL(2, 23)	$1/3$	$2/3$
J_1	19	$\mathrm{N}_G(T)$	$5/133$	$5/133$
J_2	7	PSU(3, 3), PSU(3, 3), PGL(2, 7)	$1/7$	$3/7$
J_3	19	PSL(2, 19), PSL(2, 19)	$1/31$	$2/31$
J_4	37	$\mathrm{N}_G(T)$	$1/90$	$1/90$
HS	11	M_{11}, M_{11}, M_{22}	$1/4$	$3/4$
Mc	11	M_{11}, M_{22}, M_{22}	$7/55$	$21/55$
He	17	Sp(4, 4).2	$11/147$	$11/147$
Ru	29	$\mathrm{N}_G(T)$	$1/43$	$1/43$
Suz	13	$G_2(4)$, PSL(2, 25), PSL(2, 25), PSL(2, 25)	$1/11$	$4/11$
ON	31	PSL(2, 31), PSL(2, 31)	$1/143$	$2/143$
Co_3	23	M_{23}	$3/23$	$3/23$
Co_2	23	M_{23}	$71/575$	$71/575$
Co_1	23	Co_2, Co_3, $2^{11}.M_{24}$	$1/13$	$3/13$
Fi_{22}	13	$\Omega(7,3)$, $\Omega(7,3)$, ${}^2F_4(2)'$	$374/1755$	$374/585$
Fi_{23}	23	$2^{11}.M_{23}$, PSL(2, 23)	$1/9$	$2/9$
Fi'_{24}	29	$\mathrm{N}_G(T)$	$1/9$	$1/9$
HN	19	PSU(3, 8).3	$1/39$	$1/39$
Ly	67	$\mathrm{N}_G(T)$	$7/55$	$7/55$
Th	31	$\mathrm{N}_G(T)$, 2^5.PSL(5, 2), 2^5.PSL(5, 2), 2^5.PSL(5, 2)	$1/100$	$1/25$
B	47	$\mathrm{N}_G(T)$	$1/53$	$1/53$
M	59	$\mathrm{N}_G(T)$	$1/45$	$1/45$
$G_2(3)$	13	PSL(3, 3):2, PSL(3, 3):2, PSL(3, 13)	$1/7$	$3/7$
$G_2(4)$	13	PSL(2, 13):2, PSU(3, 4):2	$4/51$	$8/51$
${}^2F_4(2)'$	13	PSL(3, 3):2 twice, PSL(2, 25) thrice	$1/13$	$5/13$
$F_4(2)$	17	Sp(8, 2), Sp(8, 2)	$1/13$	$2/13$
$F_4(3)$	73	${}^3D_4(3).3$	$4/9$	$4/9$
${}^2E_6(2)$	19	SU(3, 8).3	$1/2$	$1/2$
${}^2E_6(3)$	$19 \cdot 37$	SU(3, 27).3	$4/9$	$4/9$
$E_7(2)$	$43 \cdot 3$	SU(8, 2)	$1/2$	$1/2$
$E_7(3)$	$4 \cdot 19 \cdot 37$	$2.{}^2E_6(3).2$	$4/9$	$4/9$

$29 \cdot 2$ of $\mathrm{N}_G(E)$ generated by these involutions. Then $H = \langle T, U\rangle$ is uniquely determined and contains $\mathrm{N}_G(T)$. In particular, there is a unique maximal subgroup containing T, as we have claimed in Table IV.

We now consider the exceptional groups in the proposition. We will first determine the maximal subgroups of $G = F^*(G)$ which contain T.

All maximal subgroups of ${}^2F_4(2)'$, $G_2(3)$, $G_2(4)$, and $F_4(2)$ are known (cf. [CCNPW, Kl, Bu, NW]) and the description of $\mathscr{M}(s)$ follows immediately.

Next consider $F_4(3)$. There is a maximal subgroup $M \cong {}^3D_4(3).3$ containing T. Proceed precisely as in [We] to conclude that if H is any other maximal overgroup of T, then H is an almost simple group of type $\mathrm{PSU}(3,9)$. We will show by way of contradiction that such an H does not exist.

Let V be the 25-dimensional module for $F_4(3)$, where $F_4(3) \leq \mathrm{SO}(V)$. Then T fixes a unique 1-space W of V which is also fixed by M (because as an M-module, V splits as a direct sum of a 24-dimensional module and a 1-dimensional module; the latter is obviously the fixed space of T). Let U be an irreducible H-submodule of V. Here H has no irreducible representation over $\mathbb{F}_3$ of dimension 25 (cf. [JLPW]). Moreover, any nontrivial simple T-module has dimension 12 over $\mathbb{F}_3$ (because 3 has order 12 modulo 73). Thus, any simple H-submodule U of V has dimension 1, 12, or 24. Moreover, if it has dimension 12, then it is isomorphic to the natural 3-dimensional module over $\mathbb{F}_{81}$ (cf. [JLPW])). If U has dimension 1 or 24, then U or $U^{\perp}$ is H-invariant. Thus, H is contained in the stabilizer of W and so H is contained in M. This is a contradiction (either to maximality or by order). The remaining possibility is that U is 12-dimensional. If W is not H-invariant, then V must be a uniserial H-module (with composition factors of dimension 12, 1, and 12). However, $H^1(H, U) = 0$ (cf. [JP]) and so V cannot be uniserial with composition factors of those dimensions. This completes the proof.

Next consider ${}^2E_6(q)$, $q \leq 3$. By [CLSS, LSS], the only local maximal subgroup containing T is its normalizer. It follows by [LiSe] that the only maximal subgroups containing T are almost simple (see also [M, 6.1]). The proof of [M, 6.1] shows that the only possible maximal overgroups are isomorphic to $\mathrm{PSU}(3, q^3).3$, or to $\mathrm{PSL}(2,19)$ for $q = 2$ (also see the main theorem in [As]). In fact, there is no subgroup isomorphic to $\mathrm{PSL}(2,19)$ (see [JLPW]; one can also use GAP [Sc] and character restriction arguments to show this, as was pointed out to us by Malle). In the case $\mathrm{PSU}(3, q^3).3$ the overgroup is shown to be unique exactly as in [We].

Last, consider $E_7(q)$, $q \leq 3$. If $q = 3$, then, by [LM, Sect. 6], T is contained in a unique maximal subgroup as listed. If $q = 2$ then $|T| = 129$. Let x be the element of order 3 in T. Then $C = \mathrm{C}_G(x) = 3 \times \mathrm{SU}(3,7)$. It follows as in [LM, Sect. 7] that the only maximal overgroups of T are $\mathrm{N}_G(T)$, C, and the normalizer of a simple subgroup isomorphic to $\mathrm{PSU}(8,2)$. Since in the algebraic group E_7 there is a subgroup $\mathrm{SL}_8.2$, in $E_7(2)$ there is a subgroup M isomorphic to $\mathrm{PSU}(8,2)$. We may assume that T is contained in M (since M contains an element of order 129 and a Sylow 43-subgroup of G is cyclic). It follows that $C \leq M$ as well. We claim that *there is a unique subgroup of* $E_7(2)$ *isomorphic to* $\mathrm{PSU}(8,2)$ *and containing* T. We may view $x = \mathrm{diag}(\omega^2, \omega, \ldots, \omega) \in M = \mathrm{PSU}(8,2)$, where ω is a primitive cube root of 1. Let $y = \mathrm{diag}(\omega, \omega^2, \omega, \dots, \omega)$. Then y is conjugate to x (in M). Moreover, y is central in $H := 3 \times \mathrm{PSU}(6,2) \leq C$. Also, $D := \mathrm{C}_G(y)$ is conjugate to C in G and hence is contained in M. Now consider any subgroup $P \cong \mathrm{PSU}(8,2)$ containing T. Note that since x commutes with T, $\mathrm{C}_P(x) \cong \mathrm{C}_G(x)$. Thus, $C \leq P$. In particular, $y \in H \leq P$. Moreover, $\mathrm{C}_P(y)$ properly contains H. Since C is maximal in P, it follows that $P = \langle C, \mathrm{C}_P(y)\rangle \leq M$, so P is uniquely determined. Thus, the unique maximal overgroup of T is $\mathrm{N}_G(M)$. Since $\mathrm{N}_G(M) = M\mathrm{C}_G(x)$ (because $\mathrm{N}_G(M)/M$ has order dividing 3), it follows that $M = \mathrm{N}_G(M)$ is maximal.

Finally, consider the case of one of these exceptional groups $F^*(G) < G$. We claim that $|\mathscr{M}(s)|$ is bounded by the corresponding value in the simple case. If this number is 1 for the simple group, this is clear. The remaining cases are all in [CCNPW]. ▮

We now consider some small dimensional classical groups over very small fields that were not dealt with in Section 5:

PROPOSITION 6.3. *If* $S = F^*(G)$ *is* PSU(3,3), PSU(3,5), PSU(4,2) $\cong$ $\Omega(5,3)$, PSU(4,3), PSU(5,2), PSU(6,2), Sp(6,2), PSp(6,3), $\Omega(7,3)$, Sp(8,2), $\Omega^+(8,2)$, $\mathrm{P}\Omega^+(8,3)$, $\mathrm{P}\Omega^+(10,2)$, Sp(10,2), *or* PSL(11,2), *then* $1 - \mathrm{PC}(G) < 9/10$.

Proof. Most of our estimates below are made using the character and maximal subgroup information in [CCNPW]. Often, the permutation character of the members of $\mathscr{M}(s)$ is given explicitly in [CCNPW] and so one can compute $|x^G \cap M|/|x^G|$ exactly. If not, we can use the bounds in [Ma] or use the simple observation that $|x^G \cap M|/|x^G| \leq \max_\chi(|\chi(x)| + 1)/(\chi(1) + 1)$ for any nontrivial character χ which is a constituent of the permutation character 1_M^G. We then obtain an upper bound for the ratio of the conjugates of x in the overgroups of s by summing the estimates for the various overgroups (but not trying to improve the estimates by keeping track of intersections of maximal subgroups).

If $S = \mathrm{PSU}(3,3)$ and $|s| = 7$, then $\mathscr{M}(s) = \{\mathrm{PSL}(2,7)\}$, so (2.3) applies.

If $S = \mathrm{PSU}(3,5)$, let s be of order 7. Then s is in exactly 3 maximal subgroups M, each isomorphic to A_7 (see [CCNPW]). One computes that $\mu(g, M^S) \leq 1/5$ for any $1 \neq g \in G$. Thus, $P_s(g) \leq 3/5$. More generally, if and $G > S$ then $|\mathscr{M}(s)| \leq 2$ and the result still follows.

If $S = \mathrm{PSU}(4,2) \cong \Omega(5,3)$, take s in the conjugacy class $9A$ in [CCNPW]. Then the permutation characters of the maximal subgroups are all given and one sees that s is in exactly 2 maximal groups each of index 40 (isomorphic to $3^3.S_4$ or $3^{1+2}:2A_4$). It follows by character estimates that $P_s(x) < 9/10$ for any nontrivial $x \in S$. The same estimate holds whenever we have G satisfying $F^*(G) = S$.

If $S = \mathrm{PSU}(4,3)$ and $|s| = 7$, then there are precisely 7 members of $\mathscr{M}(s)$ and all of their permutation characters are given in [CCNPW]. One computes directly that $P_s(x) < 9/10$ for all nontrivial x. The computation is similar but easier in the almost simple but not simple case.

If $S = \mathrm{PSU}(5,2)$ and $|s| = 11$, then $\mathscr{M}(s) = \{\mathrm{PSL}(2,11)\}$, so (2.3) applies.

If $S = \mathrm{PSU}(6,2)$, let s be of order 11. Then s is contained in precisely 7 maximal subgroups (cf. [CCNPW]): 3 isomorphic to M_{22}, 3 isomorphic to PSU(4, 3).2, and the stabilizer of a nonsingular 1-space. If x is not an element in the class $2A$, then using the character table we find that x fixes at most $29n/253$ points in any transitive permutation representation of S of degree n (this follows by bounding $\chi(x)/\chi(1)$ for any nontrivial character χ, using [CCNPW]). Then $P_s(x) \leq 203/253$. If x is in the class $2A$, then we compute from the character table that x fixes 256 of the 1408 points on the cosets of PSU(4, 3).2, and 160 of the 672 nonsingular 1-spaces. Moreover, x is not contained in any subgroup isomorphic to M_{22} (since M_{22} has a unique class of involutions, and this has size greater than $|x^S|$). This shows that $P_x(s) < 9/10$. A similar but easier computation gives the result if $G > S$.

If $G = \mathrm{Sp}(6,2)$, let s be of order 9. By [CCNPW], s is contained in exactly four maximal subgroups of G: one isomorphic to PSU(4, 2):2 and three isomorphic to PSL(2, 8):3. If x is a transvection, then x is not contained in any of the latter subgroups, whence $P_s(x) = 4/7$. Otherwise, by [CCNPW] the fixed point ratio in the first case is at worst $1/2$ and in the second actions at worst $51/960$. Thus, $P_s(x) < 9/10$.

If $S = \mathrm{PSp}(6,3)$, let s be of order 14. The two maximal subgroups containing s are isomorphic to PSL(2, 27):3 and $(2 \times \mathrm{PSU}(3,3)).2$. It follows by character estimates using [CCNPW] that $P_x(s) < 9/10$ for any nontrivial x. Similarly, we see the same result holds if $G > S$.

If $S = \Omega(7,3)$, let s be of order 13. The maximal subgroups containing s are 2 copies of $G_2(3)$, 2 stabilizers of 3-dimensional totally singular subspaces, and the stabilizer of a nonsingular 6-space of + type. Using the character table, we see that the worst case is for x of type $3A$, and we find that $P_x(s) \leq 17/28$. A similar argument suffices if $G > S$ (then there are only two maximal subgroups to consider).

If $S = \mathrm{Sp}(8,2)$, let s be of order 17. By [GPPS], the three maximal subgroups containing s are isomorphic to $\mathrm{O}^-(8,2)$, Sp(4, 2):2, and PSL(2, 17). Since each of these subgroups contains the full normalizer of a Sylow 17-subgroup and there is a unique conjugacy class of each type of subgroup, it follows that s is contained in precisely one maximal subgroup of each conjugacy class. If x is a transvection, then x is contained in only the first subgroup, and we find that $P_x(s) = 8/15$. If x is not a transvection, we compute (via the character table) that x fixes at most $3/10$, $1/2$, and $1/10$ of the cosets of the three subgroups, respectively. Thus, $P_x(s) < 9/10$.

Case $S = \Omega^+(8,2)$. This case is a bit more involved than the previous ones. Let $s \in S$ be of order 15 (specifically, of type $15A$ using the notation in [CCNPW]; thus, s fixes two singular points). By [CCNPW] there are precisely seven maximal subgroups of S containing s, isomorphic to $\mathrm{Sp}(6,2)$, 2^6A_8, 2^6A_8, A_9, A_9, 3PSU $(4,2)$ or $(A_5 \times A_5).2^2$. The permutation characters for the first six are given in [CCNPW]. Using GAP (with help from Thomas Breuer), one computes the seventh permutation character. For most elements x, this is sufficient to deduce that $P_s(x) < .7$. In three cases (for x in classes 2A, 2B or 3A), more work is needed, taking intersections into account. A hand calculation yields $P_s(x) < 1$; using GAP (again with help from Thomas Breuer), one computes that in fact $P_s(x) < .7$ for all nontrivial $x \in S$.

Moreover, $P_s(x) = 0$ if $x \in G \setminus S$, so that $\mathrm{PC}(G) \geq .3$. Namely, for such an x the elements s and s^x are not conjugate in S, and hence $S = \langle s, s^x \rangle$ by [CCNPW] (i.e., there are no maximal subgroups of S which intersect 2 different S-classes of elements of order 15). It follows that $\langle x, s \rangle = \langle S, x \rangle \geq S = O_\infty(G)$ and hence $P_s(x) = 0$.

Case $S = \mathrm{P}\Omega^+(8,3)$. This also takes a bit longer to handle. Suppose that G is a group with socle S, and let $s \in S$ be in the conjugacy class $20A$ (cf. [CCNPW]). Then s is contained in precisely 9 maximal subgroups: the stabilizers of 1, 2, or 3 dimensional nondegenerate subspaces of $+$ or $-$ type, two totally singular 1-spaces, and a 4-dimensional nondegenerate subspace of $-$ type. If C is a nontrivial conjugacy class of S, a straightforward computation using [CCNPW] shows that the probability that $g \in C$ fixes one of those spaces is less than $9/10$. Since the classes $20A$, $20B$, and $20C$ are fused by the triality automorphism, the same computation is valid for those classes. If g is a diagonal outer automorphism of order 2, then the character values are not given in [CCNPW], but the same estimate holds via a computation done in GAP by T. Breuer (we may assume that $g \in \mathrm{PSO}(8,3)$ by applying a triality automorphism).

Let G be an almost simple group with socle $S < G$. By the previous paragraph, we may assume that G contains a graph automorphism of order 2 or 3. Note that the diagonal automorphisms preserve each of the classes $20A$, $20B$, and $20C$, while the graph automorphisms act as S_3 on this set. Thus in G, there is a single conjugacy class of elements of order 20 contained in S or there are 2 such classes with one of cardinality twice the other.

We will take s to be an element of order 20 in the largest G-conjugacy class of elements of order 20 contained in S.

Note that no proper subgroup of S intersects more than one of the classes of elements of order 20. Thus, if $x \in G$ does not stabilize each of the three conjugacy classes, the probability that a random element of order 20 in G together with x generate a group containing S is either 1 (if x transitively permutes the three classes) or is at least $2/3$. Thus, for the largest conjugacy class of elements (of S) of order 20 in G and for any nontrivial $x \in G$, the probability of generating a group containing S is greater than $1/10$.

We note that a GAP computation (performed by T. Breuer) shows that we may take s of order 13 when $G = S$ (cf. (8.1) below).

If $S = P\Omega^+(10,2)$, let s be of order 51 acting irreducibly on both a nonsingular space of dimension 8 and its orthogonal complement. The only maximal overgroup of s in S is the stabilizer of the nonsingular 8-space, whence (2.3) applies.

If $G = \mathrm{Sp}(10,2)$, let s be of order 51 acting irreducibly on both a nonsingular space of dimension 8 and its orthogonal complement. By [GPPS], the only maximal subgroups containing s are $M_1 = \mathrm{O}^+(10,2)$ and the stabilizer M_2 of the nonsingular 8-space. First suppose that g is not a transvection. By (3.18), $\mu(g, M_1^G) \le 9/32$. By [GM], $\mu(g, M_2^G) \le 1/2$. Thus, $P_s(g) \le 25/32$. If g is a transvection, then $\mu(g, M_1^G) \le 15/32$, while g fixes $2^8 + 2^2(2^8-1)2^7/3 \cdot 2$ of the $2^8 + 2^2(2^{10}-1)2^9/3 \cdot 2$ nonsingular 2-spaces. Thus, $\mu(g, M_2^G) < 1/4 + 1/256$, whence the result.

If $S = \mathrm{PSL}(11,2)$ and $|s| = 2^{11} - 1$, then $\mathscr{M}(s) = \{\mathrm{N}_S(\langle s \rangle)\}$, so (2.3) applies.

7. ALTERNATING AND SYMMETRIC GROUPS

In this section we will conclude the proof of the theorems by studying the alternating group A_n and the symmetric group S_n. For any integer $q \ge 2$ let c_q denote a q-cycle. Let $\mathbf{S}_k$ denote the set of all k-sets of the n-set. Throughout this section, g will denote an element of prime order p.

We begin with Theorem I, which only requires 19th century group theory for A_n and S_n:

PROPOSITION 7.1. *If $G = A_n$ or S_n then $\mathrm{PC}(G) > 1/10$ for all $n \ge 5$.*

Proof. The cases $n \le 7$ are left to the reader (use $|s| = 5, 5, 7$ for $n = 5, 6, 7$, respectively).

Case 1. *n even*. Write $n = 2m + d$ with $d = 2$ or 4 and m odd. Let $C_G = s^G$, where s is the product of disjoint cycles of lengths m and $m + d$. Note that these lengths are relatively prime, so that one power of s is an m-cycle and another is an $m + d$-cycle.

The only maximal subgroup J containing s is the stabilizer of the s-invariant m-set. For, this is clear if J is intransitive. If J is transitive then it is primitive since the cycle lengths of s are different and are not factors of n. Since $\langle s\rangle$ contains an m-cycle with $m < n/2$, we obtain the contradiction $J = G$ by an unpublished 1892 theorem of Marggraf [Wie, 13.6].

If g' denotes a p-cycle, then

$$\begin{aligned}\mu(g,\mathbf{S}_m) &\le \mu(g',\mathbf{S}_m) \le \Pr\{\langle h,s\rangle \text{ is intransitive} \mid h \in g'^G\}\\ &\le \left\{\binom{m}{p} + \binom{n-m}{p}\right\}\Big/\binom{n}{p}\\ &\le \left\{\binom{m}{2} + \binom{n-m}{2}\right\}\Big/\binom{n}{2} < 3/4.\end{aligned}$$

Thus, $1 - \mathrm{PC}(G) < 3/4$ by (2.2).

Case 2. *n odd and $G = A_n$*. Let $C_G = s^G$, where s is the product of three disjoint cycles of lengths k_1, k_2, k_3, as follows for some odd m,

$$\begin{aligned}&m+1, m, m-1 && \text{if } n = 3m\\ &m, m, m+2 && \text{if } n = 3m+2\\ &m, m, m-2 && \text{if } n = 3m-2.\end{aligned}$$

Then a power of s is a cycle of length m or $m \pm 2$ since that length is relatively prime to the other cycle lengths.

Any transitive subgroup J of G containing s is primitive. (For, a block would have to have length at least one of the three cycle-lengths and also be a factor of n; and three blocks of length m would not be permuted by s.) Then once again $J = G$ by Marggraf's theorem. Thus, by (2.2), $1 - \mathrm{PC}(G)$ is bounded above by the sum of three quantities $\mu(g,\mathbf{S}_k)$ with $m - 2 \le k \le m + 2$. Clearly, $\mu(g,\mathbf{S}_k) \le \mu(g',\mathbf{S}_k)$, where g' is either a p-cycle for $p \ge 3$ or the product of two disjoint 2-cycles.

If $p \ge 5$ then, as in Case 1,

$$\mu(g,\mathbf{S}_k) \le \left\{\binom{k}{p} + \binom{n-k}{p}\right\}\Big/\binom{n}{p} \le \left\{\binom{k}{5} + \binom{n-k}{5}\right\}\Big/\binom{n}{5},$$

and adding the required 3 terms using the specific pairs n, m we calculate that $1 - \mathrm{PC}(G) < 3/4$.

If g' is a 3-cycle, we will proceed more directly in order to determine $1 - P_{g'}(s) = \Pr\{\langle h, s\rangle$ is transitive $\mid h \in g'^G\}$ precisely. Since each point moved by g' must be in a different cycle of s, there are exactly $2k_1k_2k_3$

choices for g', so $1 - P_{g'}(s) = 2k_1k_2k_3/2\binom{n}{3}$. In view of the values of k_1, k_2, k_3, it follows that $\Pr\{s \in \mathrm{C}_G$ and $\langle g, s\rangle$ is transitive$\} > 1/10$ for each n.

Finally, when g' is the product of two disjoint transpositions we will again determine $1 - P_{g'}(s) = \Pr\{\langle h, s\rangle$ is transitive $\mid h \in g'^G\}$. Clearly, $\langle h, s\rangle$ is transitive if and only if $h = (a, b)(c, d)$ where a and c lie in one cycle of s while b lies in a second cycle and d lies in the remaining cycle. Then $1 - P_{g'}(s) = \{\sum k_\alpha(k_\alpha - 1)k_\beta k_\gamma\}/3\binom{n}{4}$, summed over the three ordered triples $(\alpha, \beta, \gamma) = (1,2,3), (2,3,1), (3,1,2)$. This is more than $1/10$ in view of the specific lengths k_α.

Case 3. *n is odd and $G = S_n$*. Let $n = 2m + 1$, let s be the product of disjoint cycles of lengths m and $m + 1$, and proceed as in Case 1. ▮

PROPOSITION 7.2. (i) *If $s \in A_n$ has at least two cycles, then $P_s(c_3) \geq 1/4 + O(1/n)$.*

(ii) $\lim \mathrm{PC}(A_{2l}) = 3/4$.

Proof. (i) Let k be a cycle length of s. Since $x(x-1)(x-2)$ is concave up for $x \geq 1$,

$$P_s(c_3) \geq \left\{\binom{k}{3} + \binom{n-k}{3}\right\} \Big/ \binom{n}{3} \geq 2\binom{[n/2]}{3} \Big/ \binom{n}{3} = 1/4 + O(1/n).$$

(ii) In view of (i), it suffices to show that, *for the same s as in Case* 1 *of the proof of* (7.1), we have $P_s(g) \leq 1/4 + O(1/n)$ *for all* $g \in G$ of prime order p. This time $P_s(g) \leq P_s(g') = P_{g'}(s)$, where g' is either a p-cycle for $p \geq 3$ or the product of two disjoint 2-cycles. Now $P_{g'}(s) = \Pr\{\langle h, s\rangle$ is intransitive $\mid h \in g'^G\}$ is at most

$$\left\{\binom{m}{p} + \binom{n-m}{p}\right\} \Big/ \binom{n}{p} \leq 1/2^{p-1} + O(1/n)$$

or

$$\left\{3\binom{m}{4} + 3\binom{n-m}{4} + \binom{m}{2}\binom{n-m}{2}\right\} \Big/ 3\binom{n}{4} = 1/4 + O(1/n),$$

respectively. ▮

In order to go further with asymptotic results, it remains to consider the case of an n-cycle $s = c_n$. This requires some preliminaries (7.4), (7.5), leading to the desired results (Propositions 7.6 and 7.8).

Whenever $l \mid n$, $1 < l < n$, let $\pi(l)$ denote the set of orbits of c_n^l, let $M(l) \cong S_{n/l} \wr S_l$ be its set-stabilizer in S_n, and write $\Pi(l) = \pi(l)^{S_n}$. We will need to estimate

$$\mu(g, \Pi(l)) = \Pr\{g' \text{ lies in } M(l) \mid g' \in g^G\} \tag{7.3}$$

whenever $1 \neq g \in G = A_n$ or S_n, using the different points of view expressed by the two sides of this equation. Note that the left side does not depend on which G is used if $g \in A_n$.

LEMMA 7.4. *Let $g \in S_n$ be of prime order q.*

(i) *If n/l is bounded then $\mu(g, \Pi(l)) = O(1/n)$.*

(ii) *Assume that $n/l \geq 8$.*

(a) *If $q \geq 5$, then $\mu(g, \Pi(l)) \leq \mu((1,2,3,4,5), \Pi(l))$;*

(b) *if $q = 3$ and g is not a 3-cycle, then $\mu(g, \Pi(l)) \leq \mu((1,2,3)(4,5,6), \Pi(l))$; and*

(c) *if $q = 2$ and g is the product of at least four disjoint transpositions, then $\mu(g, \Pi(l)) \leq \mu((1,2)(3,4)(5,6)(7,8), \Pi(l))$.*

Proof. In each situation we will define an injective map (or in one case of (i), a 2 to 1 map), $\Theta : \mathrm{Fix}_{\Pi(l)}(g) \to \mathrm{Fix}_{\Pi(l)}(c)$, where $c = (1,2)$ in (i), while in (ii) we will use $c = (1,2,3,4,5)$ if $q \geq 5$, $(1,2,3)(4,5,6)$ if $q = 3$, or $c = (1,2)(3,4)(5,6)(7,8)$ if $q = 2$. Then in (ii) we will have $\mu(g, \Pi(l)) \leq \mu(c, \Pi(l))$ by the definition of μ.

We may assume that $g = (1,2,\dots,q) \cdots (1 + (b-1)q, \dots, bq)$ for some integer $b \geq 1$. Within each cycle of g we assume that its members are written mod q. (For example, if $q = 3$ and $i = 2$, the symbols i, $i+1$, $i+2$ should be interpreted as 2, 3, 1.)

Consider $\pi \in \mathrm{Fix}_{\Pi(l)}(g)$. If $\pi \in \mathrm{Fix}_{\Pi(l)}(c)$ let $\pi\Theta = \pi$. If $\pi \notin \mathrm{Fix}_{\Pi(l)}(c)$ we define $\pi\Theta \in \mathrm{Fix}_{\Pi(l)}(c) - \mathrm{Fix}_{\Pi(l)}(g)$ by giving its precise members. For this purpose we need some shorthand notation. We will write a partition π by listing some of the elements of our n-set X, using $/$ as a divider between different blocks of π; all other elements of X are assumed to be in the same blocks of both π and $\pi\Theta$ and are represented by $*$. We emphasize that, since we are comparing fixed points of g and c, we always have both of these permutations available during our discussions. We also note that there are many other similar choices for Θ.

(i) Use $c = (1,2)$ and define $\pi \to \pi\Theta$ as follows:

$$\begin{gathered} 1, i* \,/\, 2, i+1* \to \\ 1, 2* \,/\, i, i+1* \end{gathered}$$

If $q \neq 2$, there is only one block of $\pi\Theta$ that does not contain 1 but meets a cycle of g twice. This determines i and hence also π. If $q = 2$, there are two such blocks, whence i and $i + 1$ are determined and so there are just two choices for π.

Thus, for any q we see that $|\mathrm{Fix}_{\Pi(l)}(g)| \leq (2, q)|\mathrm{Fix}_{\Pi(l)}((1,2))|$. Then

$$\begin{aligned} \mu(g, \Pi(l)) &\leq 2\mu(c, \Pi(l)) = 2|\mathrm{Fix}_{\Pi(l)}((1,2))|/|(1,2)^G| \\ &= l\binom{n/l}{2}\Big/\binom{n}{2} < 2(n/l)/n, \end{aligned}$$

which is $O(1/n)$ since n/l is bounded.

(ii) If $q \geq 5$ use $c = (1,2,3,4,5)$ and define $\pi \to \pi\Theta$ as follows:

$$\begin{array}{l} 1, i, j, u, v* \Big/ 2, i+1, j+1, u+1, v+1* \Big/ 3, i+2, j+2, u+2, v+2* \Big/ 4, u+3* \Big/ 5* \to \\ 1,2,3,4,5* \Big/ i, i+1, i+2, j, j+1* \Big/ u, u+1, u+2, j+2, v* \Big/ u+3, v+2* \Big/ v+1* \end{array}$$

Here there are three cycles of g each meeting some block of $\pi\Theta$ at least twice. This determines i, j, and u. Now v is the only member of the block of $\pi\Theta$ containing $u + 2$ such that $v + 2$ lies in the block containing $u + 3$. Then the blocks of $\pi\Theta$ containing $v + 2$ or $v + 1$ determine all members of the blocks of π containing 4 or 5.

If $q = 3$ then we must consider the possible ways a partition π can be fixed by g but not by c:

$$\begin{array}{l} 1, i, u* \Big/ 2, i+1, u+1* \Big/ 3, i+2, u+2* \Big/ 4, j, v^* \Big/ 5, j+1, v+1* \Big/ 6, j+2, v+2* \to \\ 1,2,3* \Big/ 4,5,6* \Big/ i, i+1, j* \Big/ j+1, j+2, v* \Big/ u, u+1, v+2* \Big/ i+2, u+2, v+1* \end{array}$$

$$\begin{array}{l} 1,2,3,u* \Big/ 4, i, j* \Big/ 5, i+1, j+1* \Big/ 6, i+2, j+2* \to \\ 1,2,3,i* \Big/ 4,5,6* \Big/ i+1, i+2, j* \Big/ j+1, j+2, u* \end{array}$$

$$\begin{array}{l} 4,5,6,u* \Big/ 1, i, j* \Big/ 2, i+1, j+1* \Big/ 3, i+2, j+2* \to \\ 4,5,6,i* \Big/ 1,2,3* \Big/ i+1, i+2, j* \Big/ j+1, j+2, u*. \end{array}$$

In the first of these cases three 3-cycles of g have intersection sizes 1 and 2 with blocks of $\pi\Theta$; two of these 3-cycles have members in the same block of $\pi\Theta$, thereby determining i and j, and hence also u; and finally, v is the only member of the block containing $j + 1$ such that $v + 1$ is in the block containing $i + 2$. In the second and third cases there is a unique block of $\pi\Theta$ such that the removal of exactly one member produces a g-invariant set. This determines the first listed block as well as i. Moreover, this time there are two 3-cycles of g having intersection sizes 1 and 2 with blocks; this determines j. Finally, $j + 1$, $j + 2$, u are the only members of their block whose images are not in the block containing 4, thereby determining u. As before, once i, j, u are known then we can reconstruct all blocks of π from those of $\pi\Theta$.

Finally, if $q = 2$ we introduce some terminology: the "basic" blocks of π or $\pi\Theta$ are those containing members of $I = \{1, \dots, 8\}$. We abbreviate $i' = i + 1$ (so that $i'' = i$ using the convention already introduced above). Since there are various ways g can fix π such that c does not fix π, we introduce an ordering of the blocks in π in order to decrease the number of cases to be considered. We begin by listing the members of π, starting with the basic blocks in decreasing order of size r of intersection with I. For each such r we list the corresponding blocks in increasing order in terms of the smallest member of I in the block. This produces a permutation of I, which we denote by $\mathbf{1}, \dots, \mathbf{8}$ (except in case (I) below, where this is just the identity permutation); this notion was implicit in the previous discussion of the case $q = 3$, where the two relevant permutations of $\{1, \dots, 6\}$ were 1, 2, 3, 4, 5, 6 and 4, 5, 6, 1, 2, 3. Finally, we use the abbreviation $\mathbf{1} \dots \mathbf{4}$ for $\mathbf{1}$, $\mathbf{2}$, $\mathbf{3}$, $\mathbf{4}$, with a similar meaning for $\mathbf{1} \dots \mathbf{6}$.

Now let $\pi \to \pi\Theta$ be as follows, depending upon how g fixes π:

(I)

$$\begin{gathered} 1, i, u * / 2, i', u' * / 3, j, v * / 4, j', v' * / 5 * / 6 * / 7 * \ / 8 * \to \\ 1, 2, j * / 3, 4, i * \ \ / 5, 6, u * / 7, 8, v * \ \ / i' * / j' * / u' * / v' * \end{gathered}$$

(II)

$$\begin{gathered} \mathbf{1}, \mathbf{2} * / \mathbf{3}, i, j * / \mathbf{4}, i', j' * / \mathbf{5}, u * / \mathbf{6}, u' * / \mathbf{7} * \ / \mathbf{8} * \to \\ \mathbf{1}, \mathbf{2} * / \mathbf{3}, \mathbf{4}, i * / \mathbf{5}, \mathbf{6}, u * \ / \mathbf{7}, \mathbf{8} * / i', j' * / u' * / j * \end{gathered}$$

(III)

$$\begin{gathered} \mathbf{1}, \mathbf{2}, x * / \mathbf{3}, \mathbf{4} * / \mathbf{5}, i * / \mathbf{6}, i' * / \mathbf{7} * / \mathbf{8} * \to \\ \mathbf{1}, \mathbf{2}, i * \ / \mathbf{3}, \mathbf{4} * / \mathbf{5}, \mathbf{6} * / \mathbf{7}, \mathbf{8} * / i' * / x * \end{gathered}$$

(IV)

$$\begin{gathered} \mathbf{1}, \mathbf{2}, x * / \mathbf{3}, \mathbf{4}, y * / \mathbf{5}, \mathbf{6} * / \mathbf{7}, i, j * \ / \mathbf{8}, i', j' * \to \\ \mathbf{1}, \mathbf{2}, i * \ / \mathbf{3}, \mathbf{4}, j * / \mathbf{5}, \mathbf{6} * / \mathbf{7}, \mathbf{8}, y * / i', j', x * \end{gathered}$$

(V)

$$\begin{gathered}\mathbf{1}\ldots\mathbf{4}*/\mathbf{5},i,j*/\mathbf{6},i',j'*/\mathbf{7}*/\mathbf{8}*\ \rightarrow\\ \mathbf{1}\ldots\mathbf{4}*/\mathbf{5},\mathbf{6},i*/\mathbf{7},\mathbf{8},j*\ \ /i'*/j'*\end{gathered}$$

(VI)

$$\begin{gathered}\mathbf{1}\ldots\mathbf{4}*/\mathbf{5},\mathbf{6},x,y*/\mathbf{7},i,j*\ \ /\mathbf{8},i',j'*\ \rightarrow\\ \mathbf{1}\ldots\mathbf{4}*/\mathbf{5},\mathbf{6},i,j*\ \ /\mathbf{7},\mathbf{8},i'*/j',x,y*\end{gathered}$$

(VII)

$$\begin{gathered}\mathbf{1}\ldots\mathbf{6},x,y*/\mathbf{7},i,j*\ \ /\mathbf{8},i',j'*\ \rightarrow\\ \mathbf{1}\ldots\mathbf{6},i,j*\ \ /\mathbf{7},\mathbf{8},i'*/j',x,y*\end{gathered}$$

Recall that $n/l \geq 8$, so that all of these possibilities can occur.

We now describe an algorithm that recovers π from $\pi\Theta$. Determine the smallest set of blocks of $\pi\Theta$, including the basic blocks, whose removal from $\pi\Theta$ is g-invariant; there are between three and eight such blocks. Place these at the start of the listing of the blocks in $\pi\Theta$. The number of such blocks, combined with the occurrence of basic blocks meeting I more than twice, determines which of the seven cases we are in. Next, reorder the blocks in $\pi\Theta$ so that the basic blocks occur first, in decreasing order of intersection size r with I; and then, for each such r, list the corresponding blocks in increasing order in terms of the smallest member of I in the block. A brief glance at the seven cases shows that we have obtained for $\pi\Theta$ the same permutation of I obtained above for π.

We now discuss each of the seven cases.

(I) For the block in $\pi\Theta$ containing 2, j or 3, 4, i or 5, 6, u or 7, 8, v, at least $n/l - 3 \geq 5$ other members are sent by g into the same block; this determines i, j, u, v. This also determines the blocks of π to which members of I belong, both in this case and, similarly, in the remaining six.

(II) At least $n/l - 3$ other members of the block of $\pi\Theta$ containing **4**, i or **5**, **6**, u or i', j' are sent by g into the same block.

(III) All other members of the basic block of $\pi\Theta$ containing i are sent by g into this block. All other members of the block containing x are sent into the same block.

(IV) All other members of the basic block of $\pi\Theta$ containing i or j are sent by g into the same block. All other members of the block containing **8**, y or i', j', x are sent into the same block.

(V) All other members of the block of $\pi\Theta$ containing **5**, **6**, i or **7**, **8**, j are sent by g into the same block.

(VI, VII) All other members of the basic block of $\pi\Theta$ containing i, j are sent by g into the same block. All other members of the block containing x, y are sent into the same block. ▮

Throughout the remainder of this section primes will be denoted by the symbol p. Let $\rho(n)$ denote the smallest prime divisor of n.

LEMMA 7.5. *Let $G = A_n$ or S_n.*

(i) $\Pr\{g$ *is in some* $M(l) \mid g \in (1,2,3)^G\} = 1 - \prod_{p\mid n}(1 - 1/p^2) + O(1/n)$.

(ii) $\Pr\{g$ *is in some* $M(l) \mid g \in (1,2)(3,4)^G\} = 1 - \prod_{p\mid n}(1 - 1/p^2) + O(1/n)$.

(iii) *If $x \in G$ has prime order $q \geq 5$, then* $\Pr\{g$ *is in some* $M(l) \mid g \in x^G\} \leq 1/3\rho(n)^3 + O(1/n)$.

(iv) *If $x \in G$ has order* 3 *and moves at least* 6 *points, then* $\Pr\{g$ *is in some* $M(l) \mid g \in x^G\} \leq 1/3\rho(n)^3 + O(1/n)$.

(v) *If $x \in G$ has order* 2 *and moves at least* 8 *points, then* $\Pr\{g$ *is in some* $M(l) \mid g \in x^G\} \leq 1/3\rho(n)^3 + O(1/n)$.

(vi) *If $x \in A_n$ then* $\Pr\{g$ *is in some* $M(l) \mid g \in x^{A_n}\} \leq 1 - \prod_{p\mid n}(1 - 1/p^2) + O(1/n)$.

(vii) *If $x \in S_n$, then* $\Pr\{g$ *is in some* $M(l) \mid g \in x^{S_n}\} \leq \Pr\{g$ *is in some* $M(l) \mid g \in (1,2)^{S_n}\} + O(1/n) = 1 - \prod_{p\mid n}(1 - 1/p) + O(1/n)$.

Proof. Let $1 < l$ be a divisor of n such that $k = n/l > 1$. The contributions to the various stated probabilities of the cases $k < 8$ are $O(1/n)$, by (7.4)(i). Hence, we may restrict our attention to the case $k \geq 8$.

(i) If g lies in $M(l)$ then it lies in $M(l')$ for every l' dividing l. Hence, we need to consider $M(p)$ with p prime, together with intersections of these subgroups $M(p)$, which requires that we also consider $M(l)$ for squarefree l.

Since $n/l \geq 3$, the probability that g lies in $M(l)$ is $l\binom{k}{3}/\binom{n}{3} = (n^2l^{-2} - 3nl^{-1} + 2)/(n-1)(n-2)$. By Inclusion–Exclusion, if $x = (1,2,3)$ then $\Pr\{g$ is in some $M(l) \mid g \in x^G\}$ is

$$\frac{n^2\Sigma'(-1)^{t-1}(p_1\cdots p_t)^{-2} - 3n\Sigma'(-1)^{t-1}(p_1\cdots p_t)^{-1} + 2\Sigma'(-1)^{t-1}}{(n-1)(n-2)},$$

where Σ' ranges over all $t \geq 1$ and all subsets of t distinct prime factors p_i of n such that $n/p_1\cdots p_t \geq 8$. Note that $\Sigma(-1)^{t-1}(p_1\cdots p_t)^{-i} = 1 - \prod_{p\mid n}(1 - 1/p^i)$ is bounded for $i = 1, 2$ (where in the summation Σ we now allow the possibility $(p_1\cdots p_t)^{-1} < 8/n$). This implies (i).

(ii) Since $k > 2$, once again if g lies in $M(l)$ then it fixes every member of $\pi(l)$ and hence lies in $M(l')$ for every l' dividing l. There are two ways g can fix some member π of some $\Pi(l)$: both transpositions might be in different blocks or they might be in the same block of π (these correspond to the partitions $(2,2)$ and (4) of 4). The first case occurs with probability $\binom{l}{2}\binom{k}{2}^2/\binom{n}{4}3$, while the second occurs with probability $l\binom{k}{4}3/\binom{n}{4}3$. As in (i) the sum of these probabilities can be written $\{(n-4)n^2l^{-2}+(-2n+10)nl^{-1}+(n-6)\}/(n-1)(n-2)(n-3)$. By Inclusion–Exclusion, if $x=(1,2)(3,4)$ then $\Pr\{g \text{ is in some } M(l) \mid g \in x^G\}$ is

$$\frac{\begin{array}{l}(n-4)n^2\Sigma'(-1)^{t-1}(p_1\cdots p_t)^{-2}\\ \qquad +(-2n+10)n\Sigma'(-1)^{t-1}(p_1\cdots p_t)^{-1}+(n-6)\Sigma'(-1)^{t-1}\end{array}}{(n-1)(n-2)(n-3)},$$

from which (ii) follows as before.

(iii) By (7.4)(ii), the probability that a random $g \in x^G$ is in $M(l)$ is at most the corresponding probability when x is a 5-cycle, which is $l\binom{k}{5}/\binom{n}{5} < l^{-4}$. Thus, summing over all l (and not taking into account overlaps as we did above), we see that, up to a term $O(1/n)$ caused by our restriction $n/l \geq 8$, the probability that a random conjugate of x lies in some $M(l)$ with $n/l \geq 8$ is at most

$$\sum_{l \geq \rho(n)} l^{-4} < \int_{\rho(n)}^{\infty} x^{-4}\,dx = 1/3\rho(n)^3,$$

as required.

(iv) By (7.4)(iib), $\mu(x,\Pi(l)) \leq \mu((1,2,3)(4,5,6),\ \Pi(l))$, which is $\binom{l}{2}\binom{k}{3}^2/(\binom{k}{3}^2/2) + l\binom{k}{3}\binom{k-3}{3}/\binom{n}{3}\binom{n-3}{3} < 1/l^4$; the terms correspond respectively to the partitions $(3,3)$, (6) of 6. Now proceed as in (iii).

(v) By (7.4)(iic), the probability that a random conjugate of x lies in $M(l)$ is at most the corresponding probability for the case $x = (1,2)(3,4)(5,6)(7,8)$. In the latter case we again find that $\mu(x,\Pi(l)) < 1/l^4$, which yields the desired bound as in (iii).

(vi) By (i)–(v) the stated probability is bounded above by either $1/3\rho(n)^3 + O(1/n)$ or $1-\prod_{p\mid n}(1-1/p^2)+O(1/n)$. Then $\prod_{p\mid n}(1-1/p^2) \leq 1-1/\rho(n)^2 < 1-1/3\rho(n)^3$ implies (vi).

(vii) It suffices to consider elements x of prime order q. If x is a transposition, then, as in (i), we find that the probability that $g \in x^G$ lies in some $M(l)$ is $1-\prod_{p\mid n}(1-1/p)+O(1/n)$.

If q is odd, or if x moves at least 8 points, the result follows from (iii)–(v). If $x = (1,2)(3,4)$, the result follows from (ii). Finally, if $x = (1,2)(3,4)(5,6)$ then $\mu(x, \Pi(l)) = \binom{l}{3}\binom{k}{2}^3/[\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}/3!] + l(l-1)[\binom{k}{2}\binom{k-2}{2}/2]\binom{k}{2}/[\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}/3!] + l[\binom{k}{2}\binom{k-2}{2}\binom{k-4}{2}/3!]/[\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}/3!]$, with terms corresponding to the partitions (2, 2, 2), (4, 2), (6) of 6 (recall that $k \geq 6$). As in (ii) we obtain

$$\begin{aligned}\Pr\{g \text{ is in some } M(l) \mid g \in (1,2)(3,4)(5,6)^{S_n}\}\\ = 1 - \prod_{p \mid n}(1 - 1/p^3) + O(1/n),\end{aligned}$$

which implies the result in (vii). ∎

PROPOSITION 7.6. (i) $\liminf \mathrm{PC}(A_{2l+1}) = 8/\pi^2 \approx 0.811$;

(ii) $\lim_{\rho(n)\to\infty} \mathrm{PC}(A_n) = 1$;

(iii) $\limsup \mathrm{PC}(A_{n_i}) \leq 1 - 1/\sup \rho(n_i)^2 < 1$ *for any sequence* (n_i) *such that* $\rho(n_i)$ *remains bounded*; *and*

(iv) $\limsup_{\{n \mid \rho(n) = p\}} \mathrm{PC}(A_n) = 1 - 1/p^2$ *for any prime* p.

Proof. Let $G = A_n$. We may assume that $n > 23$, and by (7.2) we may assume that n is odd. Let $C_G = c_n^G$. Then $\mathscr{M}(c_n)$ consists of some of the following groups M in very familiar permutation representations:

(a) $M(l)$ whenever $l \mid n$, $1 < l < n$;

(b) $M = \mathrm{P\Gamma L}(d,q) \cap G$ if n has the form $(q^d - 1)/(q-1)$ for some prime power q and some integer $d \geq 2$;

(c) $\mathrm{N}_G(\langle c_n \rangle)$ and n is prime.

In order to see that this list is complete, note that (a) handles the imprimitive case. By classical results of Burnside and Schur [Wie, p. 65], any maximal overgroup M that is primitive is either a regular or Frobenius group of prime degree or is 2-transitive. In the latter case the classification of finite simple groups produces the desired conclusion (b) [Fe, 4.1].

In case (a) the description given for M shows that $\langle c_n \rangle$ is in a unique subgroup of that type whenever $l \mid n$. This same uniqueness statement obviously holds for (c). In (b), $\langle c_n \rangle^G \cap M$ is a conjugacy class within M; in view of the action of $\mathrm{N}_G(\langle c_n \rangle)$ there are $O(n)$ overgroups of $\langle c_n \rangle$ of this sort for a given d (cf. (2.5)), and hence a total of $O(n \log n)$ such subgroups.

(a) By (7.5)(vi),

$$\Pr\{g \text{ is in some } M(l) \mid g \in x^G\} \leq 1 - \prod_{p \mid n}(1 - 1/p^2) + O(1/n) \quad (7.7)$$

whenever $1 \neq g \in G$.

(b) If g has k fixed points and t cycles of length p, then $n = k + pt$ and $|\mathrm{C}_G(g)| = k!p^t t!/2$. Since $g \in M \leq \mathrm{P\Gamma L}(d, q)$ and n is odd, $k \leq (n-1)/2$. Also, $|\mathrm{N}_G(M) : \mathrm{N}_G(\langle c_n \rangle)| \leq (n-1)/d$. In view of (2.1), (2.2), and (2.4), it follows that the contribution in (b) is

$$\begin{aligned}
&\leq [(n-1)/d]|M|/|g^G| \\
&< nq^{d^2}k!p^{n/p}t!/n! \\
&< n^{3+\log_2 n}k!(3^{1/3})^n[(n-k)/2]!/n! \\
&= n^{3+\log_2 n}(3^{1/3})^n[(n-k)/2]!/\{n \cdots (k+1+[(n-k)/2]) \\
&\qquad\qquad \cdot(k+[(n-k)/2]) \cdots (k+1)\} \\
&< n^{3+\log_2 n}(3^{1/3})^n/([(n-k)/2]+k+1)^{n-([(n-k)/2]+k+1)+1} \\
&< n^{3+\log_2 n}(3^{1/3})^n/(n/2)^{(n+1)/4}.
\end{aligned}$$

(c) By (2.1), $\mu(g, M^G) < \{n(n-1)\}/|G : \mathrm{C}_G(g)|$. For $g \in M$, $|\mathrm{C}_G(g)| \leq 2^{(n-1)/2}\{(n-1)/2\}!/2$, so that

$$\begin{aligned}
\mu(g, M^G) &< \{n(n-1)\}2^{(n-1)/2}\{(n-1)/2\}!/n! \\
&\leq 2^{(n-1)/2}/\{(n+1)/2\}^{(n-3)/2}.
\end{aligned}$$

In particular, $\mu(g, M^G) = O(1/n^3)$ in (b) and (c) and the total contribution for any element from all such subgroups is at most $O(1/n)$. If n is prime, then case (a) cannot occur whence $\mathrm{PC}(A_n) = O(1/n)$ and the theorem follows. So we may assume that n is not prime.

Completion of the Proof of (7.6). By (7.2)(i), if at least two cycles must be used in an (asymptotically) optimal s then the best we can hope for $\mathrm{PC}(A_{2l+1})$ is that it is $3/4 + O(1/(2l+1))$. Hence we must consider whether we can do better using an n-cycle $s = c_n$.

In that case we saw that the contributions of (b) and (c) to $P_s(g)$ are $O(1/n)$, while the contribution of (a) is bounded in (7.7); this bound can be attained, by (7.5(i), (ii)). Clearly $\prod_{p|n}(1 - 1/p^2) \geq \prod_{p>2}(1 - 1/p^2)$. If p runs over *all* primes then $\prod_p(1 - 1/p^2)^{-1} = \prod_p \sum_i (1/p^2)^i = \sum_1^\infty 1/n^2 = \pi^2/6$, so that $\prod_{p>2}(1 - 1/p^2) = (1 - 1/2^2)^{-1}(6/\pi^2) \approx 0.811 > 3/4$. It follows that n-cycles are optimal, that

$$\mathrm{PC}(A_n) = \prod_{p|n}(1 - 1/p^2) + O(1/n)$$

for any n, and that $\prod_{p>2}(1 - 1/p^2)$ is the smallest limit point of $(\mathrm{PC}(A_{2l+1}))$. This proves (i).

We also see that

$$\mathrm{PC}(A_n) \geq \prod_{p \geq \rho(n)} (1 - 1/p^2) + O(1/n) > 1 - \sum_{r=\rho(n)}^{\infty} r^{-2} + O(1/n),$$

which implies (ii).

On the other hand, for any sequence (n_i) as in (iii) we have $\mathrm{PC}(A_n) \leq 1 - 1/\rho(n)^2 + O(1/n)$, so that (iii) holds. Finally, if we fix $p = \rho(n)$ and let p_i be an increasing sequence of primes, then we see that $\lim \mathrm{PC}(A_{pp_i}) = 1 - 1/p^2$, yielding (iv). ▮

PROPOSITION 7.8.

(i) $\lim \mathrm{PC}(S_{2l}) = 1/2$.

(ii) $\liminf_{\rho(n)=p} \mathrm{PC}(S_n) = \liminf \mathrm{PC}(S_n) = 1/2$ *for any prime* p.

(iii) $\lim_{n \text{ prime}} \mathrm{PC}(S_n) = 1$.

Proof. First consider $s \in S_n$ having more than one cycle. Since we may assume that s and a transposition can generate S_n, s has two cycles. As in (7.2ii) we have $P_s(c_2) \geq 1/2 + O(1/n)$. Moreover, this bound is attainable for suitable s: as in the proof of (7.1) let s be the product of cycles of length l and $l+1$ if $n = 2l+1$, or of length $l \pm (2, l-1)$ if $n = 2l$. Since these cycle lengths are relatively prime, the argument in (7.2ii) yields $P_s(g) \leq P_s(c_2) = 1/2 + O(1/n)$ whenever $1 \neq g \in S_n$.

Now let $s = c_n$. As in the proof of (7.6), we still have cases (a–c) and (b) and (c) contribute negligibly to $P_{c_n}(g)$. Then, as in the proof of (7.6), we see that (7.5vii) yields

$$\mathrm{PC}(S_n) = \max\left\{1/2 + O(1/n),\ \prod_{p|n} (1 - 1/p) + O(1/n)\right\}.$$

(i) Here $1/2 \geq \prod_{p|n}(1 - 1/p)$, so that $\mathrm{PC}(S_n) = 1/2 + O(1/n)$ and $\lim \mathrm{PC}(S_{2l}) = 1/2$.

(ii) The above product can be made arbitrarily small, so that the $1/2$ term again dominates for infinitely many n.

(iii) This is now clear. ▮

This completes the proof of Theorems I *and* II.

Remarks. (1) For symmetric groups we get an entirely different result $\liminf \mathrm{PC}^{\#}(S_n) = 0$ using $\mathrm{PC}^{\#}(S_n) = \max_{1 \neq s \in S_n} \min_{1 \neq g \in S_n} \Pr\{\langle g, s' \rangle = S_n \mid s' \in s^G\}$. For, if s achieves $\mathrm{PC}^{\#}(S_n)$ then it must be an odd permutation having at most two cycles.

If n is even then s must be an n-cycle, and hence our previous estimates yield $\mathrm{PC}^{\#}(S_{2l}) = \prod_{p \mid n}(1 - 1/p) + O(1/n)$. This produces the stated lim inf.

On the other hand, if n is odd then s cannot be a cycle, so that we are in a situation similar to those in (7.1), (7.2), and (7.8): $\liminf \mathrm{PC}^{\#}(S_{2l+1}) = 1/2$.

(2) We have determined $\mathrm{PC}(S_n)$ for all large n, and we saw that $\lim \mathrm{PC}(S_{2l}) = 1/2$. Moreover, we saw that, for infinitely many l, we cannot use a $2l$-cycle for s when computing $\mathrm{PC}(S_{2l})$.

The situation for odd n is very different. Let (p_i) be the increasing sequence of all odd primes. For any subsequence (p_{i_j}) note that $\max\{1/2, \prod_j(1 - 1/p_{i_j})\}$ is a limit point of $(\mathrm{PC}(S_n))$. For any real number $\alpha \in [1/2, 1)$, choose p_{i_1} such that $1 - 1/p_{i_1} > \alpha$, and recursively choose $i_k > i_{k-1}$ minimal subject to $\prod_1^k(1 - 1/p_{i_j}) > \alpha$, in order to see that *the set of limit points of* $(\mathrm{PC}(S_{2l+1}))$ is $[1/2, 1]$.

8. FURTHER RESULTS AND REMARKS

(1) As we noted in Remark 1 at the end of the previous section, it is not possible to extend these results to almost simple groups by trying to require that $\langle g, s' \rangle = G$ provided that G is generated by two elements. Nevertheless, if G is almost simple with socle S such that G/S is cyclic one may ask whether, for each nontrivial $g \in G$, there exists an $x \in G$ with $G = \langle g, x \rangle$. This does hold for $G = S_n$ by the methods of the previous section. Our methods yield affirmative answers in many but not all cases.

(2) L. Pyber asked the following question: Can every finite nonabelian simple group be generated by two subgroups of odd order? A minor variation of our results yields the following result, which is somewhat stronger than Pyber needed:

THEOREM 8.1. *Every finite nonabelian simple group can be generated by a pair of elements of odd order.*

Proof. Our previous argument shows that a sporadic, alternating or Lie type group in characteristic 2 can be generated by a pair of elements of odd order. It remains to consider the case in which our group G is a simple group of Lie type over a field of odd characteristic. In the previous argument, replace the element s by s^e with e a power of 2 so that s^e has odd order. Let t be a long root element (which has odd order).

We claim that G is generated by s^e and a conjugate of t. For, consider the family $\mathscr{M}$ of maximal overgroups of s^e that contain long root elements.

Using [GPPS, Co, Ka1], we see that $\mathscr{M}$ is a subset of the set of maximal overgroups of G containing s. Using fixed point ratios as in the proof of Theorem I, we find that the union of the subgroups in $\mathscr{M}$ does not contain all long root elements (or alternatively, when $|\mathscr{M}| \leq 2$ we can apply [G2, 2.2]). ▮

(3) We note some conjectures related to Theorem II. Let G be a finite simple group.

(a) Let $1 \neq s \in G$. Let $P_s(G)$ denote the probability that if x is chosen randomly in G, then $G \neq \langle s, x \rangle$. Clearly $P_s(G) < 1$ for all s, G by Theorem I; and our results show that if $G = A_n$ and s is a 3-cycle, then there exists no constant $c < 1$ so that $P_s(G) < c$ for all n.

Show that such a constant $c < 1$ exists for G a finite group of Lie type; determine the best possible c (for $|G|$ sufficiently large). Note that we must have $c > 1/2$ (by considering $G = \mathrm{Sp}(2m, 2)$). This question is closely related to a question left open in [GKS]: determine the limit points of $\{\min_{1 \neq g \in G} \Pr\{\langle g, h \rangle = G \mid h \in G\} \mid G$ is a finite simple group$\}$.

(b) Let p and q be primes dividing $|G|$ such that $pq > 6$. Show that the probability that two random elements of orders p and q generate G tends to 1 as $|G|$ tends to infinity (or at least prove that this probability is bounded away from 0). See [LiSh1, LM] when $pq = 6$.

(c) Prove that there exists an element $s = s_G$ such that, for any nontrivial $x \in G$ (or $\mathrm{Aut}\, G$), if y is a random element of x^G, then the probability that s and s^y generate G is bounded away from 0. Presumably, one can choose precisely the same s as in our proof.

(4) It is clear from our approach that there is a need for more uniform and precise estimates concerning $\mu(G, \mathbf{X})$ when G has Lie type and $\mathbf{X}$ is a naturally occurring conjugacy class of subgroups. Such uniform estimates would make the proof of Theorem II easier. On the other hand, it is less clear that suitably precise *general* estimates can be obtained that imply Theorem I (even with a smaller constant than our $1/10$).

Examples of $\mathbf{X}$ are any classical group acting on a conjugacy class of maximal tori (in particular, on cyclic groups generated by irreducible Singer cycles, when they exist); orthogonal or symplectic groups acting on the naturally embedded irreducible unitary subgroups; and all classical groups acting on a conjugacy class of subgroups of the same type over extension fields. In general, it would be desirable to have bounds for all of the standard Aschbacher classes [KlL]. Most desirable would be bounds that made all of our special considerations in Sections 4, 5, and 6 unnecessary.

(5) One minor obstacle in our proof was that there is presently no classification of all overgroups of Singer cycles of a subgroup $\mathrm{SL}(m, q)$

inside $\Omega^+(2m, q)$ or of a subgroup $\mathrm{SL}(m, q^2)$ inside $\mathrm{SU}(2m, q)$. Such a classification would be desirable both for group-theoretic and geometric purposes.

(6) What are the "best" types of classes C_G in our theorems? The flexibility of our choice of s shows that there are many classes producing our bounds.

Better estimates should be possible: it would be interesting to have precise error terms for all of our bounds, along the lines of those in [Ba, Ka2, LiSh2]. Presumably exact error terms arise using irreducible elements when these exist in a classical group G.

(7) The classification of simple groups was used here rather heavily. We do not know how to avoid this (since, for example, there is no known bound on the number of generators required for a simple group without the classification). Nevertheless, Theorem I for classical groups was originally proved (with a poorer constant) using much more elementary group theory: $s \in C_G$ was the commuting product of a (long) root element and an irreducible or almost irreducible element, so [Ka1] could be used. One can prove a similar result for exceptional groups using [Co]. The asymptotic result for exceptional groups can also be proved without the classification.

(8) Combining our fixed point results together with those of [LiSh3] yields the following result:

THEOREM 8.2. *Let G be an almost simple group of Lie type defined over $\mathbb{F}_q$ with socle S. Given $\epsilon > 0$ and a primitive G-set Ω with $\mu(G, \Omega) > \epsilon$, there exist constants N, Q, and K (each depending upon ϵ) so that one of the following holds*:

(i) $|G| < N$;

(ii) *$q < Q$, G is a classical group, and Ω is a set of k-spaces for $k < K$; or*

(iii) *$S = \mathrm{PSL}(n, q)$ with $q < Q$, $k < K$, and Ω is either the set of complementary pairs of k and $n - k$ spaces or the set of flags of type k, $n - k$.*

One can give estimates for N, Q, and K.

(9) The *spread* of a finite group G is the largest non-negative integer t such that, if $x_1, \dots, x_t$ are nontrivial elements of G, then there exists $y \in G$ so that $G = \langle x_i, y\rangle$ for *each* i. The corollary in Section 1 asserts that the spread of a finite simple group is at least 1. Indeed, our asymptotic results show that, aside from finitely many possibilities and the groups $\Omega(2m + 1, 2)$, the spread is at least 2. In this last situation, the argument of the paper easily shows that the spread is at least 2 unless possibly we are considering 2 transvections x_1, x_2. In this case, we can take y to be an element of order $2^m + 1$—see [GS] for details. This combined with the

more precise version of Theorem II (stated in Section 1 after the theorem) can be used to show:

THEOREM 8.3. *There are only finitely many simple groups with spread less than* 2.

We conjecture that in fact the spread of any finite simple group is at least 2; this would be a much stronger result than the corollary in Section 1. The remarks after Theorem II can be used easily to show that, if (G_i) is a sequence of pairwise nonisomorphic simple groups, then the spread of G_i tends to infinity unless there is a subsequence of (G_i) consisting either of odd-dimensional orthogonal groups over a fixed field or of alternating groups of degree mp for varying m and some fixed prime p. In those cases, the spread will not tend to infinity (see [GS]). However, as we have already remarked, our results can easily be used to show that for most families the spread tends to infinity.

REFERENCES

[As] M. Aschbacher, Maximal subgroups of E_6, preprint.

[Ba] L. Babai, The probability of generating the symmetric group, *J. Combin. Theory Ser. A* **52** (1989), 148–153.

[Bu] G. Butler, The maximal subgroups of the Chevalley group $G_2(4)$, *in* “Groups—St. Andrews, 1981” (C. M. Campbell and E. F. Robertson, Eds.), London Math. Soc. Lecture Note Ser., Vol. 71, pp. 186–200, Cambridge Univ. Press, Cambridge, UK, 1982.

[CLSS] A. M. Cohen, M. W. Liebeck, J. Saxl, and G. M. Seitz, The local maximal subgroups of exceptional groups of Lie type, finite and algebraic, *Proc. London Math. Soc.* **64** (1992), 21–48.

[CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, “Atlas of Finite Groups,” Clarendon, Oxford 1985.

[Co] B. N. Cooperstein, Subgroups of exceptional groups of Lie type generated by long root elements, I, II, *J. Algebra* **70** (1981), 270–282, 283–298.

[DT] L. DiMartino and C. Tamburini, 2-generation of finite simple groups and some related topics, *in* “Generators and Relations in Groups and Geometries” (A. Barlotti *et al.*, Eds.), pp. 195–233, Kluwer Academic, Dordrecht, 1991.

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

[Fe] W. Feit, Some consequences of the classification of finite simple groups, *in* Proc. Sympos. Pure Math., Vol. 37, pp. 175–181, Amer. Math. Soc., Providence, 1980.

[GL] D. Gorenstein and R. Lyons, The local structure of finite groups of characteristic 2-type, *Mem. Amer. Math. Soc.* **42**, No. 276 (1983).

[G1] R. M. Guralnick, Generation of simple groups, *J. Algebra* **103** (1986), 381–401.

[G2] R. M. Guralnick, Some applications of subgroup structure to probabilistic generation and covers of curves, *in* “Algebraic Groups and Their Representations” (R. W. Carter and J. Saxl, Eds.), pp. 304–319, Kluwer Academic, Dordrecht, 1998.

[GH] R. M. Guralnick and C. Hoffman, The first cohomology group and generation of simple groups, *in* "Groups and Geometries, Siena, 1996" (L. DiMartino and W. M. Kantor, Eds.), pp. 81–89, Trends Math., Birkhäuser, Basel, 1998.

[GKS] R. M. Guralnick, W. M. Kantor, and J. Saxl, The probability of generating a classical group, *Comm. Algebra* **22** (1994), 1395–1402.

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

[GPPS] R. M. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl, Linear groups with orders having certain primitive prime divisors, *Proc. London Math. Soc.* **78** (1999), 167–214.

[GS] R. M. Guralnick and A. Shalev, On the spread of finite simple groups, preprint.

[JLPW] C. Jansen, K. Lux, R. Parker, and R. A. Wilson, "An Atlas of Brauer Characters," Oxford Univ. Press, Oxford, 1995.

[JP] W. Jones and B. Parshall, On the 1-cohomology of finite groups of Lie type, *in* "Proceedings, Conference on Finite Groups, Park City, Utah, 1975," pp. 313–328, Academic Press, New York, 1976.

[Ka1] W. M. Kantor, Subgroups of classical groups generated by long root elements, *Trans. Amer. Math. Soc.* **248** (1979), 347–379.

[Ka2] W. M. Kantor, Some topics in asymptotic group theory, *in* "Groups, Combinatorics and Geometry" (M. W. Liebeck and J. Saxl, Eds.), London Math. Soc. Lecture Note Ser., Vol. 165, pp. 403–421, Cambridge Univ. Press, Cambridge, UK, 1992.

[Ka3] W. M. Kantor, Finite geometry for a generation, *Bull. Belg. Math. Soc.* **3** (1994), 423–426.

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

[Kl] P. B. Kleidman, The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$ and their automorphism groups, *J. Algebra* **117** (1988), 30–71.

[KlL] P. B. Kleidman and M. W. Liebeck, The subgroup structure of the finite classical groups, London Math. Soc. Lecture Note Ser., Vol. 129, Cambridge Univ. Press, Cambridge, UK, 1990.

[LiSa] M. W. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of Riemann surfaces, *Proc. London Math. Soc.* **63** (1991), 266–314.

[LSS] M. W. Liebeck, J. Saxl, and G. M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. London Math. Soc.* **65** (1992), 297–325.

[LiSe] M. W. Liebeck and Seitz, Reductive subgroups of exceptional algebraic groups, *Mem. Amer. Math. Soc.* **580** (1996).

[LiSh1] M. W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the $(2,3)$-generation problem, *Ann. of Math.* **144** (1996), 77–125.

[LiSh2] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113.

[LiSh3] M. W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520.

[LM] F. Lübeck and G. Malle, $(2,3)$-generation of exceptional groups, *J. London Math. Soc.* **59** (1999), 109–122.

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

[M] G. Malle, Exceptional groups of Lie type as Galois groups, *J. Reine Angew. Math.* **392** (1988), 70–109.

[MSW] G. Malle, J. Saxl, and T. Weigel, Generation of classical groups, *Geom. Dedicata* **49** (1994), 85–116.

[NW] S. Norton and R. Wilson, The maximal subgroups of $F_4(2)$ and its automorphism group, *Comm. Algebra* **17** (1989), 2809–2824.

[Pu] C. Purvis, "Finite Classical Groups of Genus Zero," Ph.D. Thesis, Imperial College, University of London, 1995.

[Sc] M. Schönert *et al.*, "GAP, Groups, Algorithms and Programming," 4th ed., Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1995.

[Sh] T. Shih, "Bounds of Fixed Points Ratios of Permutation Representations of $GL_n(q)$ and Groups of Genus Zero," Ph.D. Thesis, California Institute of Technology, 1991.

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

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

[We] T. S. Weigel, Generation of exceptional groups of Lie type, *Geom. Dedicata* **41** (1992), 63–87.

[Wie] H. Wielandt, "Finite Permutation Groups," Academic Press, New York, 1964.

[Wo] A. J. Woldar, $3/2$-generation of the sporadic simple groups, *Comm. Algebra* **22** (1994), 675–685.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.