Probabilistic generation of finite simple groups

Robert M. Guralnick* and William M. Kantor*

ABSTRACT

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.

1. Introduction

For any finite group G, let $\mathrm{PC}(G)$ denote the following probability:

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

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 G together with any given nontrivial $g\in G$. We will prove the following two theorems.

Theorem I. *For every finite simple group G, $\mathrm{PC}(G)>1/10$.*

Theorem II. (a) $\liminf\{\mathrm{PC}(G)\mid G \textit{ is simple}\}=1/2$.
(b) *If (G_i) is any sequence of pairwise nonisomorphic finite simple groups, then $\lim\mathrm{PC}(G_i)=1$ unless (G_i) contains a subsequence of one of the following sorts:*
- *(A_{2m_j}), in which case $\lim\mathrm{PC}(A_{2m_j})=3/4$;*
- *(A_{p_jm}) for primes $p_j\not|\, m$ and a fixed odd integer $m>1$, in which case $\lim\mathrm{PC}(A_{p_jm})=1-1/m^2$; or*
- *$(\Omega(2m_j+1,q))$ for a fixed prime power q, in which case $\lim\mathrm{PC}(\Omega(2m_j+1,q))=1-1/q$.*

In the last part of Theorem II, q is allowed to be even; and in fact, the theorem states that the groups $\Omega(2m+1,2)\cong\mathrm{Sp}(2m,2)$ are "worst" from our PC point of view. These theorems relate to various known results of a similar flavor. In [Di,KaLu] it was shown that a random pair of elements of a finite simple alternating or classical group G generates G with probability approaching 1 as $|G|\to\infty$; the same was proved in [LiSh2] for the exceptional groups of Lie type. In [GKS] it was shown that $\min\limits_{1\neq g\in G}\Pr\{h\in G:\langle g,h\rangle=G\}$ does *not* approach 1 as $|G|\to\infty$, where G ranges through all alternating groups, or through all simple classical groups over a given field (but this minimum does approach 1 if G ranges over all classical simple groups of a given dimension). Thus, it is natural to introduce some way to restrict the choices of elements of G; we do this by using conjugacy classes. For any $a,b\in G$ write $P_a(b)=\Pr\{a'\in a^G:\langle a',b\rangle\neq G\}$; note that $P_a(b)=P_b(a)=\Pr\{a'\in a^G,b'\in b^G:\langle a',b'\rangle\neq G\}$. Then $\mathrm{PC}(G)=\max\limits_{1\neq s\in G}\min\limits_{1\neq g\in G}(1-P_s(g))$. Thus, we focus on estimating $P_s(g)$ for carefully chosen s and all $g\neq 1$. We will see that an "asymptotically optimal" class $C_G=s^G$ is not at all uniquely determined by G. Note that the theorems do not contain the results in [Di,KaLu,LiSh2].

Theorem I implies, in particular, the following property of simple groups, called "$1\frac{1}{2}$ generation" (cf. [DT, Wo]):

Corollary. *Any nontrivial element of a finite simple group G belongs to a pair of generators of G.*

This can be proved using less effort than we employ here for Theorem I.

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

* This research was supported in part by the NSF.

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. This is why $P_a(b)$ was introduced; cf. (2.2).

2. Fixed point ratios; notation

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*

$$\mu(g, \mathbf{X}) = |\mathrm{Fix}_{\mathbf{X}}(g)|/|\mathbf{X}| \quad \text{and} \quad \mu(G, \mathbf{X}) = \min\{\mu(g, \mathbf{X}) \mid g \in G,\ g \neq 1 \text{ on } \mathbf{X}\}.$$

These are related to $\mathrm{PC}(G)$ as follows. Let $s \in G$ be such that its conjugacy class s^G generates G. If $g \in G - Z(G)$, then $P_s(g) = P_g(s) \leq \sum_{M \in \mathcal{M}(s)} |g^G \cap M|/|g^G|$, where $\mathcal{M}(s)$ is the set of all maximal subgroups M of G containing s (the maximal *overgroups* of s). If M^G denotes the conjugacy class of M, then

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

In particular,

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

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 $\mathcal{M}(s)$.

For any group G, let $\mu(G) = \max\{\mu(G, \mathbf{X}) \mid G \text{ is nontrivial and primitive on } \mathbf{X}\}$. 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 is a simple group of Lie type over* $\mathrm{GF}(q)$*, and $S \leq G \leq \mathrm{Aut}S$. Assume that S is not isomorphic to any 2–dimensional linear group, and that $S \ncong \mathrm{PSp}(4,3)$. Then $\mu(G, M^G) \leq 4/3q$ for any maximal subgroup M of G.*

In order to use this for Theorem II we merely need to choose s so that $|\mathcal{M}(s)|$ stays bounded as $q \to \infty$. The next section provides some more precise bounds for classical groups in natural permutation actions. For exceptional groups G of Lie type we will use the more precise bounds for $\mu(G)$ in [FM1,FM2].

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 $|N_G(A){:}\, N_B(A)|/|N_G(B){:}\, B|$ conjugates of B.*

3. Some fixed point ratios for classical groups

Let G be a classical (linear) group defined on a d–dimensional vector space V over $\mathrm{GF}(q)$ (or $\mathrm{GF}(q^2)$ in the unitary case). In each case we need to consider the number of fixed points of an r-element g whose order modulo scalars is the prime r. Write $C = \mathrm{C}_V(g)$.

In this section we will provide bounds on $\mu(g, M^G)$ for various subgroups M of a classical group G. When $G = \mathrm{PSL}(d,q)$ stronger unpublished results are known [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 $G = \mathrm{SL}(V) = \mathrm{SL}(d,q)$, and let $\mathbf{S}_k$ denote the set of all k–spaces of V, where $1 \leq k \leq d/2$. 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 is either semisimple or unipotent. There are three cases to consider:

Case A. *g is semisimple and acts homogeneously on V* with each irreducible submodule of dimension e with $1 < e|k$ and $k|d$.

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

Case C. *g is unipotent.*

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

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

Proof. Since $\mathrm{Fix}_{\mathbf{S}_k}(x)$ can be viewed as the set of k/e–spaces of a d/e–dimensional $\mathrm{GF}(q^e)$–space,

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

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 $\mu(g, \mathbf{S}_k) < 1/q^k$ for $k \le 2$.*

Proof. Note that $\mathrm{Fix}_{\mathbf{S}_k}(g)$ is contained the set Γ of k–spaces which are of the form $X_1 \oplus X_2$ with $X_i \subseteq V_i$. Here, Γ has size

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

Thus, we may apply Lemma 3.6 below in order to conclude that (a) and (b) hold.

If $q = 2$ and $k \le 2$, then (c) follows easily after noting that g cannot as a scalar on both V_1 and V_2. $\square$

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 that intersect W in 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 $\dim \mathrm{C}_{V/J}(g) = (d-j) - \dim[V/C, g] = (d-j)-(e-j) = d-e$. Thus, J produces at most $\begin{bmatrix} d-e \\ k-j \end{bmatrix}$ 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 $\begin{bmatrix} e \\ j \end{bmatrix}\begin{bmatrix} d-e \\ k-j \end{bmatrix}$. 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 Lemma 3.6 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). $\square$

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 3.6. (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 $\mathrm{GF}(q)$–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 a $X_i \subseteq V_i$ and $\dim X_1 + \dim X_2 = k$.

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

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

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

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

Consequently, for the remainder of the proof, assume that

$$k \geq 2;\ \textit{if}\ e = 2\ \textit{then}\ d > 2k. \tag{3.7}$$

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 $\tau(W_1, W_2) = (\varphi_1(W_1), \varphi_2(W_2))$. We claim that

$$|\tau^{-1}(X_1, X_2)| > q^k\ \textit{for each}\ (X_1, X_2) \in \Gamma, \tag{3.8}$$

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 (3.8):

$$|\varphi_i^{-1}(X_1, X_2)| \geq q^k\ \textit{for}\ i = 1\ \textit{or}\ 2. \tag{3.9}$$

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 (3.9) holds. We now assume that $0 < j < k$, and divide the remainder of the proof of (3.9) 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 (3.7).

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 (3.7).

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 (3.7), 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 (3.7), we have $j(d - e - k + j) \geq j(e - k + j) \geq j(k/2) \geq k$. □

3.2. The remaining classical groups

Let G be a classical group on a d–dimensional vector space V of Witt index $m \geq 2$ over the field $\mathbb{F} = \mathrm{GF}(q^e)$ (or $\mathrm{GF}(q^2)$ in the unitary case). We will need to consider the action of G 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.) Let $\mathbf{TS}_k$ and $\mathbf{NS}_k$ denote G–orbits of totally singular and nonsingular k–spaces, respectively (there are two orbits of totally singular m–spaces when $G = \Omega^+(2m, q)$; in this paper "nonsingular" subspaces are those having 0 radical.).

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, we will be somewhat careful in this section about bounds—leading to relatively ugly-looking estimates. In this direction, we introduce additional parameters $m^{\#}, m^*$ for G, as follows

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

Note that $m^{\#} \geq m-1$. If x is any singular 1–space, then $x^\perp/x$ has exactly $|\mathbf{TS}_m|/(q^{m^{\#}}+1)$ totally singular $m-1$–spaces. The meaning of m^* will appear within the proof of (3.10). 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 maximal totally singular subspace W, where $\mathrm{dim}W = m \geq 2$. Then Q has the following structure, with each indicated module a natural one for $\mathrm{GL}(W)$, where in some cases we also use a $\mathrm{GL}(W)$–invariant subgroup Z of Q:

$\mathrm{Sp}(2m,q)$ Q can be viewed as the space $S^2(W)$ of symmetric 2–tensors. This is a reducible $\mathrm{GL}(W)$–module if q is even, in which case $\mathrm{Sp}(2m,q)$ is better viewed as $\Omega(2m+1,q)$).

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

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

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

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

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

For subspaces A and B of W let $A \bigstar B$ denote the subspace spanned by all of the vectors $a \bigstar b$ for $a \in A$, $b \in B$, where $\bigstar \in \{\wedge, \blacktriangle\}$; and in the symplectic case, let $A \odot B$ denote the subspace spanned by all of the vectors $a \otimes b + b \otimes a$ and $c \otimes c$ for $a \in A$, $b \in B$, $c \in A \cap B$.

Lemma 3.10. *If g acts nontrivially on the above 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 $h \neq 1$.

First consider the case that h is unipotent. Let X be any h–invariant 2–space of W on which h is nontrivial, and let $X = X_2 \subset X_3 \subset \cdots \subset X_m = W$ be an h–invariant sequence of subspaces with $\mathrm{dim}X_i = i$. Then, for $\bigstar \in \{\wedge, \blacktriangle, \odot\}$, h acts nontrivially on each of the 2–spaces $(X_{i+1} \bigstar X)/(X_i \bigstar X)$, $i = 2, \ldots, m-1$. It follows that $\mathrm{dimC}_{W \bigstar W}(h) \leq \mathrm{dim}(W \bigstar W) - (m-2)$.

When h is semisimple we will prove that $\mathrm{dimC}_{W \bigstar W}(h) \leq \mathrm{dim}(W \bigstar W) - (m-2)$ also holds. Suppose that the eigenvalues of h (over the algebraic closure) on W are $a_1, \ldots, a_m$. Then $\mathrm{dimC}_{W \bigstar W}(h)$ is the number of ordered pairs (i,j) such that

(i) $a_i a_j = 1$ for $i < j$ if $\bigstar = \wedge$;
(ii) $a_i a_j = 1$ for $i \leq j$ if $\bigstar = \odot$ (in odd characteristic); or
(iii) $a_i \bar{a}_j = 1$ for $i \leq j$ if $\bigstar = \blacktriangle$.

It follows easily that $\mathrm{dimC}_{W \bigstar W}(h)$ is largest when h has only 2 distinct eigenvalues. A straightforward computation yields the bound.

When G is $\mathrm{SU}(2m+1,q)$, $\Omega(2m+1,q)$ or $\Omega^-(2m+2,q)$, Q has an additional $\mathrm{GL}(W)$–composition factor, isomorphic to W. Here $\mathrm{dimC}_W(h) \leq \mathrm{dim}W - 1 = m^*$. Then $|\mathrm{C}_Q(h)| \leq |\mathbb{F}|^{\mathrm{dim}C_{W \bigstar W}(h) + \mathrm{dim}C_W(h)}$ implies the stated inequality. □

Remark. In fact, $\mathrm{dimC}_W(h) \leq \mathrm{dim}W - 2$ for those orthogonal groups in which h cannot induce a transvection on W, leading to a slightly better bound.

Lemma 3.11. *$\mu(G, \mathbf{TS}_m) < 2/|\mathbb{F}|^{m^*} + 1/|\mathbb{F}|^{m^{\#}} \leq 5/2|\mathbb{F}|^{m^*}$ if $m \geq 3$.*

Proof. Let $g \in G$ act nontrivially on $\mathbf{TS}_m$. Write $C = \mathrm{C}_V(g)$. We consider 2 cases separately. Note that the two cases overlap but contain all possibilities.

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 and that there are no $\langle g \rangle$–homomorphisms from V_1 to V_2, and that V_1 has dimension k which is at least as large as dimV_2. Note that in particular this holds if $\mathrm{C}_V(g) \neq 0$ (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 $\mathrm{Fix}_g(\mathbf{TS}_m)$ is bounded above by the number of maximal totally singular subspaces of a nonsingular subspace of dimension $k-1$ or twice the number of maximal totally singular subspaces of a nonsingular space of dimension $k-2$. If $k-1$ can occur here 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 $(X \cap V_1)^\perp = X \cap V_2$. 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 an element of $\mathbf{TS}_m$. If every g–invariant element of $\mathbf{TS}_m$ lies in C, then rad$C \neq 0$, and $|\mathrm{Fix}_{\mathbf{TS}_m}(g)|$ is at most the number of maximal totally singular subspaces of $x^\perp/x$ for a 1–space x of rad$C$, and hence is at most $|\mathbf{TS}_m|/(|F|^{m^\#} + 1)$. Hence, we will assume that g acts nontrivially on our g–invariant $W \in \mathbf{TS}_m$. Let $S_m(i)$ denote the set of members of $\mathbf{TS}_m$ intersecting W in 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 (3.10), 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 $S_m(i)$, $0 < i < m$. 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 $I^\perp/I$. *Assuming* that g is nontrivial on W/I, we can again use (3.10): g fixes at most $|S_m(i)|/|\mathbb{F}|^{m^*-i}$ members of $S_m(i)$ (note that W/I must have dimension at least 2 and so the Witt index of $I^\perp/I$ is at least 2). 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 $U \in \ TS_m$ such that x is nontrivial on $W/(U \cap W)$ is less than $\sum_0^m (2|\mathbf{S}_i(W)|/|\mathbb{F}|^i)(|S_m(i)|/|\mathbb{F}|^{m^*-i}) = 2|\mathbf{TS}_m|/|\mathbb{F}|^{m^*}$.

We have not accounted for those $U \in \mathbf{TS}_m$ such that g is trivial on W/I, i.e., such that $[g, W] \subseteq U$. This possibility only occurs for g unipotent. The number of totally singular m–spaces 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 $\mathbf{TS}_m$. □

Proposition 3.12. $\mu(G, \mathbf{TS}_k) < 2/|\mathbb{F}|^{m^*} + 1/q^{m^\#} + 1/|\mathbb{F}|^k$ *whenever* $1 \leq k \leq m$ *and* $m \geq 3$.

Proof. Let $g \in G$ act nontrivially on $\mathbf{TS}_k$. By the preceding lemma we may assume that $k \leq m-1$. 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 $U \neq U^g$, and then choose one of at least $\begin{bmatrix} m \\ k \end{bmatrix} - \begin{bmatrix} m-1 \\ k \end{bmatrix} = \{1 - (|\mathbb{F}|^{m-k} - 1)/(|\mathbb{F}|^m - 1)\}\begin{bmatrix} m \\ k \end{bmatrix}$ k–spaces in U not in U^g. By (3.11),

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

We now consider nonsingular k–spaces N. 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 3.13. *If* $m \geq 3$ *and* $l \geq 1$ *is the Witt index of the members of* $\mathbf{NS}_k$, *then* $\mu(G, \mathbf{NS}_k)$ *is bounded as follows:*

G	$\mu(G,\mathbf{NS}_k) <$
$\mathrm{Sp}(2m,q)$, 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 (3.12),

$$1-\mu(g,\mathbf{NS}_k) \geq (1-\mu(g,\mathbf{TS}_l))(1-\max_{\substack{L,L'\in\mathbf{TS}_l\\ L\neq L'}} \Pr\{N\in\mathbf{NS}_k, L\subseteq N : L'\subseteq N\}). \tag{3.14}$$

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, G_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 $i = \dim L\cap L' \leq l-1$, consider the probability $P(i) = \Pr\{N\in\mathbf{NS}_k, L\subseteq N : L'\subseteq N\}$ on the right side of (3.14). We also have, for given $I \subset L \subset N \in \mathbf{NS}_k$ such that $i = \dim I$, $P(i) = \Pr\{L'\in\mathbf{TS}_l, L\cap L' = I = \mathrm{rad}\langle L, L'\rangle : L'\subseteq N\}$. Write $\delta = k-2l$. Table 1 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 $\mathbb{F}$, G_L is the set–stabilizer of L, and $O_p(G_L)$ is regular on $S_l(i)$.)

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

Table 1

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. Then $P(i)$ is given in the last column of Table 1, including a bound that is achieved when $l = i-1$.

Now (3.13) 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 (3.12) and (3.14). □

We will need slightly more precise estimates than in the preceding result:

Lemma 3.15. *Let $1 \neq g \in G = \Omega(2m+1,q)$, and let $\mathbf{NS}^\pm_{2m}$ denote either type of nonsingular hyperplanes of V, where $m \geq 4$.*

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

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

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

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

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

If $|g| \neq 2$ 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 $C_V(G)$ 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 $\mu(g,\mathbf{NS}^\pm_{2m}) = \frac{1}{2}q^k(q^k\pm 1)/\frac{1}{2}q^m(q^m\pm 1) \leq 1/q^2 + 1/q^m$.

Suppose that $|g| = 2$. 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 2–space $\langle x, y\rangle$ with x a singular point and y a point perpendicular to it. Clearly, $\mu(g, \mathbf{NS}^{\pm}_{2m}) \leq \Pr\{H^\pm \in \mathbf{NS}^{\pm}_{2m} : H^\pm \supseteq \langle x, y\rangle\}$. Let $\langle x', y'\rangle$ denote any 2–space isometric to $\langle x, y\rangle$ with x' singular.

If y is not singular then, for $H^\pm \in \mathbf{NS}^{\pm}_{2m}$,

$$\begin{aligned}\mu(g, \mathbf{NS}^{\pm}_{2m}) &\leq \Pr\{\langle x', y'\rangle : \langle x', y'\rangle \subseteq H^\pm\}\\ &= \{(q^m \mp 1)(q^{m-1} \pm 1)/(q-1)\}\{q^{m-2}(q^{m-1} \pm 1)\}/\{(q^{2m}-1)(q^{2m}-1)/(q-1)\}\\ &= q^{m-2}/(q^m \pm 1) \leq 1/q^2 + 1/q^m.\end{aligned}$$

Similarly, if y is singular then $\mu(g, \mathbf{NS}^{\pm}_{2m}) \leq \{(q^m \mp 1)(q^{m-1} \pm 1)/(q-1)\}\{(q^{m-1} \mp 1)(q^{m-2} \pm 1)/(q-1)(q^2 - 1)\}/\{(q^{2m}-1)(q^{2m}-1)/(q-1)(q^2-1)\} \leq 1/q^2 + 1/q^m$.

(iii) $\mu(g, \mathbf{NS}^{-}_{2m}) = \frac{1}{2}q^{m-1}(q^m + \delta)/\frac{1}{2}q^m(q^m + \varepsilon)$ for $\delta, \varepsilon = \pm 1$, 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 classical group with natural module V of dimension d. We choose an element s of G and determine the set $\mathcal{M}(s)$ maximal overgroups of s in G. 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 G containing s (or in the case of $\Omega(2m+1, q)$ with q even, those that act irreducibly modulo the radical $V^\perp$).

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 $GL(d, q)$ 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 sympletic 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* 2.

G		$\lvert s\rvert$ divides	$\mathcal{M}(s)$ and decomposition of V
$\mathrm{SL}(2m,q)$	$m \geq 2$ except $\mathrm{SL}(4,2)$, $\mathrm{SL}(11,2)$		
	odd	$(q^{m+2}-1)(q^{m-2}-1)$	$(m+2) \oplus (m-2)$
	even	$(q^{m+1}-1)(q^{m-1}-1)$	$(m+1) \oplus (m-1)$
$\mathrm{SL}(2m+1,q)$	$m \geq 2$, excluding $\mathrm{SL}(11,2)$		
		$(q^{m+1}-1)(q^{m}-1)$	$(m+1) \oplus m$
$\mathrm{Sp}(2m,q)$	$m \neq 1,2,3$ and also $m \neq 4,5,6,8,10$ if q is even		
	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**
$\mathrm{SU}(2m,q)$	$m \neq 1,2,3$		
	odd	$(q^{m+2}+1)(q^{m-2}+1)$	$(m+2) \perp (m-2)$
	even	$(q^{m+1}+1)(q^{m-1}+1)$	$(m+1) \perp (m-1)$
$\mathrm{SU}(2m+1,q)$	$m \neq 1,2,3$		
	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 $(m,q) \neq (5,2)$		
	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	$(q^{\frac{1}{2}(m+4)}+1)(q^{\frac{1}{4}(m-2)}-1)(q^{\frac{1}{4}(m-6)}+1)$	$(m+4)^{-} \perp [\frac{1}{4}(m-2) \oplus \frac{1}{4}(m-2)] \perp \frac{1}{2}(m-6)^{-}$
$\Omega^{-}(2n,q)$	$n = m+1 \geq 7$		
	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	$(q^{\frac{1}{2}(n+4)}+1)(q^{\frac{1}{4}(n-2)}+1)(q^{\frac{1}{4}(n-6)}+1)$	$(n+4)^{-} \perp \frac{1}{2}(n-2)^{-} \perp \frac{1}{2}(n-6)^{-}$
$\Omega(2m+1,q)$	$m \geq 2$ and q odd, excluding $\Omega(5,3)$ and $\Omega(7,q)$		
		$q^{m}+1$	$2m^{-} \perp 1$

Table 2

Proof. The action of s on V is given in the table, 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 $\mathcal{M}(s)$ of overgroups of s is obtained using [GPPS]. When $G = \mathrm{SL}(d,q)$ the irreducible constituents have relatively prime dimensions, thereby eliminating the possibility $\mathrm{SL}(de, q^{1/e}) \trianglelefteq M \in \mathcal{M}(s)$ for some $e > 1$. 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 the table), $\mathrm{SU}(m,q) < \mathrm{Sp}(2m,q)$, $\mathrm{SU}(m,q) < \Omega^{\pm}(2m,q)$, $\mathrm{Sp}(2m/t, q^{t}) < \mathrm{Sp}(2m,q)$ 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 the table the corresponding factor in column 3 of the form $q^{k} + (-1)^{k}$.

Case 1: G **is not** $\Omega(2m+1,q)$ **for** q **of any parity.**

The last column of Table 2 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 (3.1,3.12,3.13), $\mu(G, M^{G}) < 4/q^{(d-12)/8}$ for any $M \in \mathcal{M}(s)$. Thus, by (2.2), $1 - \mathrm{PC}(G) \leq \Sigma_{M}\mu(G, M^{G}) < 20/q^{(d-12)/8} \to 0$ as $q^{d} \to \infty$, provided only that $d \geq 20$.

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 2. We will give an example of this verification in Case 2 below. In many of the situations excluded in Table 2 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: $G \cong \Omega(2m+1, q)$**.**

Here $\mathcal{M}(s)$ contains the stabilizer of a nonsingular hyperplane U, and $\mu(g, U^G) < 1/q + 1/q^m$ by (3.15). 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 $d \geq 20$.

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 (3.15i,iii). Now $1/q + 13/q^{(d-12)/8} > 1 - \mathrm{PC}(G) \geq P_s(g) > 1/q - 1/q^m$, so $\lim_{d\to\infty} \mathrm{PC}(G) = 1 - 1/q$ for fixed q.

In Theorem II(b) we only need to consider sequences (G_i) for which q is bounded. Passing to a subsequence, we see that this completes the proof of that theorem when the dimension is not bounded.

Once again, more care with these same estimates yields $1 - \mathrm{PC}(G) < 9/10$ in every case within Table 2. For example, if $m \equiv 2 \pmod 4$ with $m \geq 10$, then $\mathcal{M}(s)$ consists of the stabilizers of the three indicated subspaces, together with a subgroup $\mathrm{O}^-(2m, q)$ if q is even. Use (3.15), and the g-invariant nonsingular subspaces of dimensions $m+4$, $(3m+2)/2$ and $(3m+6)/2$ in (3.13), in order to obtain $P_s(g) \leq 3(2/q^{m-1} + 1/q^m) + (q^{(m+4)/2} + q^{m-4}) + (q^{(3m+2)/4} + q^{(m-2)/2}) + (q^{(3m+6)/4} + q^{(m-6)/2}) + (1/q) < 9/10$. □

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: $\Omega(5,3)$, $\mathrm{PSU}(4,2)$, $\mathrm{PSU}(6,2)$, $\mathrm{PSU}(5,2)$, $\mathrm{PSU}(4,2)$, $\Omega^+(8,2)$, $\mathrm{P}\Omega^+(8,3)$, $\mathrm{Sp}(6,2)$, $\mathrm{Sp}(8,2)$, $\mathrm{P}\Omega^\pm(10,2)$, $\mathrm{Sp}(10,2)$ 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 $q \to \infty$.

We will list groups, bound the order of a torus in which s lies, and list $\mathcal{M}(s)$.

$\mathrm{PSL}(2,q)$, $q = 7$ or $q > 9$; $|s| = (q+1)/(2, q+1)$; $\mathcal{M}(s) = \{\mathrm{N}_G(\langle s\rangle)\}$; $|g^G| \geq q(q \pm 1)/2$ for $g \neq 1$, so $1 - \mathrm{PC}(G) \leq 5/q$ by (2.1) and (2.2).

$\mathrm{PSL}(3,q)$, $q > 2$. Let $|s| = (q^2+q+1)/(3, q-1)$; $\mathcal{M}(s)$ is $\{\mathrm{N}_G(\langle s\rangle)\}$ if $q \neq 4$ and $\mathrm{SL}(3,2)$ if $q = 4$. If $q \geq 5$ use $|g^G| \geq (q^2+q+1)(q+1)(q-1)$ for $g \neq 1$, along with (2.1) and (2.2), to obtain $1 - \mathrm{PC}(G) \to 0$ and $1 - \mathrm{PC}(G) < 9/10$. If $q = 3$, an element $g \in M$ of order 13 or 3 has centralizer in G of order 13 or 9, respectively, so $P_s(g) \leq |g^G \cap M|/|g^G| < 9/10$. If $q = 4$ then it is straightforward to check all nontrivial g in M in order to see that $|g^G \cap M|/|g^G| \leq 4/9$.

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

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

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

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

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

$\mathrm{P}\Omega^+(8,q)$, $q \geq 4$; $s\colon 2^- \perp 6^-$; $\mathcal{M}(s)$ consists of the stabilizer of a nonsingular 2–space, together with two subgroups obtained from it by applying triality; and (3.13) gives

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

$\mathrm{P}\Omega^+(2m,q)$, $2m = 12, 16, 20$; $s{:}\,4^- \perp (2m-4)^-$; $\mathcal{M}(s)$ consists of $\mathrm{N}_G(\mathrm{P}\Omega^+(6,q^2)\}$ and the stabilizer of a nonsingular 4–space; (3.13) and (2.3) give the desired bounds.

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

$\mathrm{PSp}(6,q)$, $q \geq 4$; $s{:}\,2 \perp 4$; $\mathcal{M}(s)$ 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 $q \geq 5$ and $(2/q^2 + 1/q^3 + 1/q^2 + 1/q^2) + (1/q + 1/q^3) < 9/10$ for even $q \geq 4$, by (3.13) and (3.15).

$\mathrm{Sp}(8,q)$, $q \geq 4$ even; $|s| = q^4 + 1$; $\mathcal{M}(s) = \{\mathrm{Sp}(4,q^2).2, \mathrm{O}^-(8,q)\}$; $1 - \mathrm{PC}(G) \leq 4/3q + 1/q < 9/10$ by (2.3) and (3.15).

$\mathrm{Sp}(10,q)$, $q > 2$ even; $s{:}\,2 \perp 8$; $\mathcal{M}(s)$ consists of the stabilizer of a nonsingular 2–space and, a subgroup $\mathrm{O}^+(10,q)$; $1 - \mathrm{PC}(G) \leq (2/q^3 + 1/q^5 + 1/q^4 + 1/q^2) + (1/q + 1/q^5) < 9/10$ for even $q \geq 4$, by (3.13) and (3.15).

$\mathrm{Sp}(4k,q)$, q even, $k = 3$ or 5; $|s| = q^{2k} + 1$; $M(s) = \{\mathrm{Sp}(2,q^k).k, \mathrm{Sp}(2k,q^2).2, \mathrm{O}^-(4k,q)\}$; $1 - \mathrm{PC}(G) \leq 4/3q^2 + 1/|G{:}\,\mathrm{Sp}(2,q^k).k| + 4/3q^2 + 1/|G{:}\,\mathrm{Sp}(2k,q^2).2| + 1/q < 9/10$ by (2.3) and (3.15).

$\mathrm{Sp}(16,q)$, q even; $|s| = q^8+1$; $M(s) = \{\mathrm{Sp}(8,q^2).2, \mathrm{O}^-(16,q)\}$; $1-\mathrm{PC}(G) \leq 4/3q^2 + 1/|G{:}\,\mathrm{Sp}(8,q^2).2| + 1/q < 9/10$ by (2.3) and (3.15).

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 a 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 G whose order is given in Table 3. Then $P_s(g) \leq \nu(G) \leq 3/4$, where $\nu(G)$ is given in the table. In particular, for such groups G, $\lim_{|G| \to \infty} \mathrm{PC}(G) = 1$.*

Proof. By [FM1, FM2], we have that $\mu(G) \leq (q^{1/3}-1)/(q^2-1)$ if $G = {}^2B_2(q)$, $\mu(G) \leq 1/(q^2-q+1)$ if G is either $G_2(q), q \neq 4$, or ${}^2G_2(q)$, $\mu(G_2(4)) = 4/51$; and $\mu(G) \leq 1/(q^4+q^2+1)$ otherwise.

It follows from [We] that an upper bound for $|\mathcal{M}(s)|$ is as given in Table 3. The result follows by using $\nu(G) := |\mathcal{M}(s)|\mu(G)$. □

G	$\lvert s\rvert$	$\lvert\mathcal{M}(s)\rvert$	$\nu(G)$
${}^2B_2(q), q = 2^{2k+1} = q_0^2,\ k \geq 1$	$q_0^2 + \sqrt{2}q_0 + 1$	1	$(q^{1/3}-1)/(q^2-1)$
${}^2G_2(q), q = 3^{2k+1} = q_0^2,\ k \geq 1$	$q_0^2 + \sqrt{3}q_0 + 1$	1	$1/(q^2-q+1)$
${}^2F_4(q), q = 2^{2k+1} = q_0^2,\ k \geq 1$	$q_0^4 + \sqrt{2}q_0^3 + q_0^2 + \sqrt{2}q_0 + 1$	1	$1/(q^4-q^2+1)$
$G_2(q), q \geq 5$	$q^2 - q + 1$	$\leq 2,\ \ 1 \text{ if } 3 \not\mid q$	$2/(q^2-q+1)$
${}^3D_4(q)$	$q^4 - q^2 + 1$	1	$1/(q^2-q+1)$
$F_4(q), q \geq 4$	$q^4 - q^2 + 1$	$\leq 2,\ \ 1 \text{ if } 2 \not\mid q$	$2/(q^4-q^2+1)$
${}^2E_6(q), q \geq 4$	$q^6 - q^3 + 1$	1	$1/(q^4-q^2+1)$
$E_6(q)$	$q^6 + q^3 + 1$	1	$1/(q^4-q^2+1)$
$E_7(q), q \geq 4$	$(q-1)(q^6+q^3+1)$	≤ 3	$3/(q^4-q^2+1)$
$E_8(q)$	$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$	1	$1/(q^4-q^2+1)$

Table 3

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 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 be an element whose order is given in Table 4. Then $P_s(g) \leq \nu(G) < 9/10$, where $\nu(G)$ is given in the table.*

G	$\lvert T\rvert = \lvert s\rvert$	$\mathcal{M}(T)$	$\mu(G)$	$\nu(G)$
M_{11}	11	$\mathrm{PSL}(2,11)$	3/11	3/11
M_{12}	11	$\mathrm{PSL}(2,11), M_{11}, M_{11}$	1/3	5/9
M_{22}	11	$\mathrm{PSL}(2,11)$	3/11	3/11
M_{23}	23	$\mathrm{N}_G(T)$	7/23	7/23
M_{24}	23	$M_{23}, \mathrm{PSL}(2,23)$	1/3	2/3
J_1	19	$\mathrm{N}_G(T)$	5/133	5/133
J_2	7	$\mathrm{PSU}(3,3), \mathrm{PSU}(3,3), \mathrm{PGL}(2,7)$	1/7	3/7
J_3	19	$\mathrm{PSL}(2,19), \mathrm{PSL}(2,19)$	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	$\mathrm{Sp}(4,4).2$	11/147	11/147
Ru	29	$\mathrm{N}_G(T)$	1/43	1/43
Suz	13	$G_2(4), \mathrm{PSL}(2,25), \mathrm{PSL}(2,25), \mathrm{PSL}(2,25)$	1/11	4/11
ON	31	$\mathrm{PSL}(2,31), \mathrm{PSL}(2,31)$	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	$2^{11}.M_{23}, \mathrm{PSL}(2,23)$	1/9	2/9
Fi_{24}'	29	$\mathrm{N}_G(T)$	1/9	1/9
HN	19	$\mathrm{PSU}(3,8).3$	1/39	1/39
Ly	67	$\mathrm{N}_G(T)$	7/55	7/55
Th	31	$\mathrm{N}_G(T), 2^5.\mathrm{PSL}(5,2), 2^5.\mathrm{PSL}(5,2), 2^5.\mathrm{PSL}(5,2)$	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	$\mathrm{PSL}(3,3){:}\,2, \mathrm{PSL}(3,3){:}\,2, \mathrm{PSL}(3,13)$	1/7	3/7
$G_2(4)$	13	$\mathrm{PSL}(2,13){:}\,2, \mathrm{PSU}(3,4){:}\,2$	4/51	8/51
${}^2F_4(2)'$	13	$\mathrm{PSL}(3,3){:}\,2, \mathrm{PSL}(2,25), \mathrm{PSL}(2,25), \mathrm{PSL}(2,25)$	1/13	5/13
$F_4(2)$	17	$\mathrm{Sp}(8,2), \mathrm{Sp}(8,2)$	1/13	2/13
$F_4(3)$	73	${}^3D_4(3).3$	1/73	1/73
${}^2E_6(2)$	19	$\mathrm{SU}(3,8).3$	1/13	1/13
${}^2E_6(3)$	$19 \cdot 37$	$\mathrm{SU}(3,27).3$	1/73	1/73
$E_7(2)$	$43 \cdot 3$	$\mathrm{SU}(8,2)$	1/13	1/13
$E_7(3)$	$4 \cdot 19 \cdot 37$	$4.{}^2E_6(3).2$	1/91	1/91

Table 4

Proof. The values for $\mu(G)$ are given in [Ma] for the sporadic groups and in [FM1, FM2] for the exceptional groups. So our entire proof amounts to defining s and $T = \langle s\rangle$ so that $\mathcal{M}(s)$ is small.

First consider the sporadic simple groups other than B and M. Then the conjugacy classes of all maximal subgroups H are all known (cf. [CCNPW, JLPW]). If $T \le H$ then, since T is a Sylow subgroup 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 $\mathcal{M}(s)$. We can almost always take $\nu(G) := \mu(G)|\mathcal{M}(s)|$. If $G = HS$, then we note that $|(\chi(x)+1)/(\chi(1)|+1)| \le 1/4$ for every nontrivial character χ of HS and for every nontrivial $x \in G$. In particular, $\mu(G) \le 1/4$ (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). The remaining case is $G = M_{12}$. One computes (using the permutation characters of the three maximal subgroups as given in [CCNPW]) that we may take $\nu(G) = 5/9$.

If $G = B$ 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 $\mathrm{PSL}(2,47)$; however, $\mathrm{PSL}(2,47)$ 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 the table.

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 $\mathrm{N}_G(E) = (29{:}\, 14 \times 2)^{\cdot}2$. Then H contains all involutions in $\mathrm{N}_G(E)$. Let U be the dihedral subgroup of order $29 \cdot 2$ 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 the table.

We now consider the exceptional groups in the proposition, for which we need only prove the statements about the about maximal overgroups of T.

All maximal subgroups of $G_2(3)$, $G_2(4)$ and $F_4(2)$ are known (cf. [Kl, Bu, NW]) and the description of $\mathcal{M}(s)$ 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 GF(3) of dimension 25 (cf. [JLPW]). Moreover, any nontrivial simple T–module has dimension 12 over GF(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 GF(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] and [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].

Finally, consider $E_7(q), q \leq 3$. If $q = 3$, then, by [LM, §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 $C = C_G(x) = 3 \times \mathrm{SU}(3, 7)$. It follows as in [LM, §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 $y = (\omega, \omega^2, \omega, \ldots, \omega)$. Then y is conjugate to x (in M). Moreover, y is central in $H := 3 \times \mathrm{PSU}(6, 2) \leq C$. Also, $D := C_G(y)$ 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, $C_P(x) \cong C_G(x)$. Thus, $C \leq P$. In particular, $y \in H \leq P$. Moreover, $C_P(y)$ properly contains H. Since C is maximal in P, it follows that $P = \langle C, C_P(y)\rangle \leq M$, so P is uniquely determined. Thus, the unique maximal overgroup of T is $\mathrm{N}_G(M)$. Since $\mathrm{N}_G(M) = MC_G(x)$ (because $\mathrm{N}_G(M)/M$ has order dividing 3), it follows that $M = \mathrm{N}_G(M)$ is maximal. □

We now consider some small dimensional classical groups over very small fields left open in Section 5:

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

Proof. The following observation will be useful. By [GM], if G is a simple group other than an alternating group acting primitively on n points, then every nonidentity element fixes less than half of the points unless x is a transvection in $\mathrm{Sp}(2m, 2)$ with a point stabilizer being $\mathrm{O}^-(2m, 2)$. In particular, if $s \in G$ is contained in a unique maximal subgroup and G is not an alternating group, then either $P_x(s) < 1/2$ or x is a transvection, $G = \mathrm{Sp}(2m, 2)$ and $P_x(s) < 9/10$.

Most of our estimates below are made using the character and maximal subgroup information in [CCNPW]. Often, the permutation character of the members of $\mathcal{M}(s)$ 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 constitutent 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 (and not improving the estimates by keeping track of intersections of maximal subgroups).

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

If $G = \mathrm{PSU}(3, 5)$, let s be of order 7. Then s is in exactly 3 maximal subgroups, each isomorphic to A_7 (see [CCNPW]). One computes that $\mu(g, M^G) \leq 1/5$ for any $1 \neq g \in G$. Thus, $P_s(g) \leq 3/5$.

If $G = PSU(4, 2) \cong \Omega(5, 3)$, 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 50 (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 $x \in G$.

If $G = \mathrm{PSU}(4, 3)$ and $|s| = 7$, then there are precisely 7 members of $\mathcal{M}(s)$ and all of their permutation characters are given in [CCNPW]. One computes directly that $P_s(x) < 9/10$ for all nontrivial x.

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

If $G = \mathrm{PSU}(6, 2)$, 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 $\mathrm{PSU}(4, 3).2$, 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 G of degree n (this follows by bounding $\chi(x)/\chi(1)$ for any nontrivial character χ). 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 $\mathrm{PSU}(4, 3).2$, 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 $|x^G|$). This shows that $P_x(s) < 9/10$.

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

If $G = \mathrm{PSp}(6, 3)$, let s be of order 14. The two maximal subgroups containing s are isomorphic to $\mathrm{PSL}(2, 27){:}\,3$ and $(2 \times \mathrm{PSU}(3, 3)))^{\cdot}2$. It follows by character estimates that $P_x(s) < 9/10$ for any nontrivial x.

If $G = \Omega(7, 3)$, 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 $P_x(s) \leq 17/28$.

If $G = \mathrm{Sp}(8, 2)$, let s be of order 17. The three maximal subgroups containing s are isomorphic to $\mathrm{O}^-(8, 2)$, $\mathrm{Sp}(4, 2){:}\,2$ and $\mathrm{PSL}(2, 17)$. Since each of these subgroups contains the full normalizer of the Sylow 17–subgroup and there is a unique conjugacy class of each type of subgroup, it follows that s is contained in precisely one of each type. 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, $P_x(s) < 9/10$.

If $G = \Omega^+(8, 2)$, take s of order 15 (specifically, of type $15A$). By [CCNPW] there are precisely 6 maximal subgroups containing x, isomorphic to $\mathrm{Sp}(6, 2), 2^6A_8, 2^6A_8, A_9, A_9$ and $(A_5 \times A_5).2^2$. The permutation characters for the first 5 are given in [CCNPW], and one computes $\nu_i(x) := |x^G \cap M_i|/|x^G|$ for each $x \in G$ of prime order for these 5 maximal subgroups M_i. In the last case, we estimate $|x^g \cap M|$ by the number of elements in M of the same order as x. This leads to $P_s(x) \leq \sum_i \nu_i(x) < 9/10$, as desired.

If $G = \mathrm{P}\Omega^+(8, 3)$, let s be of order 13. Then s is contained in 12 maximal subgroups: 6 isomorphic to $\Omega(7, 3)$ (in distinct conjugacy classes) and 6 isomorphic to $3^6{:}\,\mathrm{PSL}(4, 3)$ (2 in each of 3 distinct conjugacy classes). Using the character table, we see that $P_s(x) < 9/10$ for x not a long root element (type $3A$ in [CCNPW]). If x is a long root element, then using GAP one computes directly that $P_s(x) < 6/7$ (this computation, obtained by considering all conjugates of x, was performed by T. Breuer).

If $G = \mathrm{P}\Omega^{+}(10,2)$, 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 G is the stabilizer of of the nonsingular 8-space, whence $\mathrm{PC} > 1/2$.

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. 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 (3.15), $\mu(g, M_1^G) \le 9/32$. 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 $G = \mathrm{PSL}(11,2)$ and $|s| = 2^{11}-1$, then $\mathcal{M}(s) = \{\mathrm{N}_G(\langle s\rangle)\}$, so (2.3) applies.

7. Alternating groups.

In this section we will conclude the proof of the theorems by studying the alternating group A_n. 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:

Proposition 7.1. $\mathrm{PC}(A_n) > 1/10$ *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 be the product of disjoint cycles of length 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 M containing s is the stabilizer of the s–invariant m–set. For, this is clear if M is intransitive. If M 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 $M = G$ by an unpublished 1892 theorem of Marggraf [Wie, 13.5].

If g' denotes a p–cycle, then

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

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

Case 2: n odd.

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:

$m+1, m, m-1$ if $n = 3m$
$m, m, m+2$ if $n = 3m+2$
$m, m, m-2$ if $n = 3m-2$

where m is odd. 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 $J = G$ by Marggraf's theorem [Wie, 13.5]. 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,

$$\mu(g, \mathbf{S}_k) \le \Big\{\binom{k}{p} + \binom{n-k}{p}\Big\}\Big/\binom{n}{p} \le \Big\{\binom{k}{5} + \binom{n-k}{5}\Big\}\Big/\binom{n}{5} < 3/4,$$

as is checked using the specific pairs n, m.

If g' is a 3–cycle, we will proceed more directly in order to determine $1 - P_{g'}(s) = \Pr\{h \in g'^G : \langle h, s\rangle \text{ is transitive}\}$ precisely. Since each point moved by h must be in a different cycle of s, there are exactly $2k_1k_2k_3$ choices for h, 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 $\Pr\{s \in \mathrm{C}_G : \langle g, s\rangle \text{ is transitive}\} > 1/10$ for each n.

Finally, when g' is the product of two disjoint transpositions we will again determine $1 - P_{g'}(s) = \Pr\{h \in g'^G : \langle h, s\rangle \text{ is transitive}\}$. 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 a lies in a second cycle and b 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) or (3,1,2). This is at least 1/10 in view of the specific lengths k_α. □

Proposition 7.2. (i) *If $s \in G$ has at least two cycles, then $P_s(c_3) \ge 1/4 + O(1/n)$.*
(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 $x \ge 1$,

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

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

$$\Big\{\binom{m}{p} + \binom{n-m}{p}\Big\}\Big/\binom{n}{p} \le \Big\{\binom{m}{3} + \binom{n-m}{3}\Big\}\Big/\binom{n}{3} = 1/4 + O(1/n)$$

and

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

respectively. □

By (7.2i) we need to examine n–cycles. As might be expected, these produce an optimal conjugacy class.

Proposition 7.3. $\liminf(\mathrm{PC}(A_{2l+1}) \mid l \ge 2) = 8/9$. *The set of limit points of the sequence* $(\mathrm{PC}(A_{2l+1}) \mid l \ge 2)$ *consists of* 1 *together with* $1 - 1/m^2$ *for all odd integers* $m > 1$. *Moreover, any subsequence of this sequence that converges to* $1 - 1/m^2$ *has a subsequence of the form* $(\mathrm{PC}(A_{p_i m}) \mid p_i$ *is a prime* $\nmid m)$.

Proof. We may assume that $n > 23$. Let $C_G = s^G$ with $s = c_n$. Then $\mathcal{M}(c_n)$ consists of some of the following groups M in very familiar permutation representations:

(i) The set–stabilizer of the set of all cycles of $c_n^{n/k}$ whenever $k \big| n$, $1 < k < n$;

(ii) $|\mathrm{N}_G(\langle c_n\rangle)\colon \mathrm{N}_M(\langle c_n\rangle)|$ subgroups $M = \mathrm{P\Gamma L}(d, q) \cap A_n$ if n has the form $(q^d - 1)/(q - 1)$ for some prime power q and some integer $d \ge 2$;

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

For, first of all in each of the indicated cases there is a unique conjugacy class in G of subgroups of the indicated sort, and each has a unique conjugacy class of transitive cyclic subgroups $\langle c_n\rangle$. Hence, $\mathrm{N}_G(\langle c_n\rangle)$ is transitive on the set of all maximal overgroups of each type. In order to see that this list is complete, note that (i) handles the imprimitive case. By classical results of Burnside and Schur [Wie, p. 65], any maximial 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 list [Fe, 4.1].

We need an upper bound for $\mu(g, M^G)$ for each M appearing in (i-iii).

(i) Fix k. Since n is odd, $k \ge 3$ and hence

$$\mu(g, M^G) \le \mu(c_3, M^G) = \frac{n}{k}\binom{k}{3}\Big/\binom{n}{3} = (k-1)(k-2)\Big/(n-1)(n-2).$$

However, we do not need to consider all divisors k of n here: if a conjugate of c_3 fixes an orbit of some power c_n^l of c_n then it fixes an orbit of any power of c_n^l. Thus, when calculating $\Pr\{g \in c_3^G : \langle g, c_n\rangle \text{ is imprimitive}\}$, we may assume that the blocks have prime size k. Since there is no overlap arising from from different primes, the contribution of (i) to $P_{c_n}(c_3)$ is $\sigma_n := \sum_p (p-1)(p-2)/(n-1)(n-2)$, where the sum ranges over all prime factors p of n (not counting multiplicities).

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

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

(iii) By (2.1), $\mu(g, M^G) < \{n(n-1)\}/|G\colon C_G(g)|$. For $g \in M$, $|C_G(g)| \leq 2^{(n-1)/2}\{(n-1)/2\}!/2$, so that

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

Completion of the proof of (7.3). By (7.2i), the only way we can have a limit point larger than 1/4 is to have n odd and use $C_G = c_n^G$. The upper bounds in (ii) and (iii) are $O(1/n)$, so we only need to deal with the quantity σ_n in (7.4). For type (i) we saw that the "worst" choice of g for C_G is c_3, so $1 - \mathrm{PC}(A_n) = \sigma_n + O(1/n)$.

Now consider a sequence (A_{n_i}) such that $\lim \mathrm{PC}(A_{n_i})$ exists and is not 1. Then for each n_i there is a prime factor p_i such that p_i/n_i is bounded way from 0, and hence we may assume that $n_i = p_i m$ for some constant m. All but one of the summands in σ_{n_i} tends to 0, and hence $\sigma_{n_i} \to 1/m^2$. Thus, $1 - \mathrm{PC}(A_{n_i}) \to 1/m^2$. Moreover, $p_i \nmid m$ for all large i since $p_i \to \infty$. This yields all assertions of the proposition. □

This completes the proof of Theorems I and II. Of course, there are obvious types of analogues for symmetric groups of the results in this section.

8. Further results and remarks

1. Our results can be extended to the almost simple case without too much effort except in some small cases. In particular, let $G = \langle S, x\rangle \leq \mathrm{Aut}S$ with S a simple nonabelian normal subgroup of G. If $\langle x\rangle \cap S \neq 1$, our theorems apply. So we may assume that $x \notin S$ and x has prime order. One needs only replace the collection $\mathcal{M}(T)$ by $\mathcal{M}_x(T)$, the maximal elements in the set of overgroups of T whose S-class is x–stable. Often, these sets coincide, and then one uses the fixed point ratio estimates for almost simple groups (which are generally of the same order of magnitude as for the simple groups).

2. Shalev asked the following question: can every finite nonabelian simple group be generated by 2 subgroups of odd order? A minor variation of our results proves that every finite nonabelian simple group can be generated by 2 elements of odd order. However, this requires some extra effort in a finite number of cases. We note that our proof does show this (and more) for G sporadic, alternating or a group of Lie type in characteristic 2 (because our T may be taken of odd order). If G is a group of Lie type in odd characteristic p, then G can be generated by any nontrivial element and some Sylow p–subgroup (see [G]), whence Shalev's question has a positive answer. In particular, we have proved:

Propostion 8.1. *Every finite nonabelian simple group can be generated by an element of odd order and a subgroup of odd order.*

3. Here are 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 $G \neq \langle s, x\rangle$. Our results show that $P_s(G) < 1$ for all s, G. Prove that $P_s(G) < c$ for some fixed constant less than

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

(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] and [LM] when $pq = 6$.

(c) Prove that there exists an element $s = s_G$ such that, for any nontrivial $x \in G$ (or $\mathrm{Aut}G$), the probability that s and s^x 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. 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, 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 is the "best" type of class 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] and [LiSh2]. Presumably exact error terms arise using irreducible elements when these exist in G.

7. The classification of simple groups was used here rather heavily. We do not know how to avoid this. Nevertheless, Theorem I for classical groups was orginially 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. The case of exceptional groups should be possible in a similar manner, using [Co].

8. We are grateful to T. Breuer and G. Malle for providing us with GAP computations.

References

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

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

[Bu] G. Butler, The maximal subgroups of the Chevalley group $G_2(4)$, pp. 186–200 in: Groups–St. Andrews 1981 (eds. C. M. Campbell and E. F. Robertson), LMS Lecture Notes 71, Cambridge University Press, Cambridge 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. (3) 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 Press, 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 and 283–298.

[DT] L. Di Martino and C. Tamburini, 2-generation of finite simple groups and some related topics, pp. 195–233 in: Generators and relations in groups and geometries (eds. A. Barlotti et al.), Kluwer, NY 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. Proc. AMS Symp. Pure Math. 37 (1980) 175–181.

[FM1] D. Frohardt and K. Magaard, Fixed point ratios in exceptional groups of Lie type I, preprint.

[FM2] D. Frohardt and K. Magaard, Fixed point ratios in exceptional groups of Lie type II, preprint.

[G] R. Guralnick, Generation of simple groups, J. Algebra 103 (1986), 381-401.

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

[GM] R. M. Guralnick and K. Magaard, Primitive permutation groups containing elements that fix at least half the points, preprint.

[GPPS] R. M. Guralnick, T. Penttila, C. E. Praeger and J. Saxl, Linear groups with orders having certain primitive prime divisors, preprint.

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

[JP] W. Jones and B. Parshall, On the 1-cohomology of finite groups of Lie type. Proceedings of the 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. AMS 248 (1979) 347–379.

[Ka2] W. M. Kantor, Some topics in asymptotic group theory, pp. 403-421 in: Groups, Combinatorics and Geometry (eds. M. W. Liebeck and J. Saxl), LMS Lecture Notes 165, 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. Ded. 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. LMS Lecture Note Series 129, Cambridge U. Press 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. (3) 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. (3) 65 (1992), 297–325.

[LiSe] M. W. Liebeck and Seitz, Reductive subgroups of exceptional algebraic groups, AMS Memoirs 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. Ded., to appear.

[LM] F. Lübeck and G. Malle, $(2,3)$-generation of exceptional groups, preprint.

[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. Ded. 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. Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 4th edition, 1995.

[Sh] T. Shih, Bounds of fixed point ratios of permutation representations of $GL_n(q)$ and groups of genus zero, Ph. D. Thesis, California Institute of Technology, 1991.

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

[Wie] H. Wielandt, Finite permutation groups. Academic Press, New York 1964.

[Wil] R. A. Wilson, The geometry and maximal subgroups of the simple groups of A. Rudvalis and J. Tits. Proc. London Math. Soc. 48 (1984) 533-563.

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

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