COMMUNICATIONS IN ALGEBRA, 22(4), 1395-1402 (1994)

The Probability of Generating a Classical Group

Robert M. Guralnick*
Department of Mathematics
1042 W. 36th Place
University of Southern California
Los Angeles, CA 90089-1113
USA
e-mail: guralnic@mtha.usc.edu

William M. Kantor*
Department of Mathematics
University of Oregon
Eugene, OR 97403
USA
e-mail: kantor@bright.uoregon.edu

Jan Saxl
Department of Pure Mathematics
16 Mill Lane
Cambridge University
Cambridge CB2 1SB
England
e-mail: js134@phoenix.cambridge.ac.uk

0. Introduction

In [KL] it is proved that the probability of two randomly chosen elements of a finite classical simple group G actually generating G tends to 1 as $|G|$ increases. If $g \in G$, let $P_G(g)$ be the probability that, if h is chosen randomly in G, then $\langle g, h\rangle \neq G$. Let $P_G := \max\{P_G(g) \mid g \in G^{\#}\}$. In [KL, Conjecture 2] it is suggested that a stronger result might hold: $P_G \to 0$ as $|G| \to \infty$ for simple classical groups G. In this paper we investigate this question. It turns out that there is an interesting dichotomy here: while the answer is positive when the defining dimension is fixed and the field size increases, this is not so

* Partially supported by NSF.

if the defining field is fixed. We investigate the two cases separately; along the way we obtain information on the proportion of fix-point-free elements in linear groups and on the number of conjugacy classes of maximal subgroups in classical groups.

Our main results are as follows.

Theorem I. *Let G be a quasisimple classical group over $\mathbb{F}_q$. Then*

$$P_G \geq \frac{1}{2q^2+2}.$$

Theorem II. *Let G be a quasisimple classical group of dimension n over $\mathbb{F}_q$. Then, for fixed n,*

$$\lim_{q\to\infty} P_G = 0.$$

1. Fixed Field

We first prove a preliminary general result. If G acts on a set X, let G_x denote the stabilizer of $x \in X$. If $g \in G$, let $\mathrm{Fix}(g)$ be the set of fixed points of g. If $W \subset X$, let $P'_G(W)$ denote the probability that a random element of G fixes some element of W. Note the obvious inequality $P_G(g) \geq P'_G(\mathrm{Fix}(g))$.

Lemma 1.1. *Let G be a transitive subgroup of $\mathrm{Sym}(X)$, where $|X| = m$. Let s be the minimum length of an orbit of G_x on $X - \{x\}$. Let $W \subset X$ with $|W| = w > 0$. Then*

$$P'_G(W) \geq \frac{w}{m}\left(1 - \frac{w-1}{2s}\right).$$

Proof. Let N denote the number of elements of G fixing some element of W. For any $g \in G$ let $a_i(g)$ be the number of i-element subsets of $W \cap \mathrm{Fix}(g)$. Note that $1 \geq a_1(g) - a_2(g)$. Thus

$$\begin{aligned} N &\geq \sum_{g\in G} a_1(g) - \sum_{g\in G} a_2(g) \\ &= \sum_{x\in W} |G_x| - \sum_{\substack{x,x'\in W \\ x\neq x'}} |G_{xx'}| \\ &\geq |G|\left(\frac{w}{m} - \frac{w(w-1)}{2}\frac{1}{ms}\right) \end{aligned}$$

since $|G : G_{xx'}| \geq ms$. □

There is an intransitive version of the lemma (with the same proof). Note that one can apply the lemma to $G = A_n$ or S_n with $m = n = s+1 = w+3$. Then $P'_G(W) \geq 1/2 - 1/2n$. Thus, if g is a 3 cycle in G, then $P_G(g) \geq 1/2 - 1/2n$ is bounded away from 0.

We will apply the lemma to classical groups. Throughout the remainder of this paper, G will be a classical group, with corresponding natural n-dimensional module V over $F = \mathbb{F}_q$ (or $\mathbb{F}_{q^2}$ in the unitary case).

In the lemma let X be the set of singular 1-spaces of V (or all 1-spaces, if there is no form present), and let $W = \mathrm{Fix}(g)$ with g a long root element of G. If G is an orthogonal group, we assume that the dimension of V is at least 5. Thus, in all cases, G is either doubly transitive on X or has rank 3. The quantities m, s and $w = |W|$ are easily calculated in each case. Let $P'_G := P'_G(\mathrm{Fix}(g))$, so that $P_G \geq P'_G$. Write $\binom{r}{1}_q = (q^r - 1)/(q-1)$.

We first consider the case $SL_n(q) \leq G \leq GL_n(q)$. Here, $m = \binom{n}{1}_q$, $w = \binom{n-1}{1}_q$ and $s = m - 1$. Substituting these values into the lemma yields

$$P'_G \geq \frac{1}{q^n - 1}(q^{n-1} - \frac{1}{2}q^{n-2} - \frac{1}{2}).$$

Thus:

Proposition 1.2. *If $SL_n(q) \leq G \leq GL_n(q)$ with $n \geq 2$, then*

$$P'_G \geq \frac{1}{q+1}.$$

Next, consider $G = Sp_n(q)$ with $n \geq 4$ and even. Since g is a transvection and all 1-spaces are singular, m and w are the same as above. In this case, $s = w - 1$. This yields $P'_G \geq (q^{n-1} - 1)/2(q^n - 1)$, and hence we have

Proposition 1.3. *If $G = Sp_n(q)$ with $n \geq 4$ and even, then*

$$P'_G \geq \frac{1}{2(q+1)}.$$

The next case is $SU_n(q) \leq G \leq GU_n(q), n \geq 3$. Again, g is a transvection. Set $\epsilon = (-1)^n$. Then $m = f(q,n) := (q^n - \epsilon)(q^{n-1} + \epsilon)/(q^2 - 1)$ and $s = q^2 f(q, n-2) = w - 1$. Hence $P'_G \geq w/2m = f(q,n)/(1 + q^2 f(q, n-2))$.

Next, consider $\Omega_n(q) \leq G \leq O_n(q)$ with $n \geq 5$ and nq odd. In this case, $m = \binom{n-1}{1}_q$ and $s = q\binom{n-3}{1}_q$. There is an orthogonal decomposition $V = V_1 \perp V_2$, where V_i is a nonsingular subspace invariant under g, V_1 is 4-dimensional of + type, and g acts trivially on V_2. Moreover, the $q + 1$ fixed 1-spaces of g contained in V_1 are all singular. Thus $w = \binom{n-5}{1}_q q^2 + q + 1$. This yields $P'_G \geq (q^{n-3} - \frac{1}{2}q^{n-4} - \frac{1}{2})/(q^{n-1} - 1)$.

Finally, consider $\Omega^\epsilon_n(q) \leq G \leq O^\epsilon_n(q)$ with $n = 2k \geq 6$ and $\epsilon = \pm$. In this case, $m = h(q,n) := (q^k - \epsilon 1)(q^{k-1} + \epsilon 1)/(q - 1)$ and $s = qh(q, n-2)$. We decompose V as for the odd dimensional orthogonal groups with V_1 a 4-dimensional space of + type and V_2 of the same type as V. Thus $w = h(q, n-4)q^2 + q + 1$. In all cases, we find that:

Proposition 1.4. *Let $SU_n(q) \leq G \leq GU_n(q), n \geq 3$, or $\Omega^\epsilon_n(q) \leq G \leq O^\epsilon_n(q), n \geq 5$. Then*

$$P'_G \geq \frac{1}{2q^2 + 2}.$$

Propositions 1.2-1.4 complete the proof of Theorem I.

Note that the same argument shows that, if the codimension of the fixed point space of g is bounded, then for h random in G there is a reasonable probability that not only will $\langle g, h\rangle$ not be G but in fact it will fix some 1-space. This should be compared to [K, 3.3]: if g, h are chosen randomly among nongenerating pairs of elements of a simple classical group of dimension $n > 5$ (but $n > 8$ in the orthogonal case), then the group they generate will most likely fix a 1-space or a hyperplane.

Of course, additional variations on this theme are easily manufactured. For example, if g is restricted to being an involution of the classical group G, then $\mathrm{Fix}(g)$ can still be quite large if $n > 2$, and hence $P_G(g)$ is bounded away from 0 for fixed q. On the other hand, it is not clear what happens if, for example, g is restricted to being fixed-point-free on X.

We close this section with a proposition giving the number of non-fixed-point-free elements of $GL_n(q)$ in its action on $V - \{0\}$. See [W, Theorems 1, 2] when q a prime. While we will not need this result, it seems of interest in its own right.

Proposition 1.5. *Let G be either $GL_n(q)$ or $SL_n(q)$. The number of elements of G fixing at least one nonzero vector of V is*

$$|G| \sum_{i=1}^{n} \frac{(-1)^{i-1}}{(q-1)(q^2-1)\cdots(q^i-1)}. \tag{1}$$

Proof. Denote the quantity in (1) by λ. Write m_i for the order of the pointwise stabilizer in G of a subspace of dimension i. Then

$$\lambda = \sum_{i=1}^{n} (-1)^{i-1} \binom{n}{i}_q m_i q^{\binom{i}{2}}, \tag{2}$$

where

$$\binom{n}{i}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}$$

is the number of i-dimensional subspaces of V. For $i > 0$ write

$$S_i = \{(V_i, g) \mid g \in G,\ V_i \subseteq C_V(g) \text{ and } \dim(V_i) = i\}.$$

It follows from (2) that

$$\lambda = \sum_{i=1}^{n} (-1)^{i-1} |S_i| q^{\binom{i}{2}}. \tag{3}$$

Now consider the contribution to the right hand side of (3) for each element $g \in G$. If g fixes no nonzero vector, it features in none of the sets S_i and so contributes nothing to (3). So assume that $C_V(g)$ has dimension $j > 0$. Then the contribution to (3) of g is

$$\sum_{i=1}^{j} (-1)^{i-1} \binom{j}{i}_q q^{\binom{i}{2}}. \tag{4}$$

However, it is a well-known result of Cauchy that this expression is 1 (cf. [GJ, 2.6.12.2]). Thus λ is the number of elements of G fixing some nonzero vector, as claimed. □

Suppose W is a j-dimensional subspace of V. Then the argument of the previous proof shows that the number of elements of G fixing some nonzero vector of W is

$$\sum_{i=1}^{j} (-1)^{i-1} \binom{j}{i}_q m_i q^{\binom{i}{2}}.$$

2. Fixed Dimension

Fix a positive integer n and let G be a classical quasisimple group of dimension n defined over the field $\mathbb{F}_q$ with $q = r^a$, r prime. Let V be as before.

Our approach is similar to that in [KL]. The major difference is that, in [KL], small maximal subgroups contribute less than large ones and the important quanity is $\sum |M|$,

where the sum is over a set of representatives of conjugacy classes of maximal subgroups. Instead we need to obtain a bound on the number $\rho(G)$ of conjugacy classes of maximal subgroups of G. We split up the maximal subgroups into nine families of maximal subgroups according to a theorem of Aschbacher [A] (see also [KLi]).

The families are:

$[\mathcal{C}_1]$ Stabilizers of totally singular or nonsingular subspaces of V.
$[\mathcal{C}_2]$ Stabilizers of direct sum decompositions of V.
$[\mathcal{C}_3]$ Stabilizers of extension fields of F of prime degree.
$[\mathcal{C}_4]$ Stabilizers of tensor product decompositions $V = V_1 \otimes V_2$.
$[\mathcal{C}_5]$ Stabilizers of subfields of F of prime index.
$[\mathcal{C}_6]$ Normalizers of symplectic-type ℓ-groups ($\ell \neq r$ prime) in absolutely irreducible representations.
$[\mathcal{C}_7]$ Stabilizers of tensor product decompositions $V = V_1 \otimes \cdots \otimes V_m$ with each V_i of the same dimension.
$[\mathcal{C}_8]$ Stabilizers of forms.
$[\mathcal{S}]$ Normalizers of simple groups acting absolutely irreducibly on V such that the representation is defined over no proper subfield of F.

Aschbacher proved that every maximal subgroup of G is in one of the families listed above. Let Δ be the normalizer of G in the corresponding projective linear group (so Δ is the group of similarities of the form on V involved in the definition of G).

Let $\rho_i(G)$ be the number of Δ-conjugacy classes of maximal subgroups of G in $\mathcal{C}_i$. The next result follows from [KLi, Chapter 4] (see also [KL]). Let $\log(m) = \log_2(m)$.

Lemma 2.1.
(a) $\rho_1(G) \leq (3/2)n$.
(b) $\rho_2(G) \leq 2d(n) + 1$, *where* $d(n)$ *is the number of divisors of* n.
(c) $\rho_3(G) \leq \pi(n) + 2$, *where* $\pi(n)$ *is the number of prime divisors of* n.
(d) $\rho_4(G) \leq 2d(n)$.
(e) $\rho_5(G) \leq \pi(a) + 1 \leq \log(a) \leq \log\log(q)$.
(f) $\rho_6(G) \leq 1$.
(g) $\rho_7(G) \leq 3\log(n)$.
(h) $\rho_8(G) \leq 4$.

Let $\rho_0(G)$ be the number of G-conjugacy classes of maximal subgroups of G in $\cup_{i=1}^{8} \mathcal{C}_i$.

Corollary 2.2. $\rho_0(G) \leq c_1(n)\log\log(q)$ *for some constant* $c_1(n)$ *depending only on* n.

Proof. This follows from Lemma 2.1 and the observation that a Δ-conjugacy class of subgroups of G breaks up into at most n G-conjugacy classes. □

Now we must count the number of classes of maximal subgroups of G in $\mathcal{S}$. It is convenient to consider two families of simple groups. Let $\mathcal{S}_1$ (respectively $\mathcal{S}_2$) be the set of simple subgroups of G which act absolutely irreducibly on V, are defined over no subfield and are not (respectively are) isomorphic to a Chevalley group of the same characteristic as G. Let $\sigma_i(G)$ be the number of G-conjugacy classes of subgroups of G in $\mathcal{S}_i$.

Lemma 2.3. $\sigma_1(G) \leq c_2(n)$ *for some constant* $c_2(n)$ *depending only on* n.

Proof. As above, it suffices to prove this for Δ-conjugacy classes. Note that two simple subgroups are in the same Δ-class if and only if the corresponding representations of the covering groups are equivalent. By [LaS] (see also [KLi,§5.3]), there exists a finite family

$\mathcal{F}(n)$ of simple groups such that $\mathcal{S}_1 \subset \mathcal{F}(n)$. These groups have a total of at most $c_2(n)$ irreducible representations and the result follows. □

Finally, we consider $\mathcal{S}_2$. We only obtain an upper bound for the number of absolutely irreducible representations of dimension n which are defined over no proper subfield of F. This is sufficient for our application. We do not address the issue of when these representations correspond to maximal subgroups in the corresponding classical group. Indeed, it is quite likely that $\sigma_2(G) \leq c_3(n)$ for some constant $c_3(n)$ depending only on n.

Lemma 2.4. *Let $L \in \mathcal{S}_2$. Then the untwisted Lie rank d of L is at most $n-1$. Set $a' = a$ unless G is a unitary group, in which case set $a' = 2a$. Assume L is defined over the field F_{q^b}.*

(i) *If L is untwisted or is a Suzuki or Ree group, then $a' | b$ and $n \geq 2^{b/a'}$.*
(ii) *If L has type ${}^2A_d$, ${}^2D_d$, $d > 4$, or ${}^2E_6$, then $a'|2b$ and $n > 2^{b/a'}$.*
(iii) *If L has type ${}^3D_4$, then $a'|3b$ and $n \geq 2^{b/a'}$.*
In particular, the number of isomorphism classes of simple groups in $\mathcal{S}_2$ is bounded above by a function of n.

Proof. The bound on d follows from the fact that the rank of L is bounded by the rank of the linear group it is contained in. Now (i) - (iii) follow from from the Steinberg tensor product theorem (see [KlL, 5.4.6-8]). Since $b/a' \leq \log(n)$, the divisibility conditions in (i) - (iii) imply that there are at most $3\log(n)$ possibilities for b. Since there is a constant c such that there are at most cn possibilities for the type of L (by the bound on d), it follows that there are at most $3cn\log(n)$ possibilities for the isomorphism type of L. □

Lemma 2.5. *Let $L \in \mathcal{S}_2$. The number of irreducible representations of L into $GL_n(F)$ is bounded above by $c_4(n)(\log(q))^{\log(n)}$.*

Proof. Suppose L is defined over $\mathbb{F}_{q^b}$. By Steinberg's tensor product theorem, the irreducible modules for L can all be expressed as tensor products $\otimes_{i=1}^{b} R_i^{(r^i)}$, where R_i is a restricted irreducible module for L and $R_i^{(r^i)}$ is the module R_i twisted by the ith power of the Frobenius automorphism. If R is a restricted module for L, then $R \cong R(\lambda)$ for some weight $\lambda = \sum_{i=1}^{d} c_i\lambda_i$, where the λ_i are fundamental weights; here d is the untwisted Lie rank of L. By the preceding lemma, $d < n$. If R has dimension at most n, it follows (by restricting to SL_2) that each $c_i < n$ (this is not a very good bound). Thus, there are at most n^n possibilities for each R_i.

If $R = \otimes_{i=1}^{b} R_i^{(r^i)}$ is irreducible of dimension n, then at most $\log(n)$ of the R_i are nontrivial. Let t be the greatest integer at most $\log(n)$. The number of subsets of size t in a set of size b is bounded above by b^t. Thus, the number of irreducible representations of L of dimension n is bounded by $(n^{n\log(n)})b^t$.

By Lemma 2.4, $b \leq 2a\log(n) \leq 2\log(n)\log(q)$, and so the number of irreducible representations of L of dimension n is at most $c_4(n)(\log(q))^{\log(n)}$, as desired. □

Corollary 2.6. $\sigma_2(G) \leq c_5(n)(\log(q))^{\log(n)}$.

Proof. This follows from the two preceding Lemmas. □

Theorem 2.7. *There exists a function $c(n)$ such that $\rho(G) \leq c(n)(\log(q))^{\log(n)}$.*

Proof. This follows from Lemmas 2.1, 2.3 and 2.6. □

In fact, with more effort one should be able to improve the statement of Theorem 2.7 to $\rho(G) \leq c(n)\log\log(q)$. However, the above version is more than sufficient for our purposes.

Proof of Theorem II. Fix $g \in G^{\#}$. For each conjugacy class $\mathcal{M}_i$ of maximal subgroups of G, let $\mathcal{M}_i(g)$ be the set of those subgroups in $\mathcal{M}_i$ which contain g. Let $M_i \in \mathcal{M}_i$. It follows from the main result in [LS] that $|\mathcal{M}_i(g)| \leq (2/q)|\mathcal{M}_i|$ (unless G is $L_2(q)$ with $q = 7$ or $q = 9$). Then, since $|\mathcal{M}_i| = |G : M_i|$,

$$\begin{aligned} P_G(g) &\leq |G|^{-1} \sum_i |\mathcal{M}_i(g)||M_i| \\ &\leq (2/q) \sum_i |\mathcal{M}_i||M_i||G|^{-1} \\ &= (2/q)p(G) \\ &\leq 2c(n)(\log(q))^{\log(n)} q^{-1}. \end{aligned}$$

by Theorem 2.7. The result follows. □

A similar result is undoubtedly true for the exceptional Chevalley groups. The only obstacle is that there is no known general bound for the number of classes of embeddings of a simple group into an exceptional group.

As an immediate consequence of Theorem II, we see that any finite simple classical group is generated by an involution and one other element, provided q is sufficiently large (depending upon n). This additional restriction on q is in fact not necessary [MSW].

Finally, we note another consequence of Theorem 2.7. Let G be a simple classical group of dimension n in characteristic r. It follows from Steinberg's tensor product theorem that the number of conjugacy classes of r'-elements in G is q^{ℓ} where ℓ is the (untwisted) Lie rank of G. Thus Theorem 2.7 implies that, for sufficiently large q (depending upon n), the number of conjugacy classes of maximal subgroups of G is less than the number of conjugacy classes of elements. This should be true without restriction on q. In [AG] it was proved that it is true for finite solvable groups and was conjectured to be true for all finite groups.

References

[A] M. Aschbacher, "On the maximal subgroups of the finite classical groups", Invent. Math. 76 (1984), 469-514.

[AG] M. Aschbacher and R. Guralnick, "Solvable generation of groups and subgroups of the lower central series", J. Algebra 77 (1982), 189-207.

[GJ] I.P. Goulden and D.M. Jackson, Combinatorial Enumeration, Wiley and Sons, 1983.

[K] W.M. Kantor, "Some topics in asymptotic group theory" in Groups, Combinatorics and Geometry, editors M. Liebeck and J. Saxl, London Mathematical Society Lecture Note Series 165, Cambridge University Press, Cambridge, 1992, 403-421.

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

[KLi] P.B. Kleidman and M.W. Liebeck, The Subgroup Structure of the Finite Classical Groups, London Mathematical Society Lecture Note Series 129, Cambridge University Press, Cambridge, 1990.

[LaS] V. Landazuri and G.M. Seitz, "On the minimal degrees of projective representations of the finite Chevalley groups", J. Algebra 32 (1974), 418-443.

[LS] 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.

[MSW] G. Malle, J. Saxl and T. Weigel, "Generation of classical groups", to appear.
[W] L. Washington, "Some remarks on Cohen-Lenstra heuristics", Math. of Comp. 47 (1986), 741-747.

Received: September 1992