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 \( (g, h) \neq G \). Let \( P_G = \max \{ P_G(g) \mid g \in G^* \} \). In [KL, Conjecture 2] it is suggested that a stronger result might hold: \( P_G \rightarrow 0 \) as \( |G| \rightarrow \infty \) 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
Theorem 1. Let $G$ be a quasi-simple classical group over $\mathbb{F}_q$. Then

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

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

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

1. Fixed Field

We first prove a preliminary general result. If $G$ acts on a set $X$, let $G_x$ denote the number of $x \in X$. If $g \in G$, let $Fix(g)$ 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 $P_G(y) \geq P_G(Fix(g))$.

Lemma 1.4. Let $G$ be a transitive subgroup of $Sym(X)$, 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 $y \in G$ let $a_y$ be the number of $y$-element subsets of $W \cap Fix(y)$. Note that $1 \geq a_y - a_y(y)$. Thus

$$N \geq \sum_{y \in G} a_y - \sum_{y \in G} a_y(y) - \sum_{y \in G} |G_x| - \sum_{1 \leq i \leq s, 1 \leq j \leq w} |G_{x_i}||G_{x_j}||G_{x_i-x_j}|$$

$$\geq |G| \left( \frac{w}{m} - \frac{w(w-1)}{3} \right)$$

since $|G : G_x| \geq m$. \qed

There is an intrinsical version of the lemma (with the same proof). Note that one can apply the lemma to $G - A_1$ or $S_n$ with $m = n - s + 1 = w + 3$. Then $P_G(W) \geq \frac{1}{2w - 1/2}$. Thus, if $w$ is a 3-cycle in $G$, then $P_G(W) \geq 1/2 - 1/2w$. Thus, if $w$ is a 3-cycle in $G$, then $P_G(W) \geq 1/2 - 1/2w$ 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 $\mathbb{F}_q$ (or $\mathbb{F}_p$ 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 room problem), and let $W = Fix(g)$ 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 $P_G = P_G(Fix(g))$, so that $P_G \geq P_G$. Write $(q^n - 1)/(q - 1)$. 

PROBABILITY OF GENERATING A CLASSICAL GROUP

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

$$P_G \geq \frac{1}{q^n - 1} \left( q^{n-1} - \frac{1}{2} q^{n-2} - \frac{1}{2} \right).$$

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, $s = m - 1$. This yields $P_G \geq \frac{1}{q - 1/2}$, 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 $e = (1, 1, 0)$. Then $m = f(q, n) = (q^n - e)(q^{n-1} + e)/q^3 - 1$ and $s = qf(q, n - 2) = w - 1$. Hence $P_G \geq w/2m = f(q, n)/(1 + q^2)/(q, n - 2)$.

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

Finally, consider $O_n(q) \leq SL_n(q)$ with $n = 2k \geq 6$ and $e = \pm$. In this case, $m = f(q, n) = (q^n - e)(q^{n-1} + e)/q^2 - 1$ and $s = qf(q, n - 2)$. We decompose $V$ as for the odd dimensional orthogonal $V_1 \subset V$ a 4-dimensional space of $+1$ type and $V_2$ of the same type as $V$. Thus $w = (q^{n-1}_n - 1)/q^{n-1}_n + 1$. In all cases, we find that:

Proposition 1.4. Let $SU_n(q) \leq G \leq GU_n(q)$, $n \geq 3$, or $O_n(q) \leq G \leq GU_n(q), n \geq 5$. Then

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

Propositions 1.2-1.4 complete the proof of Theorem 1.

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 reasonably probability that not only will $(g, h)$ not be $G$ but in fact it will fix some 1-space. This should be compared to [K, 3]. If $g, h$ are chosen randomly among nongenerating pairs of elements of $n$ simple classical group of dimension $n > 5$ (but $n > 8$ in the orthogonal case), then the group 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 $Fix(g)$ can still be quite large if $n > 2$, and hence $P_G$ is bounded away from 0 for fixed $g$. On the other hand, it is not clear what happens if, for example, $g$ is restricted to being fixed-point-free on $X$. 

1397
Theorem 1. Let $G$ be a quasi-simple classical group over $\mathbb{F}_q$. Then

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

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

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

1. Fixed Field

We first prove a preliminary general result. If $G$ acts on a set $\mathbb{X}$, let $G_\mathbb{X}$ denote the number of $x \in \mathbb{X}$. If $g \in G$, let $\text{Fix}(g)$ be the set of fixed points of $g$. If $W \subseteq \mathbb{X}$, let $P_G(W)$ denote the probability that a random element of $G$ fixes some element of $W$. Note the obvious inequality $P_G(W) \geq P_G(\text{Fix}(g))$.

Lemma 1.4. Let $G$ be a transitive subgroup of $\text{Sym}(\mathbb{X})$, where $|\mathbb{X}| = m$. Let $s$ be the minimum length of an orbit of $G$ on $\mathbb{X} - \{x\}$. Let $W \subseteq \mathbb{X}$ 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 $n_g$ be the number of $1$-element subsets of $W \cap \text{Fix}(g)$. Note that $1 \geq n_g = n(g, y)$.

Thus,

$$N \geq \sum_{g \in G} n_g - \sum_{g \not\in G} n_g \geq \left| \mathbb{X} \right| - \left| \mathbb{X} \cap \text{Fix}(g) \right| - \left| \mathbb{X} \cap \text{Fix}(g) \right| \geq |G| \left( \frac{w}{m} - \frac{w(w-1)}{3} \right),$$

since $|G : G_{\mathbb{X}}| \geq m$. \qed

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

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 $\mathbb{F}_q$ (or $\mathbb{F}_p$ 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 $W = \text{Fix}(g)$ 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 $P_G = P_G(\text{Fix}(g))$, so that $P_G \geq P_G$. Write $(q)_k = (q^k - 1)/(q - 1)$.

PROBABILITY OF GENERATING A CLASSICAL GROUP

We first consider the case $SL_n(q) \leq G \leq GL_n(q)$. Here, $m = \binom{n}{2}$, $w = \binom{n-1}{2}$ and $s = m - 1$. Substituting these values into the lemma yields

$$P_G \geq \frac{1}{q^m - 1} \left( q^{m-1} - \frac{1}{2} q^{m-2} - \frac{1}{2} \right).$$

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 $P_G \geq \binom{n}{2}/2(q^{n-1} - 1)$, 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 $r = (-1)^n$. Then $m = f(q, n) = (q^n - r)(q^n - r + r)(q^n - r + r)$ and $s = q^n f(q, n - 2) = w - 1$. Hence $P_G \geq w/2m = f(q, n)/(1 + q^2)(q, n - 2)$. Thus, $P_G \geq 1/(q + 1)$.

Next, consider $G = SL_n(q) \leq O_n(q)$ with $n \geq 5$ and odd. In this case, $m = \binom{n-1}{k}$ and $s = q^n/(q^n - 1)$. There is an orthogonal decomposition $V = V_1 \perp V_2$, where $V_1$ is a nonsingular subspace invariant under $g$, $V_2$ is $4$-dimensional of type $A$, and $g$ acts trivially on $V_2$. Moreover, the $q+1$ fixed $1$-spaces of $g$ contained in $V_2$ are all singular. Thus $w = \binom{n}{2} - (q^n - 1)/2$. This yields $P_G \geq \binom{q^n - 1}{2} - (q^n - 1)/2$. Since $P_G \geq \binom{n}{2}/2(q^n - 1)$, the same argument shows that, if the codimension of the fixed point space fixes $V_1$ and $V_2$, the $q^{n-1}$ fixed $1$-spaces of $g$ contained in $V_2$ are all singular. Thus $w = \binom{n}{2} - (q^n - 1)/2$. In all cases, we find that:

Proposition 1.4. Let $SU_n(q) \leq G \leq GU_n(q)$, $n \geq 3$, or $O_n(q) \leq G \leq O_n(q)$, $n \geq 5$. 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 $(g, h)$ not be $G$ but in fact it will fix some $1$-space. This should be compared to [K, 39].

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 $\text{Fix}(g)$ can still be quite large if $n > 2$, and hence $P_G$ 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 $X$. 

1895

GURARLICK, KANTOR, AND SAXL
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 $q$ is 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

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

**Proof.** Denote the quantity in (1) by $\lambda$. Write $m_\lambda$ for the order of the pointwise stabilizer of $\lambda$ in of a subspace of dimension $i$. Then

$$\lambda = \sum_{i=1}^{n} (-1)^{i-1} \binom{n}{i} m_\lambda i(i).$$

where

$$\binom{n}{i} = \frac{q^i - 1}{i! (q-1)(q^2-1) \cdots (q^i-1)}$$

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

$$S_i = \{ (V, g) \mid g \in G, V \subseteq C_1(g) \text{ and } \dim(V) = i \}.$$  

It follows from (2) that

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

Now consider the contribution to the right hand side of (3) for each element $g \in G$. If $V$ has no nonzero vector, it features in none of the sets $S_i$, and so contributes nothing to (3). So assume that $C_1(g)$ has dimension $j > 0$. Then the contribution to (3) of $g$ is

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

However, it is a well known result of Cauaky that this expression is 1 (cf. [GJ, 2.6, 12.2]). Thus $\lambda$ is the number of elements of $G$ fixing some nonzero vector, as claimed. \(\square\)

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

$$\sum_{i=1}^{j} (-1)^{j-i} \binom{j}{i} m_\lambda i(i).$$

2. Fixed Dimension

Fix a positive integer $n$ and let $G$ be a classical quasisimple group of dimension $n$ defined over the field $F_q$ with $q = r^s$, $r$ 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 quantity is $\sum [M]$.

**PROBABILITY OF GENERATING A CLASSICAL GROUP**

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 [KL]).

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.
- $[\mathcal{C}_6]$ Stabilizers of symmetric type $t$-groups ($t \neq r$ 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.
- $[\mathcal{C}_9]$ 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 $\Delta$ be the normalizer of $G$ in the corresponding projective linear group (so $\Delta$ is the group of similarities of the form on $V$ involved in the definition of $G$). Let $\rho(G)$ be the number of $\Delta$-conjugacy classes of maximal subgroups of $G$ in $\mathcal{C}_t$.

The next result follows from [KL, Chapter 4] (see also [KL]). Let $\log(m) = \log_2(m)$.

**Lemma 2.1.**

(a) $\rho_t(G) \leq \log_2(m)$.
(b) $\rho_t(G) \leq \log_2(n) + 1$, where $d(n)$ is the number of divisors of $n$.
(c) $\rho_t(G) \leq \frac{n(n)}{\pi(n) + 2}$, where $\pi(n)$ is the number of prime divisors of $n$.
(d) $\rho_t(G) \leq \log_2(m)$.
(e) $\rho_t(G) \leq \frac{n}{\pi(n) - 1} \leq \log_2(n) \leq \log_2(q)$.
(f) $\rho_t(G) \leq 1$.
(g) $\rho_t(G) \leq 3 \log_2(m)$.
(h) $\rho_t(G) \leq 4$.

Let $\rho_t(G)$ be the number of $G$-conjugacy classes of maximal subgroups of $G$ in $0 \otimes_1 C_i$.

**Corollary 2.2.** Let $\rho_t(G) = \frac{m}{\log_2(m)}$ for some constant $c_1(n)$ depending only on $n$.

**Proof.** This follows from Lemma 2.1 and the observation that a $\Delta$-conjugacy class of subgroups of $G$ breaks up into at most $n$ $G$-conjugacy classes. \(\square\)

Now we must count the number of classes of maximal subgroups of $G$ in $S_t$. It is convenient to consider two families of simple groups. Let $S_1$ (respectively $S_2$) 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 $\sigma_t(G)$ be the number of $G$-conjugacy classes of subgroups of $G$ in $S_t$.

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

**Proof.** As above, it suffices to prove this for $\Delta$-conjugacy classes. Note that two simple subgroups are in the same $\Delta$-class if and only if the corresponding representations of the covering groups are equivalent. By [LoS] (see also [KL, §5.3]), there exists a finite family
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 $q$ is a prime.

While we will not need this result, it seems of interest in its own right.

**Proposition 1.8.** 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

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

**Proof.** Denote the quantity in (1) by $\lambda$. Write $m_i$ for the order of the pointwise stabilizer of $i$ i.e. of a subspace of dimension $i$. Then

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

where

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

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

$$S_i = \{(\nu, g) \mid g \in G, V_i \leq G, \dim(V_i) = i\}.$$

It follows from (2) that

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

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

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

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

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

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

### 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 $q = r^s$, $r$ 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 quantity 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 [KL]).

The families are:

- $[c_1]$ Stabilizers of totally singular or nonsingular subspaces of $V$.
- $[c_2]$ Stabilizers of direct sum decompositions of $V$.
- $[c_3]$ Stabilizers of extension fields of $F$ of prime degree.
- $[c_4]$ Stabilizers of tensor product decompositions $V = V_1 \otimes V_2$.
- $[c_5]$ Stabilizers of subfields of $F$ of prime index.
- $[c_6]$ Stabilizers of symplectic-type $f$-groups (if $q = r$ prime) in absolutely irreducible representations.
- $[c_7]$ Stabilizers of tensor product decompositions $V = V_1 \otimes \cdots \otimes V_m$ with each $V_i$ of the same dimension.
- $[c_8]$ Stabilizers of forms.
- $[c_9]$ 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 $\Delta$ be the normalizer of $G$ in the corresponding projective linear group (so $\Delta$ is the group of similarities of the form on $V$ involved in the definition of $G$).

Let $\rho(G)$ be the number of $\Delta$-conjugacy classes of maximal subgroups of $G$ in $C$. The next result follows from [KL, Chapter 4] (see also [KL]). Let $\log(m) = \log_2(m)$.

**Lemma 2.1.**

(a) $\rho(G) \leq |G|/|2|.$
(b) $\rho(G) \leq 2\delta(n) + 1$, where $\delta(n)$ is the number of divisors of $n$.
(c) $\rho(G) \leq \pi(n) + 2$, where $\pi(n)$ is the number of prime divisors of $n$.
(d) $\rho(G) \leq 2d(n)$.
(e) $\rho(G) \leq \pi(n) + 1 \leq \log(n) \leq \log \log(q)$.
(f) $\rho(G) \leq 1$.
(g) $\rho(G) \leq 3\log(n)$.
(h) $\rho(G) \leq 4$.

Let $\rho_G(n)$ be the number of $G$-conjugacy classes of maximal subgroups of $G$ in $\mathfrak{U}_{E_{6n}}$, $\mathfrak{E}_{6n}$.

**Corollary 2.2.** $\rho_G(n) \leq \sigma(n)\log \log(q)$ for some constant $\sigma(n)$ depending only on $n$.

**Proof.** This follows from Lemma 2.1 and the observation that a $\Delta$-conjugacy class of subgroups of $G$ breaks up into at most $n$ $G$-conjugacy classes. \(\square\)

Now we must count the number of classes of maximal subgroups of $G$ in $S$. It is convenient to consider two families of simple groups. Let $S_1$ (respectively $S_2$) 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 $\sigma_1(G)$ be the number of $G$-conjugacy classes of subgroups of $G$ in $S_1$.

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

**Proof.** As above, it suffices to prove this for $\Delta$-conjugacy classes. Note that two simple subgroups are in the same $\Delta$-class if and only if the corresponding representations of the covering groups are equivalent. By [LoS] (see also [KL, §5.3]), there exists a finite family...
If \( \sigma(n) \) of simple groups such that \( S_1 \subset F(n) \). These groups have a total of at most \( c_1(n) \) irreducible representations and the result follows. \( \square \)

Finally, we consider \( S_2 \). We only obtain an upper bound for the number of absolutely irreducible representations of dimension \( n \) which are defined over no proper subfield of \( \mathbb{F} \). 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. (It is quite likely that \( \sigma_2(G) \leq c_2(n) \) for some constant \( c_2(n) \) depending only on \( n \).

**Lemma 2.1.** Let \( L \in S_2 \). Then the untwisted Lie rank \( d \) of \( L \) is at most \( n-1 \). Set \( d' = \min \{ d, G \} \) is a unitary group, in which case \( d' = 2n \). Assume \( L \) is defined over the field \( \mathbb{F} \).

- If \( L \) is untwisted or is a Simul or free group, then \( d' \leq n \).
- If \( L \) has type \( E_8, D_4 \), or \( F_4 \), then \( d' \leq 2n \).
- If \( L \) has type \( B_n, \) then \( d' = 2n \) and \( n \geq 2^{n/2} \).

In particular, the number of isomorphism classes of simple groups in \( S_2 \) 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) - (ii) follow from the Steinberg tensor product theorem (see [KL, 5.4 & 8]). Since \( b/c \leq \log(n) \), the divisibility conditions in (ii) imply that there are at most \( 3\log(n) \) possibilities for \( b \). Since there is a constant \( c \) such that there are at most \( c \log(n) \) possibilities for the type of \( L \) (by the bound on \( d \)), it follows that there are at most \( 3c \log(n) \) possibilities for the isomorphism type of \( L \).

**Lemma 2.5.** Let \( L \in S_2 \). The number of irreducible representations of \( L \) into \( GL(n,F) \) is bounded above by \( c_2(n)(\log(q))^{\log^2(n)} \).

**Proof.** Suppose \( L \) is defined over \( \mathbb{F}_q \). By Steinberg's tensor product theorem, the irreducible modules for \( L \) can all be expressed as tensor products of \( R_{i_1}^c R_{i_2}^{c_2} \), which \( R_i \) is a restricted indecomposable module for \( L_i \). Theorem 2.1 twisted by the \( i \)-th power of the Frobenius automorphism. If \( R \) is a restricted module for \( L \), then \( R \equiv R_{i^n} \) for some integer \( n \leq n \), where the \( i^n \) are fundamental weights; here \( d \) is the untwisted Lie rank of \( L \). By the preceding lemmas, \( d \leq n \). If \( R \) has dimension at most \( n \), then it follows (by restricting to \( S(L) \) that each \( c_i \leq n \) (this is a very good bound). Thus, there are at most \( d^n \) possibilities for each \( R_i \).

If \( R \equiv R_{i^n} \) is irreducible of dimension \( n \), then at most \( \log(n) \) of the \( R_i \) are nontrivial. Let \( t \) be the greatest integer at \( \log(n) \). The number of subsets of size \( t \) of a set of size \( h \) is bounded above by \( \binom{h}{t} \). Thus, the number of irreducible representations of \( L \) of dimension \( n \) is bounded by \( (n^{t}(\log(n))^{\log^2(n)} \).

By Lemma 2.4, \( b \leq 2n(\log(n)) \leq 2n(\log(q)) \), and so the number of irreducible representations of \( L \) of dimension \( n \) is at most \( c_1(n)(\log(q))^{\log^2(n)} \), as desired. \( \square \)

**Corollary 2.6.** \( \sigma(n) \leq c_2(n)(\log(q))^{\log^2(n)} \).

**Proof.** This follows from the two preceding Lemmas. \( \square \)

**Theorem 2.7.** There exists a function \( c(n) \) such that \( \rho(G) \leq c(n)(\log(q))^{\log^2(n)} \).

**Proof.** This follows from Lemmas 2.1, 2.3 and 2.6. \( \square \)

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

**References**


$\mathcal{F}(n)$ of simple groups such that $S_i \in \mathcal{F}(n)$. These groups have a total of at most $e_2(n)$ irreducible representations and the result follows. \qed

Finally, we consider $S_2$. We only obtain an upper bound for the number of absolutely irreducible representations of dimension $n$ which are defined over no proper subfield of $k$. 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. However, it is quite likely that $\sigma_2(G) \leq e_2(n)$ for some constant $e_2(n)$ depending only on $n$.

Lemma 2.1. Let $L \in S_2$. Then the twisted Lie rank $d$ of $L$ is at most $n - 1$. Set $d'$ to be a nontrivial group in any case set $d' = 2n$. Assume $L$ is defined over the field $k'$.

1. If $L$ is un twisted or is a Simhash group, then $d'|b$ and $n \geq 2^d'/2$.
2. If $L$ has type $\mathfrak{A}_n$, $d' = 4$, or $\mathfrak{F}_4$, then $d'|b$ and $n \geq 2^d'/4$.
3. If $L$ has type $\mathfrak{B}_n$, then $d' = 3$ and $n \geq 2^d'/3$.

In particular, the number of isomorphismclasses of simple groups in $S_2$ is bounded above by $e_2(n)$ as 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 (1) - (3) follow from the Steinberg tensor product theorem (see [Ku, 5.4.6.8]). Since $b'/d' \leq \log(q)$, the divisibility conditions in (2) imply that there are at most $3\log(q)$ possibilities for $b$. Since there is a constant $c \leq 1$ that there are at most $cn$ possibilities for the type of $L$ (by the bound on $d'$), it follows that there are at most $3\log(q)$ possibilities for the isomorphism type of $L$.

Lemma 2.2. Let $L \in S_2$. The number of irreducible representations of $L$ into $GL_n(F)$ is bounded above by $e_2(n)(\log(q))^{\log(n)}$.

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

If $R = \otimes_{k=1}^n R_{1,k}$ is irreducible of dimension $n$, then at most $n^d$ (or $R$) 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 $(n^d)^{b^t}$.

By Lemma 2.4, $b \leq 2\log(n)$, and so the number of irreducible representations of $L$ of dimension $n$ is at most $e_2(n)(\log(q))^{\log(n)}$, as desired. \qed

Corollary 2.6. $\sigma_2(G) \leq e_2(n)(\log(q))^{\log(n)}$, as desired. \qed

Proof. This follows from the two preceding Lemmas. \qed

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. \qed

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

Proof of Theorem 2.1. Fix $g \in G^\infty$. For each conjugacy class $M_i$ of maximal subgroups of $G$, let $\mathcal{M}_i(q)$ be the set of those subgroups in $M_i$ which contain $g$. Let $M_i \in \mathcal{M}_i$. It follows from the main result in [LS] that $|\mathcal{M}_i(q)| \leq (2/g)|M_i|$ (unless $G$ is $L_3(q)$ with $q = 7$ or $q = 9$). Then, since $|M_i| = |G : M_i|$, $P_G(q) = \left| \sum_{i=1}^{|G| \mathcal{M}_i(q)| |M_i|^{-1} \right| \leq (2/g)P_G(q)$, $\leq 2\pi(n)(\log(q))^{\log(n)}q^{-1}$.

by Theorem 2.7. The result follows. \qed

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 2.1, we see that any finite simple classical group is generated by an involution and one 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 $p$. It follows from Steinberg's tensor product theorem that the number of conjugacy classes of $p'$-elements in $G$ is $q^p$ where $p$ is the (un twisted) 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


GURALNICK, KANTOR, AND SAXL


Received: September 1992