COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **23** (1) (2003) 73–87

ON THE SPREAD OF FINITE SIMPLE GROUPS

ROBERT M. GURALNICK, ANER SHALEV

Received October 23, 1999
Revised January 1, 2001

The spread of a finite group is the maximal integer k so that for each k non-identity elements of G there is an element generating G with each of them. We prove an asymptotic result characterizing the finite simple groups of bounded spread. We also obtain estimates for the spread of the various families of finite simple groups, and show that it is at least 2, with possibly finitely many exceptions. The proofs involve probabilistic methods.

1. Introduction

In recent years there has been considerable interest in generation properties of finite simple groups and permutation groups, and many results were obtained using counting and probabilistic methods. See for instance [1,14, 10,15–17,9]. In this paper we follow a similar approach in the study of the spread of finite simple groups, solving some problems from [5–7].

Let G be group. The spread $s(G)$ of G is defined to be the maximal integer k such that for any k non-identity elements $x_1,\dots,x_k \in G$ there exists $y \in G$ such that $\langle x_i, y\rangle = G$ for all $i = 1,\dots,k$. Note that groups of spread at least one are precisely the so called 3/2-generated groups. By [9] $s(G) \geq 1$ for any finite simple group. The spread of symmetric and alternating groups is studied in [3–7]. It was shown that (with some small exceptions), $s(S_{2n}) = 2$, $s(S_{2n+1}) = 3$ and $s(A_{2n}) = 4$. It was suggested in [6] that $s(A_{2n+1})$ might

Mathematics Subject Classification (2000): 20B30, 20D08; 20P05

The first author acknowledges the support of the NSF; the second author acknowledges the support of the Israel Science Foundation and the hospitality of USC; both authors acknowledge the support and hospitality of MSRI

tend to infinity with n. We show that this is not the case. More specifically, we show that $s(A_n)$ tends to infinity if and only if the smallest prime divisor $p(n)$ of n tends to infinity. In particular, this provides a positive answer to a problem from [5] as to whether $s(A_p)$ tends to infinity with p where p is prime.

We then study the spread of finite simple groups in general and prove the following.

Theorem 1.1. *Let G_i be a sequence of finite simple groups with $|G_i|$ tending to infinity. Then $s(G_i) \to \infty$ if and only if there does not exist an infinite subsequence of the G_i consisting either of odd dimensional orthogonal groups over a field of fixed size or alternating groups of degree all divisible by a fixed prime.*

We note that lower bounds on the spread of some classical groups were recently obtained in [2]. Our method for obtaining lower bounds is probabilistic, and relies crucially on recent results from [9]. The upper bounds on the spread are obtained via direct constructions.

In Section 2 we prove Theorem 1.1. Section 3 is devoted to explicit estimates of $s(G)$ for the various finite simple groups G. We give upper and lower bounds for all families of finite simple groups which are roughly of the same order of magnitude. For A_n, the spread is largest when n is prime and otherwise can be estimated between two polynomials of small degree in the smallest prime divisor of n. If G is a finite simple group of Lie type of rank ℓ over the field of q elements, then we show the spread can be bounded between two polynomials in q of bounded degree (in the case of odd dimensional orthogonal groups), of degree $c_i\ell$, $i = 1, 2$ (in the other cases except for linear and unitary groups) and of degree $c_i\ell p$ where p is the smallest prime divisor of the dimension of the natural module (in case G is linear or unitary).

We also show the following.

Theorem 1.2. *$s(G) \geq 2$ for all but finitely many finite simple groups G.*

It might be that $s(G) \geq 2$ for all finite simple groups; indeed, there are no known examples of finite simple groups with spread 1. We do show that $s(G) = 2$ for almost all the groups $G = Sp(2m, 2)$.

One can study the structure of arbitrary finite groups of spread at least 1. If G is abelian, then G is either cyclic or is an elementary abelian p-group of rank 2 for some prime p. If G is cyclic, then $s(G)$ is infinite. If G is elementary abelian p-group of rank 2, then $s(G) = p$.

Let G be such a group that is not abelian. Clearly, if N is any minimal normal subgroup of G, then G/N is cyclic. It follows that N is unique and either is a nonabelian simple group or is an elementary abelian p-subgroup for some prime p and G/N acts faithfully and irreducibly on N. This latter situation was studied by [20]. In that case clearly, $s(G) \geq 2$. Indeed, one sees easily that $s(G) \geq |N|-1$ (indeed, $s(G) = |N|-1$ unless G/N has prime order in which case $s(G) = |N|$).

It is still open whether $s(G) \geq 1$ for the case that N is nonabelian simple and G/N is cyclic (and there are no examples with $s(G) \leq 1$). The results in [9] show that given any nontrivial element in G, there exists a mate so that the pair generates a subgroup containing N and in many but not all cases generates G.

We note that our results on lower bounds for the spread of simple groups depend on the classification of simple groups. However, one can modify the proofs suitably so that for the known classes of finite simple groups, one gets similar results without the use of the classification theorem.

2. Proof of Theorem 1.1

Let G be a finite simple group. For a conjugacy class C of G and an element $x \in G$ let $P(x,C)$ denote the probability that $\langle x, y\rangle = G$ where y is a randomly chosen element of C. Let $P(C) = \min\{P(x,C) : 1 \neq x \in G\}$, and set $PC(G) = \max_C P(C)$ where C ranges over the conjugacy classes of G. Thus, if $PC(G) = r$ then there exists a conjugacy class $C \subset G$ such that for every non-identity element $x \in G$ we have $P(x,C) \geq r$. Let us call this class C a good class of G.

Lemma 2.1. *With the above notation we have*

$$s(G) \geq \lceil (1 - PC(G))^{-1} - 1 \rceil.$$

Proof. Let $k < (1-PC(G))^{-1}$ be an integer. We have to show that $s(G) \geq k$. Let $x_1, \ldots, x_k$ be non-identity elements of G, and let C be a good class. Then the probability that a random element y from C satisfies $\langle x_i, y\rangle \neq G$ for a given i is $1 - PC(G)$. Therefore the probability that $\langle x_i, y\rangle \neq G$ for some i is at most $k(1 - PC(G))$ which is strictly less than one. It follows that some $y \in C$ satisfies $\langle x_i, y\rangle = G$ for all $i = 1, \ldots, k$, so $s(G) \geq k$. ∎

We now invoke the following result from [9].

Theorem 2.2. *Let G_i be a sequence of finite simple groups with $|G_i| \to \infty$. Either $\lim_i PC(G_i) = 1$ or there exists an infinite subsequence of the G_i*

consisting either of odd dimensional orthogonal groups over a field of fixed size or alternating groups of degree all divisible by a fixed prime.

Combining 2.1 and 2.2 we obtain

Corollary 2.3. *Let G_i be a sequence of finite simple groups with $|G_i| \to \infty$. Either $s(G_i) \to \infty$ or there exists an infinite subsequence of the G_i consisting either of odd dimensional orthogonal groups over a field of fixed size or alternating groups of degree all divisible by a fixed prime.*

In order to complete the proof of Theorem 1.1 it now remains to show that $s(G)$ is bounded when $G = A_n$ and $p(n)$ is bounded, and when G is an odd dimensional orthogonal group over a bounded field.

In the case $G = A_n$ we may assume that n is not prime, otherwise $n = p(n)$ is bounded and the conclusion follows trivially.

Proposition 2.4. *Let $n > 4$ be a composite positive integer and let $p = p(n)$. Then $s(A_n) < \binom{2p+1}{3}$.*

Proof. Let $T = \{(i,j,k) : 1 \le i < j < k \le 2p+1\}$. We claim that for each element $y \in A_n$ there exists $x \in T$ such that $\langle x, y\rangle \ne A_n$. Suppose y consists of c cycles. If there is $x \in T$ whose support is disjoint from one of these cycles, then $\langle x, y\rangle$ is intransitive. Since $2p+1 \ge 5$ this is the case unless $c = 1$. So suppose y is a full cycle. We show that $\langle x, y\rangle$ is imprimitive for some $x \in T$. Color the indices $1, \dots, 2p+1$ with p colors according to which orbit of $y^{n/p}$ they belong to. Then there are i, j, k, $1 \le i < j < k \le 2p+1$ of the same color. Hence $x = (i,j,k)$ and y both preserve the partition consisting of the orbits of $y^{n/p}$. Therefore $\langle x, y\rangle \ne A_n$. It follows that $s(A_n) < |T|$. This completes the proof. ∎

In the next result, we use the well known fact that every element of $Sp(2m,q)$ with q even is contained in a conjugate of $O^{\pm}(2m,q)$ (cf. [18]).

Proposition 2.5. *Let $G = \Omega(2m+1,q)$, $m \ge 2$.*
(i) *If q is odd then $s(G) \le (q^2+q)/2$.*
(ii) *If q is even then $s(G) \le q$.*

Proof. Let V be the natural orthogonal module for G. First consider the case that q is odd. Note that there exists a conjugacy class C in G of elements which have -1 eigenspace a hyperplane of V. Let D denote the set of 1-spaces which are the fixed spaces of such elements and fix $L \in D$.

Let $W = L \perp U$ with U a nonsingular 2-dimensional subspace of $+$ type be a 3-dimensional nonsingular subspace of V. We first claim that given

any vector $w \in W$, it is orthogonal to some L', a nonsingular 1-space of the same type as L in W. This is clear since U contains both singular 1-spaces and nonsingular 1-spaces of both types. The number of such 1-spaces in W is $s := (q^2 \pm q)/2$ (depending on the type of L). Denote these subspaces $L_1, \ldots, L_s$. It follows that every vector in V is orthogonal to one of these L_i (we can write $v = v_1 + v_2$ with $v_1 \in W$ and $v_2 \in W^\perp$; so $(v, L_i) = (v_1, L_i) = 0$ for some i).

Now choose elements $r_1, \ldots, r_s \in G$ so that $r_i \in C$ and the fixed space of r_i is $L_i \subset W$. Let $g \in G$. Then g fixes some vector in V and so this vector is orthogonal to at least one of the L_i, whence $G \neq \langle g, r_i \rangle$ for some i. Hence $s(G) < (q^2 + q)/2$.

We now prove part (ii). So q is even. In this case, V has a 1-dimensional socle. The stabilizers of the complementary hyperplanes are precisely the orthogonal groups.

Consider a dihedral subgroup of order $2(q+1)$ which acts trivially on a subspace of codimension 2. Note that any hyperplane not containing the 1-dimensional socle is fixed by one of the $q+1$ transvections in the dihedral group (consider the dual representation and the corresponding statement about vectors). Now given any $g \in G$, g is conjugate to an element in $O^{\pm}(2m, q)$ and so fixes a complementary hyperplane to the socle. Thus, $\langle g, t \rangle$ fixes this hyperplane for some transvection t among the $q+1$ given. This completes the proof. ∎

3. Explicit bounds

Some upper bounds on $s(G)$ for certain simple groups G were already provided in the previous section. In this section we look more closely at upper bounds and lower bounds for all infinite families of finite simple groups.

3.1. Alternating groups

We first consider alternating groups of non prime degree. We formulate a lower bound in terms of $p(n)$, though the proof below provides more refined bounds (in terms of the arithmetic properties of n).

Proposition 3.1. *Let n be a composite positive integer. Then $s(A_n) \geq cp(n) \log p(n)$.*

Proof. By the proof of [9, 7.6] there exists a constant c_1 such that

$$PC(A_n) \geq \prod_{p|n}(1-1/p^2) - c_1/n.$$

This yields (using $1-x \geq e^{-2x}$ for $0 \leq x \leq 1/2$)

$$PC(A_n) \geq e^{-2\sum_{p|n} p^{-2}} - c_1/n \geq e^{-2\sum_{p \geq p(n)} p^{-2}} - c_1/n,$$

where p ranges over primes. Using $1-e^{-x} \leq x$ it now follows that

$$1 - PC(A_n) \leq c_1/n + 2\sum_{p \geq p(n)} p^{-2}.$$

Now, it is easy to see, using the Prime Number Theorem, that

$$\sum_{p \geq x} p^{-2} = \Omega((x \log x)^{-1}).$$

Since n is composite we have $n \geq p(n)^2$, and so

$$1 - PC(A_n) \leq c_1 p(n)^{-2} + c_2(p(n)\log p(n))^{-1} \leq c_3(p(n)\log p(n))^{-1}.$$

Combining this with 2.1 we obtain

$$s(A_n) \geq cp(n)\log p(n).$$ ∎

It would be interesting to close the gap between the bounds on $s(A_n)$ given in 2.4 and 3.1.

We now turn to alternating groups of prime degree, whose spread is considerably larger. The next result determines the spread almost exactly for A_n with n a generic prime.

Proposition 3.2. *Let $n > 23$ be a prime integer such that n is not of the form $(q^d-1)/(q-1)$ for any $d > 1$ and prime power q. If $r|(n-1)$, set $f(n,r) = (n-1)!/[(r-1)r^{(n-1)/r}((n-1)/r)!)]$. Then*

$$f(n,p) - 1 \leq s(A_n) \leq f(n,p) + 2,$$

where $p = p((n-1)/2)$.

Proof. Set $G = A_n$. Let p be the smallest prime divisor of $(n-1)/2$. Let T_1' be the set of subgroups of order p each fixing only 1 (and no other points). Choose a generator for each subgroup in T_1' and let T_1 be the set of those generators. Let T_2 be the set of 3 three cycles $(1,2,3),(2,3,4),(1,2,4)$. Set

$T=T_1\cup T_2$. We show that there is no element $y\in G$ such that $\langle x,y\rangle=G$ for all $x\in T$.

Let $y\in G$. If y is not an n-cycle, then y must consist of at least 3 cycles (since n is odd) and it easily follows that $\langle x,y\rangle$ is not transitive for some $x\in T_2$.

So suppose that y is an n-cycle. Let M be the normalizer of $\langle y\rangle$. Consider the stabilizer of 1 in M; it is cyclic of order $(n-1)/2$ and acts semiregularly. Thus, it contains some element of T_1. So $\langle x,y\rangle$ is proper for some $x\in T_1$.

Note that if $x,x'\in T_1\cap M^g$, then $x=x'$ (since there is a unique subgroup of M^g of order p fixing 1). Also $|T_1|=|x^G|/n(p-1)=f(n,p)$.

This implies that $s(A_n)\le f(n,p)+2$.

Conversely, it follows (cf. [9]) that M is the unique maximal subgroup containing y. Note that M is isomorphic to a nonabelian group of order $n(n-1)/2$.

Let $1\ne x\in M$ be of prime order r. Let $\mu(x)=|x^G\cap M|/|x^G|$. It is well known that $\mu(x)=\mathrm{fix}(x)/|G:M|$, where $\mathrm{fix}(x)$ is the set of fixed points of x on the cosets of M.

We need an upper bound for $\mu(x)$. If $r=n$, then $\mu(x)=1/(n-2)!$ (since x has a unique fixed point on the cosets of M). Otherwise, x has a unique fixed point in the natural representation and $|x^G\cap M|=(r-1)n$. So $\mu(x)=(r-1)n/[n!/r^{(n-1)/r}(n-1/r)!]=f(n,r)^{-1}$. This clearly is a maximum when $r=p$. Hence $\mu(x)\le f(n,p)^{-1}$.

Let T be a subset of G of cardinality less than $f(n,p)$ consisting of nonidentity elements. We will show that there exists an element z so that $G=\langle x,z\rangle$ for each $x\in T$. Without loss of generality, we may assume that each element of T has prime order. Then $\mu(x)\le f(n,p)^{-1}$ for all $x\in T$, and so the union of the sets of fixed points of the elements of T has cardinality less than $|G:M|$. It follows that $T\cap M^g$ is empty for some g, whence $G=\langle x,y^g\rangle$ for each $x\in T$. ∎

Note that when p is fixed and $n\to\infty$ the upper bound above is about $(n!)^{1-p^{-1}}\ge(n!)^{1/2}$. The spread is particularly large when $(n-1)/2$ is also prime in which case $f(n,p)=f(n,(n-1)/2)=n!/[n(n-3)(n-1)^2/4]$.

We now consider the primes $n>23$ not covered by the previous result (for smaller primes, there are some extra subgroups that one would need to consider). Note that the set of such of primes has density zero (it is unknown whether there are infinitely many such primes).

Given an odd positive integer n let b its residue modulo 4, and define

$$g(n)=\frac{n!}{[(n+b-4)/4]![(n+4-b)/2]!2^{(n+b-4)/4}}.$$

Note that $g(n)$ is the size of the smallest conjugacy class of involutions fixing less than $n/2$ points.

Let $h(n)$ be the size of the largest conjugacy class of involutions in A_n. So

$$h(n) = \frac{n!}{(n-2k)!k!2^k}$$

with $n-2k$ within 1 of $\sqrt{n+2}$).

Proposition 3.3. *Let $n>23$ be a prime integer of the form $(q^d-1)/(q-1)$ with q a prime power and $d\geq 2$. Then*

$$g(n)/(n(\log\log n)n^{\log n}) \leq s(A_n) \leq h(n)+2.$$

Proof. Let y be an n-cycle and let $G=A_n$. The only maximal subgroups containing y are the normalizer M of $\langle y\rangle$ and if $n=(q^d-1)/(q-1)$, then subgroups of the normalizer $R:=P\Gamma L(d,q)$ of $L_d(q)$.

Let $x\in PGL(d,q)$ be an involution which is trivial on a hyperplane (a transvection if q is even and a reflection if q is odd). Then x has $(q^{d-1}-1)/(q-1)$ fixed points if q is even $1+(q^{d-1}-1)/(q-1)$ fixed points if q is odd. Let $T=x^G\cup\{(1,2,3),(2,3,4),(1,2,4)\}$. Suppose that $z\in G$ generates with each element of T. As in the previous result, z must be an n-cycle, but then $\langle z,w\rangle$ is contained in a conjugate of $PGL(d,q)$ for some $w\in T$. Thus, $s(G)\leq |x^G|+2=n!/t!2^{(n-t)/2}((n-t)/2)!+2\leq h(n)+2$, where t is the number of fixed points of x.

If x is any element of prime order r conjugate to an element of R with t fixed points, then

$$|x^G\cap R|/|x^G| < |R|/|x^G| \leq n^{\log n}t!r^{(n-t)/r}((n-t)/r)!/n!.$$

Using the fact that $t<n/q\leq n/2$ [9], we see that

$$|x^G\cap R|/|x^G| < n^{\log n}t!2^{(n-t)/2}((n-t)/2)!/n!.$$

Maximizing over t yields

$$|x^G\cap R|/|x^G| < n^{\log n}/g(n).$$

The total number of maximal subgroups containing a given n-cycle is at most $1+\sum_d(n-1)/d$, where the sum is over all possible d occurring (for a given d (which determines q), there are at most $(n-1)/d$ possible subgroups of the $P\Gamma L(d,q)$ containing a given n-cycle). Since $d<\log n$ and d is prime (because $q^d-1)/(q-1)$ is prime), it follows there are at most $n\log\log(n)$ maximal subgroups containing a given n-cycle.

It thus follows that if y is a n-cycle, and $1 \neq x \in G$, the probability that a random conjugate of x fails to generate together with y is less than $n(\log\log(n))n^{\log n}/g(n)$.

Of course, this is the same probability that fixing x, a random conjugate of y fails to generate with x. In particular, if $s < g(n)/(n(\log\log n)n^{\log n})$ and $x_i, 1 \leq i \leq s$ are nontrivial elements of G, the probability that y fails to generate with at least one of the x_i is less than 1. This proves the lower bound. ∎

The result above can be improved slightly by keeping track of what the possible values of q are above. When $q = 2$ and n is a Mersenne prime, our estimates are fairly accurate. In that case the spread is asymptotically $(n!)^{1/4}$. With a bit more careful analysis one can improve the lower bound in 3.3 to $g(n)/n^{\log n}$.

3.2. Odd dimensional orthogonal groups

The odd dimensional orthogonal groups behave differently than the other groups of Lie type. This includes $Sp(2m,q) = \Omega(2m+1,q)$ for q even. The reason is that any element fixes some vector in the orthogonal representation of dimension $2m+1$.

Proposition 3.4. *Let $G = \Omega(2m+1,q)$ with q odd and $m \geq 2$. Suppose $(m,q) \neq (2,3)$, then $s(G) \geq q-1$.*

Proof. Assume that we choose V so that the corresponding quadratic form preserved has square discriminant (we say of $+$ type). Let $g \in G$ be the element of maximal order acting irreducibly on a hyperplane (of $-$ type). By [12], except for the one case omitted, the only maximal subgroup of G containing g is the stabilizer of this hyperplane (or equivalently the 1-dimensional subspace orthogonal to it). Note that the total number of such hyperplanes is $N := q^m(q^m-1)/2$.

We need a slight refinement of the results in [9]. Let h be any nontrivial element of G. We wish to obtain a lower bound for the number $f(h)$ of hyperplanes of $-$ type fixed by h.

We claim that $f(h) \leq f(r)$ for $r \in G$ with $-r$ a reflection. Note that the total number of hyperplanes of $-$ type is $N := q^m(q^m-1)/2$. Also, note that $f(r) \leq 1 + q^{m-1}(q^m+1)/2$.

Clearly, we may assume that h has prime order in G. If h has odd order, then we are just counting the number of 1-spaces of the appropriate type

in the fixed space U of h. Now no element of odd order in G is trivial on a hyperplane (this is clear for semisimple elements and G does not contain transvections). Thus the total number of 1 spaces (or hyperplanes) fixed by h is at most $(q^{2m-2}-1)/(q-1) < f(r)$.

If h has order 2, then the number of fixed 1-spaces of a given type is just the sum of the fixed 1-spaces in each of the 2 eigenspaces for h. A straightforward computation shows that the maximum is achieved when one of the eigenspaces is a hyperplane (by determinant, necessarily the -1 eigenspace). So the maximum is achieved when $-h$ is a reflection.

It follows that if $1 \neq h \in G$ and we choose a random element in the conjugacy class of g, the probability that $\langle h, g\rangle$ fix a hyperplane (or equivalently a 1-space) of given type is at most $f(r)/N < 1/(q-1)$. Thus, given $h_1, \ldots, h_{q-1}$ nontrivial elements in G, the probability that a randomly chosen conjugate of g fixes one of the $-$ type 1-spaces fixed by any of the h_i is at most $(q-1)f(r)/N < 1$. So choose a conjugate which fixes none of these 1-spaces. It follows by the result of [12] quoted above, that $G = \langle g, h_i\rangle$ for each i. ∎

We now turn our attention to the case of q even.

Proposition 3.5. *Let $G = Sp(2m,q) = \Omega(2m+1,q)$ with q even and $m \geq 2$.*
(i) *If q is sufficiently large, then $s(G) \geq q-3$.*
(ii) *If m is sufficiently large, then $s(G) = q$.*

Proof. Let V be the natural symplectic module for G. The proof of the symplectic case in [9] shows that there exists an element $g \in G$, so that if $1 \neq h \in G$, the probability that a conjugate of g together with h does not generate G is at most $1/q + 3/q^2$. Thus, if q is sufficiently large, some conjugate of g together with $h_i, 1 \leq i \leq q-3$ will generate. This proves (i).

If m is sufficiently large, then the proof in [9] shows that for a particular choice of g, the probability that h and a random conjugate of g fail to generate is at most $1/q + 13/q^{(2m-12)/8}$. Moreover, if h is not a transvection, this probability is at most $1/q^2 + 13/q^{(2m-12)/8}$. Thus, if $h_1, \ldots, h_q$ are nontrivial elements of G with e of the h_i transvections, the probability that a random conjugate of g together with some h_i fails to generate G is less than $e/q + (q-e)/q^2 + d/q^k < 1$ for m sufficiently large (here k tends to infinity with m) unless $e = q$, i.e. each of the h_i is a transvection.

So assume that $h_1, \ldots, h_q$ are transvections. Let $y \in G$ be an element of order $q^m + 1$ acting irreducibly on the natural symplectic module. The only maximal subgroup containing y and a transvection are conjugate to $O^-(2m,q)$ (for example, this follows by [13]). In the orthogonal represen-

tation of G, y fixes a unique hyperplane and so is contained in a unique conjugate H of $O^-(2m,q)$.

Set $N=|G:H|=q^m(q^m-1)/2$. The probability that a random transvection is in H is less than $1/q+1/q^m$ but greater than $1/q$ (or equivalently the probability that a random conjugate of H contains a fixed transvection). This implies that given any q transvections, at least 2 must be in a common conjugate of H. Thus, we may assume that h_1 and h_2 are contained in a common conjugate of H.

We certainly can find a 4-dimensional nonsingular subspace left invariant by $J:=\langle h_1,h_2\rangle$ with J trivial on its orthogonal complement.

Now $C_G(J)$ contains $Sp(2m-4,q)$ (the subgroup acting trivially on the 4-dimensional subspace). On the other hand, $C_G(J)\cap H\cong O^{\pm}(2m-4,q)$. Thus, $|C_G(J):C_H(J)|\geq q^{m-2}(q^{m-2}-1)/2$ and so J is contained in at least $q^{m-2}(q^{m-2}-1)/2$ conjugates of H (conjugate by an element in each of the cosets of $C_G(J)/C_G(H)$). Thus, the union of the fixed points of h_1 and h_2 on the cosets of H is at most $N(2/q+2/q^m-1/q^4+1/q^{m+2})$. Hence the union of the fixed points of all the h_i on the cosets of H is at most $N(1+1/q^{m-1}-1/q^4+1/q^{m+1})<N$. So we can find some conjugate of H not containing any of the h_i, whence $G=\langle y^g,h_i\rangle$ for some $g\in G$. This shows that $s(G)\geq q$. The result now follows by Proposition 2.5. ∎

3.3. Groups of Lie Type

In this section we will show that in many cases $q^{a\ell}<s(G)<q^{b\ell}$ where ℓ is the rank of G and a and b are positive constants (independent of ℓ and q). The lower bound follows from the proofs of the results in [9].

The groups of Lie type fall into several categories which explain their behavior – one needs to find a family of large subgroups containing every element (the notion of large is made specific below):

(i) Odd dimensional orthogonal groups (including $Sp(2m,q)$ with q even) – here every element leaves invariant a hyperplane;

(ii) $\Omega^+(2m,q)$ and $U(2m,q)$ — here every element has some nontrivial invariant subspace;

(iii) $Sp(2m,q),q$ odd, $\Omega^-(2m,q)$ – here every element either has a nontrivial invariant subspace or is contained in a rather large subgroup (a classical group of dimension m over the field of q^2 elements);

(iv) $L(m,q)$ and $U(m,q)$, m odd – here there exist elements which may live in no large subgroup; if g is an element acting irreducibly, the largest subgroup containing it will be a classical group of dimension m/p defined over the field of q^p elements where p is the smallest prime divisor of m.

The following is shown in [9]. The result there is not stated quite as precisely as this, but the proof immediately implies these statements.

Proposition 3.6. *Let G be a finite simple group of Lie type of rank ℓ defined over the field of q elements.*
(i) *There exist a constant c and an element $g \in G$ such that for any $1 \neq x \in G$, the probability that a random conjugate of g together with x does not generate G is $< c/q$;*
(ii) *if G is not isomorphic to $\Omega(2\ell+1,q)$ and $\ell > 10$, then there exists an element $g \in G$ such that for any $1 \neq x \in G$, the probability that a random conjugate of g together with x does not generate G is $< 20/q^{(\ell-6)/4}$.*

If G is a group of Lie type, let $W(G)$ denote its Weyl group. Note that $W(G)$ depends only on the type of G and not on q.

Lemma 3.7. *Let G be a simple finite group of Lie type of Lie rank ℓ defined over the field of q elements. Then $s(G) \leq d|G|/(q-1)^\ell$ for a positive constant d depending only on the type of G.*

Proof. Let S_0 be the conjugacy class of long root elements in G. The conjugacy classes of maximal tori of G are indexed by equivalence classes of elements of $W(G)$ (see [19]). Let S_i be a family of conjugacy classes such that at least one S_i intersects each maximal torus of G. Let $S = \cup S_i$. Let $g \in G$. Let M be a maximal subgroup of G containing g. If g is contained in a parabolic subgroup of G, then $\langle g, s\rangle \neq G$ for some $s \in S_0$. If g is not contained in any parabolic subgroup, then the centralizer of G contains no unipotent elements and so is a maximal torus. Thus, g centralizes some $s \in S$ and so again $\langle g, s\rangle \neq G$ for some $s \in S$. Note that $|S| \leq d|G|/(q-1)^\ell$ where $d-1$ is the number of conjugacy classes of maximal tori in G. ∎

The previous two results immediately yield:

Corollary 3.8. *Assume that G is a finite simple group of Lie type defined over the field of q elements with Lie rank $\ell \leq 10$. There exist positive constants c, d such that $q/c \leq s(G) \leq d|G|/q^\ell$.*

We note that one can be much more precise. We now consider the groups of Lie rank greater than 10.

Proposition 3.9. *Let G be a simple finite group of Lie type of Lie rank $\ell > 10$ not isomorphic to $\Omega(2\ell+1,q)$.*
(i) *$s(G) > q^{(\ell-6)/4}/20$.*

(ii) *If G is not isomorphic to $U(m,q)$ or $L(m,q)$ with m odd (in either case), then $s(G)<q^{8\ell}$.*

Proof. (i) follows from the result of [9] given above.

Since $\ell>8$, we know that G is classical group other than an odd dimensional unitary group or linear group. We may also assume that G acts irreducibly on its natural module V (as we have already dealt with $\Omega(2m+1,q)$ with q even).

Let S be the conjugacy class of long root elements. Note that $|S|<q^{4\ell}$. Suppose that $g\in G$ has a nontrivial invariant subspace. Then it must leave invariant a nonsingular subspace or a totally singular subspace. Since $\ell>10$ is sufficiently large, any such subspace is left invariant by a long root element and so g together with some element of S cannot generate.

Suppose that g acts irreducibly. So G is isomorphic to one of $G=L(2m,q),U(2m,q),Sp(2m,q)$, or $\Omega^-(2m,q)$. In each case g is contained in a classical subgroup of dimension m defined over the field of q^2 elements. Let S' denote the conjugacy class of G containing a long root element of this m-dimensional classical group. One easily computes that $|S'|+|S|<q^{8\ell}$.

Thus, we see that there is no element $g\in G$ such that $G=\langle g,s\rangle$ for all $s\in S_1\cup S_2$. ∎

We now turn to the two remaining cases – $L(m,q)$ and $U(m,q)$. The spread for these cases behaves very much like alternating groups – it depends on the smallest prime dividing m. In case $G=L(m,q)$, a lower bound for $s(G)$ was determined in [2]. We provide upper and lower bounds in both cases. Our lower bound is not as precise as that given in [2].

Proposition 3.10. *Let $G=L(m,q)$ or $U(m,q)$. Let p denote the smallest prime divisor of m. There exist positive constants a and b such that $q^{apm}<s(G)<q^{bpm}$.*

Proof. By the previous result, we may assume that m is odd.

We first prove the upper bound. Let S be the conjugacy class of transvections in G. Let H be the subgroup of G containing $L(m/p,q^p)$ or $U(m/p,q^p)$. Let S' be the conjugacy class of G containing the transvections in this smaller classical group.

Precisely as in the previous result, we see that $s(G)<|S|+|S'|$. An easy calculation shows that $|S|+|S'|<q^{4pm}$.

We now prove the lower bound. We only give the proof in the unitary case. The proof for the linear case is identical but also follows from Theorem 1 of [2].

Let $g \in U(m,q)$ of order $(q^m+1)/(q+1)$ acting irreducibly on the natural module (this exists for m odd). It follows from [12] (with a small number of exceptions) that the maximal overgroups of g are precisely the normalizers of $U(m/r,q^r)$ where r is a prime dividing m. These are also the normalizers of certain subgroups of the centralizer of g (in $GL(m,q)$). There is precisely one for each prime divisor r. Denote these subgroups by $H(r)$. So $H(r)$ is a subgroup of $GU(m/r,q^r).r$ (viewed in the linear group).

Let $x \in H(r)$. Let x^G denote the conjugacy class of x. We want to obtain upper bounds for $f(x) = f_r(x) := |x^G \cap H(r)|/|x^G|$. If x is not conjugate to an element of H, then $f(x) = 0$. We may assume that x has prime order in G. If $x \in GU(m/r,q^r)$, then we see either that each irreducible x-submodule of the natural module for G occurs a multiple of r times. This gives a lower bound for $C_G(x)$ and shows that $|x^G| < q^{crm}$ for some constant c (independent of r and m). If x is not conjugate to an element of $GU(m/r,q^r)$, then x must have order r and by Lang's theorem is conjugate to the standard field automorphism of order r (note r is odd) of $GU(m/r,q^r)$ and moreover all such elements are conjugate in $GU(m/r,q^r)$ (cf. [8, §7]). If r does not divide q, then this implies that each eigenvalue for x (over the algebraic closure) occurs with multiplicity m/r, while if r does divide q, then x has exactly m/r Jordan blocks of size r. In either case, we see that $|x^G| < q^{crm}$ as well. It follows by [17] that there is a constant ϵ (roughly $1/4$ at least for m large) so that $f(x) < |x^G|^{-\epsilon} < q^{-a'rm}$ for some positive constant a'.

It follows that $PC(G) > 1 - \sum_{r|m} q^{-a'rm}$ where the sum is over all primes dividing m (for take g to be as above; given any nontrivial $x \in G$, it follows that a random conjugate of x together with g generates unless this conjugate is in one of the $H(r)$ and the probability of that happening is $f_r(x)$). Note that

$$\sum_{r|m} q^{-a'rm} < \int_p^\infty q^{-a'xm} dx = a'm(\ln q) q^{-a'mp} < q^{-amp},$$

for some positive constant a. Thus, $PC(G) > (1 - q^{-amp})$ and the result now follows by Lemma 2.1. ∎

References

[1] L.B. Beasly, J.L. Brenner, P. Erdős, M. Szalay and A.G. Williamson: Generating alternating groups by pairs of conjugates, *Period. Math. Hungar.* **18** (1987), 259–269.

[2] A.A. Bereczky: On the density of generating pairs in projective special linear groups and projective symplectic groups in odd characteristic, Ph.D. Thesis, U. Florida, 1999.

[3] G. Binder: The bases of the symmetric group, *Izv. Vyss. Ucebn. Zaved. Matematika* **78** (1968), 19–25.
[4] G. Binder: The two-element bases of the symmetric group, *Izv. Vyss. Ucebn. Zaved. Matematika* **90** (1970), 9–11.
[5] J.L. Brenner and James Wiegold: Two-generator groups I, *Michigan Math. J.* **22** (1975), 53–64.
[6] J.L. Brenner and James Wiegold: Two-generator groups II, *Bull. Austral. Math. Soc.* **22** (1980), 113–124.
[7] J.L. Brenner, R.M. Guralnick and J. Wiegold: Two-generator groups III, *Contemp. Math.* **33** (1984), 82–89.
[8] D. Gorenstein and R. Lyons: The local structure of finite groups of characteristic 2-type, *Memoirs, Amer. Math. Soc.* **42** (1983), vol. 276.
[9] R.M. Guralnick and W.M. Kantor: Probabilistic generation of finite simple groups, *J. Algebra* **234** (2000), 743–792.
[10] R.M. Guralnick, W.M. Kantor and J. Saxl: The probability of generating a classical group, *Comm. in Algebra* **22** (1994), 1395–1402.
[11] R.M. Guralnick, M.W. Liebeck, J. Saxl and A. Shalev: Random generation of finite simple groups, *J. Algebra* **219** (1999), 345–355.
[12] R.M. Guralnick, T. Penttila, C.E. Praeger and J. Saxl: Linear groups with orders having certain primitive prime divisors, *Proc. London Math. Soc.* **78** (1999), 167–214.
[13] W.M. Kantor: Subgroups of classical groups generated by long root elements, *Trans. Amer. Math. Soc.* **248** (1979), 347–379.
[14] W.M. Kantor and A. Lubotzky: The probability of generating a finite classical group, *Geom. Ded.* **36** (1990), 67–87.
[15] M.W. Liebeck and A. Shalev: The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103–113.
[16] M.W. Liebeck and A. Shalev: Classical groups, probabilistic methods, and the (2,3)-generation problem, *Annals of Math.* **144** (1996), 77–125.
[17] M.W. Liebeck and A. Shalev: Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520.
[18] J. Saxl and G. Seitz: Subgroups of algebraic groups containing regular unipotent elements, *J. London Math. Soc.* (2) **55** (1997), 370–386.
[19] T.A. Springer and R. Steinberg: Conjugacy classes, in Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69) pp. 167–266, Lecture Notes in Mathematics, Vol. 131 Springer, Berlin, 1970.
[20] G. Szekeres: On a certain class of metabelian groups, *Annals of Mathematics* **49** (1948), 43–52.

Robert M. Guralnick

Department of Mathematics
University of Southern California
Los Angeles, CA 90089-1113, USA
guralnic@math.usc.edu

Aner Shalev

Institute of Mathematics
Hebrew University
Jerusalem 91904, Israel
shalev@math.huji.ac.il