WILLIAM M. KANTOR AND ALEXANDER LUBOTZKY

THE PROBABILITY OF GENERATING A FINITE CLASSICAL GROUP

For Jacques Tits on his sixtieth birthday

ABSTRACT. Two randomly chosen elements of a finite simple classical group G are shown to generate G with probability $\to 1$ as $|G| \to \infty$. Extensions of this result are presented, along with applications to profinite groups.

1. INTRODUCTION

If two elements are chosen at random from a finite simple group G, will they probably generate G? Intuition strongly suggests that the answer is 'yes'. The purpose of this paper is to prove that intuition is correct, at least in the case of a classical group G. The case of alternating groups is a beautiful result due to Dixon [11], who also asked whether the corresponding result is true for all finite simple groups. However, whereas his theorem is proved using nineteenth-century results concerning permutation groups, the proof of our result unfortunately uses the classification of finite simple groups.

We will prove the following:

THEOREM. *Let G_0 denote a finite simple classical group, and let $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$. If $P(G)$ is the probability that two randomly chosen elements of G do* **not** *generate a group containing G_0, then $P(G) \to 0$ as $|G| \to \infty$.*

The proof consists of one crude estimate for $P(G)$ (see (*) in Section 2), followed by a fairly standard use of the results in [1] (similar to that in [21]). On the whole, the proof is less informative than the result itself. In Section 2 we will consider the (marginally easier) case of $\mathrm{PSL}(V)$, and in Section 3 that of the remaining classical groups. In Section 4 we note that the theorem continues to hold for the groups ${}^2B_2(q)$, ${}^2G_2(q)$, $G_2(q)$, ${}^3D_4(q)$ and $E_6(q)$. Thus, only the groups ${}^2F_4(q)$, $F_4(q)$, ${}^2E_6(q)$, $E_7(q)$ and $E_8(q)$ remain to be considered.

In Sections 5–7 we consider situations involving direct products of simple groups. First, in Section 5 we discuss the evaluation of $P(G)$ for a finite group G that is a product of nonabelian finite simple groups. Methods similar to those in that section are then used in Section 6 in order to answer a question posed by Fried and Jarden [12] concerning the probability of generating free *profinite* groups. The Theorem is not used in Sections 5 or 6. Finally, Section

Research by W.M.K. was supported in part by the NSF and the NSA; and research by A.L. was supported in part by the BSF.

Geometriae Dedicata **36**: 67–87, 1990.

7 studies the probability of generating some special types of profinite groups by translating results about the rate of convergence of $P(G)$ to 0 when $|G| \to \infty$ obtained in the course of the proof of the theorem.

2. Proof of theorem: PSL(V) case

The case of PSL(V) is slightly easier than that of the remaining classical groups, and will be presented first. Section 3 contains the modifications required for the remaining classical groups.

Write $G_0 = \mathrm{PSL}(V) = \mathrm{PSL}(n, q)$, and let $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0) = \mathrm{P\Gamma L}(V)\langle\tau\rangle$, where τ is the inverse transpose map.

Consider $g, h \in G$. Clearly, $\langle g, h\rangle$ does not contain G_0 if and only if it is contained in a subgroup L of G maximal with respect to this property. Since $\Pr(g, h \in L) = (|L|/|G|)^2$,

$$(*) \qquad P(G) \leqslant \sum \left(\frac{|L|}{|G|}\right)^2 \leqslant \sum \left(\frac{|L|}{|G|}\right)^2 \cdot \left(\frac{|G|}{|L|}\right) = \sum \frac{|L|}{|G|}$$

where the last two sums are over representatives L of conjugacy classes of all the subgroups of G maximal with respect to not containing G_0.

By [1], each group L falls into one of the following classes of subgroups of G:

- $\mathbf{C}_1$: The stabilizer of a subspace of V, or (if G is not contained in $\mathrm{P\Gamma L}(V)$) of a pair of subspaces V_1, V_2 such that $\dim V_1 + \dim V_2 = n$ and either $V_1 \subseteq V_2$ or $V = V_1 \oplus V_2$.
- $\mathbf{C}_2$: The stabilizer of a direct sum decomposition $V = \oplus V_i$ for V_i of the same dimension.
- $\mathbf{C}_3$: The stabilizer of a field extension of $\mathbb{F}_q$ whose degree is a prime dividing n.
- $\mathbf{C}_4$: The stabilizer of a tensor product decomposition $V = V_1 \otimes V_2$.
- $\mathbf{C}_5$: The centralizer of a field automorphism.
- $\mathbf{C}_6$: The normalizer of a symplectic-type r-group for a prime $r \neq p$ (in an irreducible representation).
- $\mathbf{C}_7$: The stabilizer of a tensor product decomposition $V = \otimes V_i$ for V_i of the same dimension.
- $\mathbf{C}_8$: A classical subgroup embedded as usual.
- $\mathbf{C}_9$: $L = N_G(S)$, where S is a nonabelian simple subgroup of PSL(V) such that $S \leqslant L \leqslant \mathrm{Aut}(S)$, and the universal cover $\tilde{S}$ of S acts absolutely irreducibly on V in a representation defined over no proper subfield of $\mathbb{F}_q$. (Here, $\tilde{S}$ is the largest perfect group which, modulo its center, is isomorphic to S.)

By [21, Theorem – or, more precisely, (4.1)], $|L| \leqslant k := q^{3n}$ for L in $\mathbf{C}_9$. On the other hand, in [1, §1] there is a thorough discussion of the conjugacy classes of subgroups L of types $\mathbf{C}_1$–$\mathbf{C}_8$, from which it follows that the numbers of conjugacy classes are bounded above as follows:

$\mathbf{C}_1$: $2n$
$\mathbf{C}_2$, $\mathbf{C}_3$, $\mathbf{C}_4$: n (an upper bound on the number of divisors of n)
$\mathbf{C}_5$: $\log q$ (where, throughout this paper, logarithms are always to the base 2)
$\mathbf{C}_6$: 1
$\mathbf{C}_7$: $\log n$
$\mathbf{C}_8$: 4.

In each case, $|G:L| \geqslant \frac{1}{2}q^{n-1}$. Since $|G| > \frac{1}{2}q^{n^2-1}/n$, (*) becomes (with Σ' denoting the sum over $\mathbf{C}_1$–$\mathbf{C}_8$ and Σ_9 denoting the sum over $\mathbf{C}_9$)

$$(**) \qquad P(G) \leqslant \sum \frac{|L|}{|G|} = \sum{}' \frac{|L|}{|G|} + \sum_9 \frac{|L|}{|G|}$$

$$\leqslant \frac{\{5n + \log q + 1 + \log n + 4\}}{\frac{1}{2}q^{n-1}} + \frac{2n(\Sigma_9 |L|)}{q^{n^2-1}}.$$

The first term is negligible, so consider the second one. Recall that $|L| \leqslant k$ for L in $\mathbf{C}_9$.

The number of possible simple groups S of a given order $s \leqslant k$ is itself $\leqslant 2$ (by the classification of finite simple groups). Fix such a simple group S. The number of (equivalence classes of) absolutely irreducible projective representations of S in characteristic p is at most $|\tilde{S}|$, where $|\tilde{S}| \leqslant |S| \log |S|$. For each such representation, maximality forces L to be the normalizer of (the image of) S; and L is isomorphic to a subgroup of $\mathrm{Aut}(S)$ containing S, so that $|L| \leqslant |S| \log |S|$. (All of these estimates are very crude: slightly less crude ones are used in Lemmas 1 and 3 below.) Thus,

$$\sum_9 |L| \leqslant \sum_{s \leqslant k} \sum_{|S| = s} \sum_{\text{representations of } S} |L|$$

$$\leqslant k \cdot 2 \cdot k \log k \cdot k \log k \leqslant 2(q^{3n})^3 (\log q^{3n})^2,$$

so that, if $n \geqslant 10$, then

$$\frac{2n(\Sigma_9 |L|)}{q^{n^2-1}} \leqslant \frac{4n \cdot q^{9n}(3n \log q)^2}{q^{n^2-1}} \leqslant \frac{36n^3(\log q)^2}{q^{n-1}} \to 0$$

as $|G| \to \infty$.

This proves the Theorem for $n \geqslant 10$. The remaining cases can be handled by slightly sharpening some of the above estimates in order to handle

dimensions $n \geqslant 8$, and then referring to existing lists of subgroups of $\mathrm{SL}(n, q)$ for $n \leqslant 7$. However, since a better approach will be needed for the remaining classical groups, we present it here in preparation for the next section.

LEMMA 1. *If n is restricted to be at most 9, then $P(G) \to 0$ as $|G| \to \infty$.*

Proof. The only cases needing comment are those in $\mathbf{C}_9$ (i.e., the terms in $\Sigma_9 |L|/|G|$), when L has a simple normal subgroup S such that V is an absolutely irreducible projective S-module.

If S is an alternating group A_m then $9 \geqslant n \geqslant m - 2$ [28], so that there are $O(1)$ terms of this sort. Of course, there are $O(1)$ terms with S sporadic.

Thus, we may assume that S is a group of Lie type defined over $\mathbb{F}_r$ for some prime power r. Let $l = l(S)$ denote the absolute rank of S and $\tilde{S}$ (i.e., the rank of the corresponding algebraic groups over an algebraic closure of $\mathbb{F}_r$), unless S is ${}^2B_2(r)$, ${}^2G_2(r)$ or ${}^2F_4(r)$, in which case let $l(S)$ denote the relative rank of S (namely, 1, 1 or 2 respectively). Since $n \leqslant 9$ there are $O(1)$ terms in which $(q, r) = 1$, by [20]. (Namely, that paper shows that, with $O(1)$ exceptions, $9 \geqslant n \geqslant \frac{1}{2}r^{l/2}$. More precisely, there are fewer than 20 exceptional groups S, each contributing $< 5 \cdot 10^8/|G|$ to $\Sigma |L|/|G|$.)

This leaves the case of terms $|L|/|G|$ in which L has a simple normal subgroup S whose characteristic p is that of G. Write $r = p^a$ and $q = p^b$. Then

$$n \geqslant m^{a/(a,b)}$$

by [21, (2.1)–(2.2)], where $m = m(S)$ is defined to be the smallest degree of a faithful, irreducible, projective $\tilde{S}$-module over an algebraically closed field of characteristic p. As $9 \geqslant n \geqslant m$, S is either a classical group or $G_2(q)$, ${}^2G_2(q)$, ${}^2B_2(q)$ or ${}^3D_4(q)$ (since $m \geqslant 25$ for the groups $F_4(r)$, ${}^2F_4(r)$, $E_6(r)$, ${}^2E_6(r)$, $E_7(r)$ and $E_8(r)$; cf. [21]).

Since $p^a = r \leqslant |S| \leqslant q^{3n} \leqslant p^{27b}$, there are at most $27b$ possibilities for $r = p^a$. Also, $9 \geqslant n \geqslant m \geqslant l$; while each choice of p^a and l produces at most seven groups S up to isomorphism (there are at most seven groups of Lie type of a given rank over a given field), so there are $O(b)$ possible groups S. Fix one of them. Table I gives values of m, l, δ and M, where $M = M(S)$ has been chosen so that $|S| \leqslant 2r^M$ (required here) and $r^M/2m \leqslant |S|$ (required in Section 3) hold (note that, in the table, $M \leqslant m^2 - 1$ and $l \leqslant m - 1$ in every case), while δ is such that there are exactly $r^{\delta l}$ inequivalent absolutely irreducible $\tilde{S}$-modules in characteristic p [26]. In particular, there are at most $r^{\delta l}$ conjugacy classes of subgroups of G isomorphic to S. Fix one such subgroup and temporarily identify it with S. We have $L = N_G(S)$. Since $S \leqslant L \leqslant \mathrm{Aut}(S)$, $|L| = O(a \cdot |S|)$.

TABLE I

S	$l(S)$	$m(S)$	$M(S)$	δ
$\mathrm{PSL}(m, r)$, $m \geqslant 2$	$m-1$	m	m^2-1	1
$\mathrm{PSp}(2k, r)$, $k \geqslant 2$	k	$2k$	$\frac{1}{2}(m^2+m)$	1
$\mathrm{P\Omega}(2k+1, r)$, r odd, $k \geqslant 3$	k	$2k+1$	$\frac{1}{2}(m^2+m)$	1
$\mathrm{P\Omega}^+(2k, r)$, $k \geqslant 4$	k	$2k$	$\frac{1}{2}(m^2-m)$	1
$\mathrm{P\Omega}^-(2k, r)$, $k \geqslant 4$	k	$2k$	$\frac{1}{2}(m^2-m)$	2
$\mathrm{PSU}(m, r)$, $m \geqslant 3$	$m-1$	m	m^2-1	2
${}^2B_2(r)$	1	4	5	1
${}^2G_2(r)$	1	7	7	1
$G_2(r)$	2	$5+(2, r-1)$	14	1
${}^3D_4(r)$	4	8	28	3

Verification of column 4 of this table is an elementary exercise using the orders of the various groups [13, p. 491].

Thus, each of the $O(b)$ simple groups S contributes $O(a|S|\cdot r^{\delta l}/|G|)$ to the sum $\Sigma_9 |L|/|G|$. Here,

$$\frac{|S|\cdot r^{\delta l}}{|G|} \leqslant \frac{2r^M r^{\delta l}}{q^{n^2-1}/2n} = 4np^{a(M+\delta l)-b(n^2-1)}.$$

First assume that $S = {}^3D_4(r)$. Then $\delta = 3$, $l = 4$, $9 \geqslant n \geqslant m^{a/(a,b)} = 8^{a/(a,b)}$, and hence $a/(a,b) = 1$, so that $a \mid b$. Consequently, $4np^{a(M+\delta l)-b(n^2-1)} \leqslant 4np^{40a-80b} \leqslant 4nq^{-40}$ for this particular S.

Now we may assume that $\delta \leqslant 2$.

We claim that $|S|\cdot r^{\delta l}/|G| \leqslant 4np^{-(n-1)b} = 4nq^{-(n-1)}$. In fact, we will show that $4np^{a(M+\delta l)-b(n^2-1)} \leqslant 4np^{-(n-1)b}$. For, since $l \leqslant m-1$ and $M \leqslant m^2-1$, we have

$$\frac{b}{a}(n^2-1-(n-1))-(M+\delta l) \geqslant \frac{b}{(a,b)}\,\frac{m^{2a/(a,b)}-m^{a/(a,b)}}{(a,b)/a} - (m^2-1+\delta(m-1)).$$

If $\delta = 1$ then the right side is $\geqslant (m^2-m)-(m^2-1+2(m-1)) > 0$. So assume that $\delta = 2$ (so that, in particular, $m \geqslant 4$). Then the right side is $\geqslant 0$ if $a/(a,b) \geqslant 2$, or if $a = (a,b)$ but $b/(a,b) \geqslant 2$. This leaves us with the case $a = b$, so that $q = r$. Then

$$\frac{b}{a}(n^2-n)-(M+\delta l) \geqslant (n^2-n)-(m^2-1+2(m-1))$$

$$= n^2-(m+1)^2+3,$$

and this is positive unless $n = m$. Finally, assume that $q = r$ and $n = m$. Then

S cannot be $\mathrm{PSU}(n, r)$ embedded in $\mathrm{P\Gamma L}(n, q)$, and hence $M = \frac{1}{2}(m^2 - m)$ and $l = \frac{1}{2}m$ by Table I (since $\delta = 2$). Now

$$\frac{b}{a}(n^2 - n) - (M + \delta l) = (m^2 - m) - (\tfrac{1}{2}(m^2 - m) + 2(\tfrac{1}{2}m)) \geqslant 0.$$

This proves the claim. Since $a = O(b) = O(\log q)$, it follows that each of the $O(b) = O(\log q)$ groups S contributes $O((\log q)q^{-(n-1)})$ to $\Sigma_9 |L|/|G|$, so that $\Sigma_9 |L|/|G| \to 0$ as $|G| \to \infty$. □

REMARK. Combining the various inequalities used above produces the (crude!) estimate $P(G) < 10^{10}n^3(\log q)^2/q^{n-1}$, which will be needed later (cf. Proposition 13).

3. The remaining classical groups

Now we consider all of the remaining classical groups. The argument is divided into two separate parts, according to whether the dimension n is large (at least 21) or small. These are handled in Lemmas 2 and 3, respectively.

First we note the following simple

REMARK. Let $H \leqslant \mathrm{GL}(V)$, and assume that H is absolutely irreducible on the $\mathbb{F}_q$-space V. If H preserves a nonsingular alternating, symmetric or hermitian form on V, then that form is uniquely determined up to scalars. If V has characteristic 2 and H preserves a quadratic form on V, then that form is uniquely determined up to scalars.

Proof. The first assertion is standard. For the second, assume that f and g are H-invariant quadratic forms on V having the same associated bilinear form. Then it is elementary to check that $f - g$ is a semilinear map $V \to \mathbb{F}_q$ relative to the squaring automorphism of $\mathbb{F}_q$, and the kernel of this map is H-invariant. Thus, $f - g = 0$, so that $f = g$ and f is unique up to scalars since the associated bilinear form is. □

Now let G_0 denote a finite simple symplectic, orthogonal or unitary group, defined on a vector space V of dimension n over $\mathbb{F}_q$ (or $\mathbb{F}_{q^2}$ if G_0 is unitary), where we assume that G_0 is not isomorphic to any group of the form $\mathrm{PSL}(n', q')$. If q is even, $2n > 4$ and G_0 is $\mathrm{P\Omega}(2n + 1, q)$ we will view G_0 as the isomorphic group $\mathrm{Sp}(2n, q)$. In all other cases we may assume that G_0 is not isomorphic to a classical group of smaller dimension (thus, we are excluding $\mathrm{P\Omega}(5, q)$, which is isomorphic to $\mathrm{PSp}(4, q)$, as well as the related cases $\mathrm{P\Omega}^+(6, q) \cong \mathrm{PSL}(4, q)$ and $\mathrm{P\Omega}^-(6, q) \cong \mathrm{PSU}(4, q)$; cf. [7]). In particular, if G is an orthogonal group then we will assume that $n \geqslant 7$.

Let G denote a group satisfying $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$.

LEMMA 2. *If n is restricted to be at least* 21, *then* $P(G) \to 0$ *as* $|G| \to \infty$.

Proof. Inequality (*) still holds, and by [1] there are still classes $\mathbf{C}_1$–$\mathbf{C}_9$, but with further conditions on the various subspaces and subgroups involved. For example, subspaces are either totally singular or nonsingular, and many of the direct sum decompositions are orthogonal decompositions, all of which contribute additional cases.

If L is in one of these new classes $\mathbf{C}_1$–$\mathbf{C}_8$ then it is easy to check that $|G:L| \geqslant \frac{1}{2}q^{l(G)}$. In view of the description of the conjugacy classes in $\mathbf{C}_1$–$\mathbf{C}_8$ found in [1, §1] the following analogue of (**) continues to hold:

$$(***) \qquad P(G) \leqslant \sum \frac{|L|}{|G|} = \sum{}' \frac{|L|}{|G|} + \sum_{9} \frac{|L|}{|G|}$$

$$\leqslant \frac{3\{5n + \log q + 1 + \log n + 4\}}{\frac{1}{2}q^{l(G)}} + \sum_{9} \frac{|L|}{|G|}$$

Note that $\Sigma_9 |L|/|G|$ will involve a somewhat smaller denominator than in the previous section: we will use the estimate $|G| \geqslant q^{M(G_0)}/2n$, where $M(G_0)$ is listed in Table I.

By [21], it is still true that $|L| \leqslant (q^2)^{3n}$ in the unitary case, but the inequality $|L| \leqslant q^{3n}$ is no longer true for the remaining classical groups G, because there is a further type of subgroup that must be considered:

E: $S_k < \mathrm{PO}^{\pm}(n, p)$ for $p \neq 2$ and either $n = k + 1 \equiv 1 \pmod p$ or $n = k + 2 \equiv 2 \pmod p$; $S_{4k+2} < \mathrm{PO}(4k + 1, 2)$, $S_{8k+1} < \mathrm{PO}^{+}(8k, q)$, $S_{8k} < \mathrm{PO}^{+}(8k + 2, 2)$, $S_{8k+4} < \mathrm{PO}^{-}(8k + 2, 2)$, and $S_{8k+5} < \mathrm{PO}^{-}(8k + 4, q)$.

In each case there is a unique class of subgroups of the indicated type. Of course, there are additional cases produced by the listed ones, namely embeddings of alternating groups obtained by intersecting each of the above embeddings with the appropriate simple group $\mathrm{P}\Omega(V)$.

For each of the cases in **E** it is straightforward to check that $|L|/|G| \leqslant q^{-l(G)}$. Thus, **E** contributes at most $q^{-l(G)}$ to (***).

Write $\mathbf{C}_{9'} = \mathbf{C}_9 - \mathbf{E}$, and let $\Sigma_{9'}$ denote the sum over representatives of conjugacy classes of the groups in $\mathbf{C}_{9'}$. If G is not unitary then, once again, $|L| \leqslant q^{3n}$ for L in $\mathbf{C}_{9'}$; write $k = q^{3n}$ in this case, and $k = q^{6n}$ in the unitary case. Now we can proceed exactly as before in order to obtain that $\Sigma_{9'} |L|/|G| \leqslant k \cdot 2 \cdot k \log k \cdot k \log k/|G|$. If G is not unitary then the right side is $\leqslant 2(q^{3n})^3(\log q^{3n})^2/(q^{(n^2-n)/2}/2n)$ (cf. Table I); while if G is unitary then the right side is $\leqslant 2(q^{6n})^3(\log q^{6n})^2/(q^{n^2-1}/2n)$. In any case, if $n \geqslant 21$ then $\Sigma_{9'} |L|/|G| = O(n^3(\log q)^2 q^{-n+1})$, so that $\Sigma_{9'} |L|/|G| \to 0$ as $|G| \to \infty$. □

LEMMA 3. *If n is restricted to be at most* 20, *then* $P(G) \to 0$ *as* $|G| \to \infty$.

Proof. We will assume until near the end of the proof that $G \leqslant \mathrm{P\Gamma L}(V)$ (which will be the case except, perhaps, if G_0 is $\mathrm{PSp}(4, 2^b)$ or $\mathrm{P\Omega}^+(8, q)$). Proceeding as in Lemma 1, we find that the only cases needing comment are those in $\mathbf{C}_{9'}$, when L has a simple normal subgroup S whose universal cover $\tilde{S}$ acts absolutely irreducibly on V.

If S is alternating, sporadic, or of Lie type in characteristic different from p, then (as in Lemma 1) there are only $O(1)$ groups S and L to consider, and hence $O(1)$ absolutely irreducible $\tilde{S}$-representations. Each such representation leaves invariant at most one nonsingular alternating, quadratic or hermitian form, up to scalar multiplication (by the Remark). Hence, these groups S contribute $O(1)$ terms to $\Sigma_{9'} |L|/|G|$, and hence contribute $O(1/|G|)$ to $P(G)$.

This leaves the case of terms $|L|/|G|$ in which L has a simple normal subgroup S of Lie type defined over $\mathbb{F}_r$ for some power r of p. If $m = m(S)$, $l = l(S)$, a and b are as before, then $20 \geqslant n \geqslant m^{a/(a,b)} \geqslant m$ by [21, (2.1)–(2.2)]. Moreover, if S is not classical then it is ${}^2B_2(r)$, ${}^2G_2(r)$, $G_2(r)$ or ${}^3D_4(r)$ (since $m \geqslant 25$ for the groups $F_4(r)$, ${}^2F_4(r)$, $E_6(r)$, ${}^2E_6(r)$, $E_7(r)$ and $E_8(r)$; cf. [21]).

As in Lemma 1 we have $r \leqslant |S| \leqslant k^{3n} \leqslant q^{3 \cdot 6n} \leqslant q^{360}$, so that there are at most $360b$ possibilities for r, and hence there are $O(b)$ possible groups S. Fix S. Let δ be as before, so that there are $r^{\delta l}$ absolutely irreducible $\tilde{S}$-modules V to consider [26]. Each of them admits at most one $\tilde{S}$-invariant nonsingular alternating, quadratic or hermitian form, up to scalar multiplication (by the Remark).

Let M, m, l and δ be as in Table I, and let $M(G_0)$ and $l(G_0)$ be the corresponding quantities for G_0. Note that the table shows that

$$M(G_0) - l(G_0) \geqslant (\tfrac{1}{2}n^2 - \tfrac{1}{2}n) - \tfrac{1}{2}n = \tfrac{1}{2}n^2 - n.$$

We will show that *each of the $O(b)$ groups S contributes $O(n(\log q)^2 q^{-l(G_0)})$ to the sum* $\Sigma_{9'} |L|/|G|$.

Exactly as in Lemma 1, if $S = {}^3D_4(r)$ then $20 \geqslant n \geqslant m^{a/(a,b)} = 8^{a/(a,b)}$ implies that $a|b$. Moreover, $a \leqslant \frac{1}{2}b$: if $a = b$ then we would have $n \geqslant 24$ [21, (2.2)]. Now

$$40a - (M(G_0) - l(G_0))b \leqslant 40a - (\tfrac{1}{2}n^2 - n)b \leqslant 20b - 24b < 0,$$

so that

$$\frac{|S| \cdot r^{\delta l}}{|G|} \leqslant \frac{2r^M r^{\delta l}}{(q^{M(G_0)}/2n)} \leqslant 4np^{40a - M(G_0)b} < 4nq^{-l(G_0)}.$$

From now on we may assume that $\delta \leqslant 2$.

If $n = m$ then (cf. [21]) S lies in $\mathbf{C}_5$ (centralizing a field automorphism) or $\mathbf{C}_8$ (a classical group). We are assuming that this is not the case.

Thus, $n > m$.

There is one additional case we must single out: $S = \mathrm{P}\Omega(7, q)$, lying in $G_0 = \mathrm{P}\Omega^+(8, q)$ but acting irreducibly on the standard module. There is just one conjugacy class of such subgroups of G_0 (e.g., by [21] again). By considering $\mathrm{Aut}(S)/S$ as usual, we see that this group S contributes $O(24(\log q)|S|/|G|) = O((\log q)q^{-4})$ to the sum $\Sigma_{9'}\,|L|/|G|$.

Now we will proceed as in Lemma 1. Each of the $O(b)$ groups S contributes $O(a|S|\cdot r^{\delta l}/|G|)$ to the sum $\Sigma_{9'}\,|L|/|G|$. Here $|S|\cdot r^{\delta l}/|G| \leqslant 2r^M r^{\delta l}/|G| \leqslant 4nr^{M+\delta l}/q^{M(G_0)}$, and we will show that the right side is $\leqslant 4nq^{-l(G_0)}$. That is, we will show that

$$\Delta := \frac{b}{a}(M(G_0) - l(G_0)) - (M + \delta l) > 0$$

where we are assuming that $n > m$.

First suppose that $S = \mathrm{PSL}(m, r)$ or $\mathrm{PSU}(m, r)$. Then

$$\Delta \geqslant \frac{b}{a}(\tfrac{1}{2}n^2 - n) - (m^2 - 1 + 2(m-1))$$

$$\geqslant \tfrac{1}{2}\frac{b}{(a,b)}\,\frac{m^{2a/(a,b)} - 2m^{a/(a,b)}}{(a,b)/a} - (m^2 + 2m - 3).$$

If $a/(a,b) \geqslant 2$ then the right side is positive. Thus, we may assume that $a|b$.

By [21, (1.1)], $n \geqslant \frac{1}{2}m(m-1)$. If $m \geqslant 5$ then $n \geqslant \frac{1}{2}m(m-1) \geqslant 2m$, so that

$$\Delta \geqslant \frac{b}{a}(\tfrac{1}{2}n^2 - n) - (m^2 + 2m - 3) \geqslant 0.$$

It remains to consider the cases in which $m \leqslant 4$.

Let $m = 4$, so that $n \geqslant 6$. Then $\Delta \geqslant 2(\frac{1}{2}n^2 - n) - (m^2 + 2m - 3) \geqslant 0$ if $b/a \geqslant 2$, so assume that $b = a$. Similarly, we may assume that $n \leqslant 7$. If $n = 7$ then, by the table, $M(G_0) - l(G_0) = 7^2 - 7$ or $\frac{1}{2}(7^2 - 7)$, and hence $\Delta \geqslant 0$ again. Let $n = 6$. Then G_0 is not orthogonal (see the remarks preceding Lemma 2), so that G_0 is unitary or symplectic. In the unitary case $M(G_0) - l(G_0) = 6^2 - 6 > m^2 + 2m - 3$. So suppose that $G_0 = \mathrm{PSp}(6, q) > S = \mathrm{PSL}(4, q)$ or $\mathrm{PSU}(4, q)$. All irreducible subgroups of $\mathrm{PSL}(V)$ isomorphic to S are conjugate, and lie in an orthogonal group (cf. [21]). Now the Remark at the start of this section produces a contradiction.

If $m = 3$ then $\Delta \geqslant (b/a)(\frac{1}{2}n^2 - n) - 12$, so that we may assume that $n \leqslant 6$. Then once again G_0 is not orthogonal, so that $\Delta \geqslant (b/a)\frac{1}{2}(n^2 - n) - 12$. If now

$n = 6$ then $\Delta \geqslant 0$, so assume that $n \leqslant 5$. If $n = 5$ then G_0 must be unitary, in which case $\Delta \geqslant (n^2 - n) - 12 > 0$. If $n = 4$ then, for the same reason, we may assume that G_0 is not unitary, so that $G_0 = \mathrm{PSp}(4, q)$. However, this group contains neither $\mathrm{PSL}(3, q)$ nor $\mathrm{PSU}(3, q)$. Since $n > m$, this completes the discussion of the case $S = \mathrm{PSL}(m, r)$ or $\mathrm{PSU}(m, r)$.

Next suppose that $S = \mathrm{PSp}(m, r)$, or $S = \mathrm{P\Omega}(m, r)$ with $m \geqslant 7$. Then $\delta = 1$ and

$$\Delta \geqslant \frac{b}{a}(\tfrac{1}{2}n^2 - n) - (\tfrac{1}{2}m^2 + \tfrac{1}{2}m + \tfrac{1}{2}m) \geqslant \tfrac{1}{2}\frac{b}{(a,b)}\frac{m^{2a/(a,b)} - 2m^{a/(a,b)}}{(a,b)/a} - (\tfrac{1}{2}m^2 + m).$$

The right side is positive unless $(a, b)/a = 1$ and $(a, b)/b = 1$. So assume that $q = r$. If $m = 4$ and $n \geqslant 6$ then $\Delta \geqslant (\frac{1}{2}n^2 - n) - (\frac{1}{2}m^2 + m) \geqslant 0$; while if $m = 4$ and $n = 5$, then G_0 must be unitary, and we have $\Delta = (n^2 - n) - (\frac{1}{2}m^2 + m) \geqslant 0$. Now assume that $m \geqslant 5$. If also $n \geqslant 2m - 2$ then $\Delta \geqslant (\frac{1}{2}n^2 - n) - (\frac{1}{2}m^2 + m) \geqslant 0$.

By [21, (1.1)], since $n > m$ either $n \geqslant \frac{1}{2}m(m - 1) - 2$ or one of the following occurs: $S = \mathrm{PSp}(6, q)$, $n = 14$; or $S = \mathrm{PSp}(2l, q)$ with q even or $\mathrm{P\Omega}(2l + 1, q)$ with q odd, where $2 \leqslant l \leqslant 6$, and $n = 2^l$. Since we may assume that $m \geqslant 5$ and $n < 2m - 2$, this leaves only the last of these cases. But then $\Delta \geqslant (\frac{1}{2}n^2 - n) - (\frac{1}{2}m^2 + m) \geqslant 0$ if $l > 3$, so assume that $l = 3$; and $\Delta = (n^2 - n) - (\frac{1}{2}m^2 + m) \geqslant 0$ if G_0 is unitary. Now we may assume that $S \cong \mathrm{P\Omega}(7, q)$ lies in $G_0 = \mathrm{P\Omega}^{\pm}(8, q)$ or $\mathrm{PSp}(8, q)$. However, all irreducible subgroups of $\mathrm{PSL}(8, q)$ isomorphic to S are conjugate, and lie in an orthogonal group $\mathrm{P\Omega}^{+}(8, q)$ (again using [21]), in which case $G_0 = \mathrm{P\Omega}^{+}(8, q)$ (by the Remark); but this is a possibility that was discussed earlier.

Finally, assume that S is $\mathrm{P\Omega}^{\pm}(m, r)$ with m even and $m \geqslant 6$, or that S is exceptional (i.e., ${}^2B_2(r)$, ${}^2G_2(r)$ or $G_2(r)$). Then, by the Table, $M + \delta l \leqslant \frac{1}{2}m^2 + \frac{1}{2}m$, so that

$$\Delta \geqslant \frac{b}{a}(\tfrac{1}{2}n^2 - n) - (\tfrac{1}{2}m^2 + \tfrac{1}{2}m).$$

As before, this is $\geqslant 0$ if $(a, b)/a \geqslant 2$, so assume that $(a, b)/a = 1$. Then $\Delta \geqslant (\frac{1}{2}n^2 - n) - (\frac{1}{2}m^2 + \frac{1}{2}m) \geqslant 0$ since $n \geqslant m + 1$.

This proves our claim that $|S| \cdot r^{\delta l}/|G| \leqslant 16np^{-(n-1)b}$. As in Lemma 1 we find that each of the $O(b)$ groups S contributes $O(ap^{-(n-1)b}) = O(bp^{-(n-1)b})$ to $\Sigma_{9'}|L|/|G|$, so that $\Sigma_{9'}|L|/|G| \to 0$ as $|G| \to \infty$.

It remains to consider the cases in which G does not lie in $\mathrm{P\Gamma L}(V)$. Then G_0 is $\mathrm{PSp}(4, 2^b)$ or $\mathrm{P\Omega}^{+}(8, q)$).

If $G_0 = \mathrm{PSp}(4, 2^b)$ but G is not inside $\mathrm{P\Gamma Sp}(4, 2^b)$, then [1, §14] provides a

slight variation on the list $\mathbf{C}_1$–$\mathbf{C}_9$, and the above argument goes through without any difficulty.

Finally, we are left with the case $G_0 = P\Omega^+(8, q)$ but with G is not inside $P\Gamma O^+(8, q)$. Here, the results of [1] do not provide a list of the sort we have used above, but [18] does contain such a list, and the theorem follows as before. □

This completes the proof of the theorem.

REMARK. A check of the proof shows that $P(G) = O(n^3(\log q)^2 q^{-l(G_0)})$.

4. Some exceptional groups

In this section we wish to note the following (essentially known) fact:

PROPOSITION 4. *Let G_0 denote one of the groups ${}^2B_2(q)$, ${}^2G_2(q)$, $G_2(q)$, ${}^3D_4(q)$ or $E_6(q)$, and let $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$. If $P(G)$ is the probability that two randomly chosen elements of G do* **not** *generate a group containing G_0, then $P(G) \to 0$ as $|G| \to \infty$.*

Proof. The conjugacy classes of maximal subgroups of G are completely known in the cases ${}^2B_2(q)$, ${}^2G_2(q)$, $G_2(q)$, ${}^3D_4(q)$ ([2], [9], [16]–[18], [27]). It is straightforward to use these lists precisely as before.

Assume that $G_0 = E_6(q)$. In [3], [4], [19] the possible maximal subgroups L of G are divided into two classes, **A** and **B**, say, with the following properties: **A** contains subgroups known to occur as maximal subgroups of G for suitable q, and all the conjugacy classes of subgroups in **A** are determined; while **B** consists of a short list of $O(1)$ groups whose occurrence or conjugacy classes have yet to be determined. For L in **A**, it is easy to check that $|L|/|G| \leqslant q^{-16}$. Using (*) together with the conjugacy classes provided in [3], [4], [19], it is not difficult to check that **A** contributes $O((\log q)q^{-15})$ to (*).

This leaves us with the groups L in **B**. Here, $L = N_G(S)$ and $L \leqslant \mathrm{Aut}(S)$ for a nonabelian simple group S, namely, $S \cong A_6$, A_7, A_8, PSL(2, 7), PSL(2, 11), PSL(2, 13), PSL(2, 19), PSL(3, 3), PSU(3, 3), M_{11}, M_{12}, J_1 or HJ. It must be emphasized that even the existence of some of these as subgroups of G is left open in [3], [4], and is not relevant to our discussion. In each case, $|S| \mid b$, where $b := 2^7 3^3 5^2 7 \cdot 11 \cdot 13 \cdot 19$. In each case it is not difficult to check that S is generated by two semisimple elements x, y (i.e., p'-elements), no matter what p happens to be.

Each semisimple element $x \in G_0$ of order dividing b lies in a maximal torus T. There are exactly 25 conjugacy classes of maximal tori of G_0, and each has

order $\geqslant (q-1)^6/3$ (cf. [8], [25, (2. liv, 2.4iii)]). Moreover, each maximal torus contains $O(1)$ elements of order dividing b. Since we may assume that $q \geqslant 5$, it follows that $|x^{G_0}| \leqslant |G_0|/|T| < 12|G_0|/q^6$, and hence that the number of semisimple elements of G_0 of order dividing b is $O(|G_0|/q^6)$. In particular, the number of subgroups of G_0 generated by two semisimple elements of order dividing b is $O(|G_0|^2/q^{12})$.

Thus, the number of subgroups S is $O(|G_0|^2/q^{12})$. In particular, since $|L| = |N_G(S)| = O(1)$ we see that the number of pairs of elements of G lying in some such subgroup L is also $O(|G_0|^2/q^{12})$. Consequently, $\Pr(g, h \in L) = O(1/q^{12})$, as required. (An alternative approach to the last part of this proof can be based on the observation that $\{g \in G \mid g^b = 1\}$ defines a subvariety of G, in which case the main result of [23] can be applied.) □

Note that there are exactly q^{36} unipotent elements of $G_0 = E_6(q)$, so that the probability is $q^{36}/|G_0| = O(|G_0|/q^6)$ that an element is unipotent. It follows that the considerations above could have used a pair of elements each of which is semisimple or unipotent.

It would, of course, be desirable to avoid the aforementioned lists, since that would (presumably) produce a proof in the cases of the remaining simple groups. On the other hand, it is quite clear what kinds of lists are required for the cases of the remaining groups: ${}^2F_4(q)$, $F_4(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$. While it seems likely that all maximal subgroups of the latter groups will be known in the near future, we expect that a list (as in [3]) suitable for the purposes of our results will exist fairly soon. A very recent result [22] seems to provide such a list in case the characteristic is not too small.

It is not difficult to devise or conjecture variations on the theorem. We content ourselves with two of the latter:

CONJECTURE 1. *If G is a finite simple (classical) group, and two elements are randomly chosen from G one of which is an involution, then they generate G with probability $\to 1$ as $|G| \to \infty$.*

CONJECTURE 2. *Let G be a finite simple (classical) group, and fix $g \in G$, $g \neq 1$. If an element h is randomly chosen from G, then $\langle g, h \rangle = G$ with probability $\to 1$ as $|G| \to \infty$.*

5. Direct products of simple groups

In this section we will discuss the generation of direct products of finite simple groups. For any group H and any integer $k \geqslant 2$ let $Q(H, k)$ denote the probability that k elements generate H; thus, $Q(H, 2) = 1 - P(H)$ in our previous notation.

First we observe that, for our purposes, it suffices to consider the direct product G^m of m copies of a group G:

LEMMA 5. *Let $G_1, \dots, G_t$ be pairwise nonisomorphic simple groups, let $m_1, \dots, m_t$ be positive integers, and let $G = G_1^{m_1} \times \cdots \times G_1^{m_t}$. Then*

(a) *A subset of G generates G if and only if its projection into $G_i^{m_i}$ generates $G_i^{m_i}$ for each i; and*
(b) $Q(G, k) = \Pi_{i=1}^{t} Q(G_i^{m_i}, k)$.

Proof. Part (a) is straightforward, and (b) is then an immediate consequence. □

Consequently, we will consider a power G^m of a simple group G. Let $D_k(G)$ denote the set of ordered k-tuples generating G.

PROPOSITION 6. *Consider a $k \times m$ 'matrix' (x_{ij}) of km elements of a nonabelian simple group G, with 'rows' $r_i = (x_{ij}) \in G^m$ and 'columns' $c_j = (x_{ij}) \in G^k$. Then the r_i generate G^m if and only if the c_j lie in different* Aut(G)*-orbits of $D_k(G)$ – where the action of* Aut(G) *is the diagonal one.* (Each such orbit has length |Aut(G)|.)

Proof. Write $G^m = G_1 \times \cdots \times G_m$ with each $G_j \cong G$. Clearly $H := \langle r_1, \dots, r_k \rangle$ cannot be all of G^m except, perhaps, if the projections of the r_i into each factor G_j generate G_j, that is, if all the c_j lie in $D_k(G)$. Assume that this is the case. Since H projects onto G_m, $H \cap G_m \trianglelefteq G_m$ (as all the required conjugations are induced by elements of H). By simplicity, $H \cap G_m = G_m$ or 1.

Assume that the c_j are in different Aut(G)-orbits. By induction, the projection of H into $G_1 \times \cdots \times G_{m-1}$ is onto. If $H \cap G_m = G_m$ then $H = G^m$. Similarly, we may assume that $H \cap G_j = 1$ for each j. Using the above projection we see that $H \cap (G_1 \times \cdots \times G_{m-1}) \trianglelefteq G_1 \times \cdots \times G_{m-1}$ (once again all the required conjugations are induced by elements of H). Since G is nonabelian and simple, while $H \cap G_j = 1$ for each j, it follows that $H \cap (G_1 \times \cdots \times G_{m-1}) = 1$. Hence the projection $H \to G_m$ is an isomorphism, and similarly so is each projection $H \to G_j$. In particular, we obtain an isomorphism $G_1 \to H \to G_m$ sending $x_{1j} \to r_j = (x_{1j}, \dots, x_{mj}) \to x_{mj}$. But then c_1 and c_m are in the same Aut(G)-orbit, which is not the case.

Conversely, assume without loss of generality that $\varphi(c_1) = c_2$ for some $\varphi \in \mathrm{Aut}(G)$. Then the projection of H into $G_1 \times G_2$ consists of the elements of the form $(g, \varphi(g))$, $g \in G$, and hence H cannot be G^m.

Finally, the last statement of the lemma is obvious. □

The converse part of the proposition can be found in [24].

COROLLARY 7 [14]. *If G is a nonabelian finite simple group and if $d_k(G)$*

denotes the largest integer m such that G^m has k generators, then $d_k(G) = |D_k(G)|/|\mathrm{Aut}(G)|$.

The corollary is immediate in view of the previous proposition; Hall's proof [14] is different from ours, but is just as simple.

COROLLARY 8. *If $n \geq 5$, and if $m \geq n^{cn}$ for some constant c, then A_n^m is generated by $O[\log m/(n \log n)]$ elements. In particular, for fixed n, A_n^m is generated by $O(\log m)$ elements.*

Proof. By Corollary 7, A_n^m is generated by k elements if $m \leq |D_k(A_n)|/|\mathrm{Aut}(A_n)|$. For all sufficiently large n, $|D_k(A_n)| \geq \frac{1}{2}|A_n|^k$ by [11]. Consequently, there is a constant $\delta > 0$ such that $|D_k(A_n)| \geq \delta |A_n|^k$ for all $n \geq 5$. Then $|D_k(A_n)|/|\mathrm{Aut}(A_n)| \geq \delta(\frac{1}{2}n!)^k/2n!$ since $\mathrm{Aut}(A_n) = S_n$ for $n \neq 6$; if $n = 6$ then $|\mathrm{Aut}(A_n)| = 2|S_n|$.

Thus, if $m \leq \delta(\frac{1}{2}n!)^k/2n!$ then A_n^m is generated by k elements. Taking logarithms shows that $k = O[\log m/(n \log n)]$ elements suffice to generate A_n^m. □

The second part of the corollary is a special case of the fact that G^m is generated by $O(\log m)$ elements for every nonabelian finite simple group G [29].

Let $c(\beta, m)$ denote the probability that distinct balls are obtained when m balls are chosen (with repetition) from among β balls. Then

$$c(\beta, m) = \prod_{i=1}^{m-1} \left(1 - \frac{i}{\beta}\right).$$

We will need the following rough estimate for $c(\beta, m)$ pointed out to us by Persi Diaconis: if $m = O(\sqrt{\beta})$ then

$$c(\beta, m) = \prod_{i=1}^{m-1} \left(1 - \frac{i}{\beta}\right) = \exp\left\{\sum_{i=1}^{m-1} \log\left(1 - \frac{i}{\beta}\right)\right\}$$

$$= \exp\left\{-\sum_{i=1}^{m-1} \frac{i}{\beta} + O\left(m \cdot \frac{m^2}{\beta^2}\right)\right\} = \exp\left\{-\frac{m^2}{2\beta} + O\left(\frac{m}{\beta}\right)\right\}.$$

PROPOSITION 9. *If G is a nonabelian finite simple group, then*

$$Q(G^m, k) = Q(G, k)^m c(d_k(G), m) = \frac{Q(G, k)}{|G|^{k(m-1)}} \prod_{i=1}^{m-1} (Q(G, k)|G|^k - i|\mathrm{Aut}(G)|).$$

Proof. The first equality is immediate in view of Proposition 6 and Corollary 7. For the second, note that if we write

$$\beta = d_k(G) = \frac{|D_k(G)|}{|\mathrm{Aut}(G)|} = \frac{Q(G, k)|G|^k}{|\mathrm{Aut}(G)|}$$

then

$$Q(G^m,k) = Q(G,\ k)^m c(\beta,m) = Q(G,k)^m \prod_{i=1}^{m-1}\left(1-\frac{i}{\beta}\right)$$

$$= Q(G,k)^m \prod_{i=1}^{m-1}\left(1 - i\frac{|\mathrm{Aut}(G)|}{Q(G,k)|G|^k}\right)$$

$$= \frac{Q(G,k)^m}{Q(G,k)^{m-1}|G|^{k(m-1)}} \prod_{i=1}^{m-1}(Q(G,\ k)|G|^k - i|\mathrm{Aut}(G)|). \qquad \square$$

Consequently, $Q(G^m,k)$ can be estimated in terms of $|G|$ and $Q(G,k)$. According to the theorem, $Q(G,2)$ – and hence also $Q(G,k)$ – is near 1 for large G, provided that G is a simple alternating or classical group (and probably for all finite simple groups). In other words, $|D_k(G)|$ is near $|G|^k$ for large G of that sort. We will now present some applications of the preceding results.

PROPOSITION 10. *Let Ω_m denote the set of finite groups that are direct products of $m \geqslant 2$ nonabelian finite simple classical (or alternating) groups. Then the probability that two elements of $H \in \Omega_m$ generate H approaches* 1 *as the orders of* **all** *of the factors of H approach* ∞. (In particular, for a fixed m all but finitely many groups in Ω_m are generated by two elements.)

Proof. Lemma 6 allows us to reduce to the case $H = G^m$. For each G we have $|\mathrm{Aut}(G)| < |G| \log |G|$. Thus, if G is large then so is $|D_m(G)|/|\mathrm{Aut}(G)|$, and hence $c(d_k(G), m)$ is near 1 (as m is fixed). Since $Q(G,2) \to 1$, Proposition 9 implies the result. $\square$

We give two examples of the uses of Proposition 9 which will be needed in Section 6.

EXAMPLE 1. (i) *For each prime $p \geqslant 5$, $\mathrm{PSL}(2,p)^p$ is generated by two elements.*

(ii) *The probability that two elements generate $\mathrm{PSL}(2,p)^p$ approaches e^{-1} as the prime $p \to \infty$.*

(iii) *The probability that three elements generates $\mathrm{PSL}(2,p)^p$ approaches* 1 *as the prime $p \to \infty$.*

Proof. The subgroup structure of $\mathrm{PSL}(2,p)$ has been known for over a century (cf. [10]). Using it, together with the elementary observation (*) in Section 2, it is straightforward to check that $P(\mathrm{PSL}(2,p)) \leqslant p^{-1} + 10p^{-2} \leqslant 6p^{-1}$ for all p (compare (**) in Section 2). On the other hand, by considering the probability that two elements of $\mathrm{PSL}(2,p)$ fix the same point of the projective line it is easy to check that $P(\mathrm{PSL}(2,p)) \geqslant p^{-1} - 2p^{-2}$.

In particular, for each $\varepsilon > 0$ we see that $1 - (1+\varepsilon)p^{-1} <$

$Q(\mathrm{PSL}(2,p),2) < 1 + (1+\varepsilon)p^{-1}$ for all sufficiently large p. Consequently, $Q(\mathrm{PSL}(2,p),2)^p \to e^{-1}$ as $p \to \infty$.

By Corollary 7,

$$\beta := d_2(\mathrm{PSL}(2,p)) = \frac{|D_2(\mathrm{PSL}(2,p))|}{|\mathrm{Aut}(\mathrm{PSL}(2,p))|} \geqslant (1-6p^{-1})\frac{|\mathrm{PSL}(2,p)|^2}{|\mathrm{PGL}(2,p)|} > p,$$

which proves (i). Moreover, $\beta > p^3/8$ for all sufficiently large p, so that

$$c(\beta,p) = \exp\left\{-\frac{p^2}{2\beta} + O\left(\frac{p}{\beta}\right)\right\} \to 1 \quad \text{as } p \to \infty,$$

and hence Proposition 9 implies (ii).

Next, note that there is an obvious variation of (*) for three generators (or, for that matter, any number of generators). As above, for each $\varepsilon > 0$ this produces the estimate

$$1 - (1+\varepsilon)p^{-2} < Q(\mathrm{PSL}(2,p),3) < 1 + (1+\varepsilon)p^{-2}$$

for all sufficiently large p. Consequently, this time,

$$Q(\mathrm{PSL}(2,p),3)^p \to 1 \quad \text{as } p \to \infty.$$

Since $c(d_3(\mathrm{PSL}(2,p)),p) \to 1$ as before, this implies (iii). □

EXAMPLE 2. (i) *$A_n^{n!/8}$ is generated by two elements for all sufficiently large n.*

(ii) *The probability that $[\sqrt{n}]$ elements generate $A_n^{n!/8}$ approaches 0 as $n \to \infty$. (In particular, for any fixed k, the probability that k elements generate $A_n^{n!/8}$ approaches 0 as $n \to \infty$.*

Proof. By [11] and Corollary 7, for all large n we have

$$d_2(A_n) = \frac{|D_2(A_n)|}{|\mathrm{Aut}(A_n)|} \geqslant \tfrac{1}{2}\frac{|A_n|^2}{|S_n|} = n!/8,$$

so that (i) holds.

Let $k = [\sqrt{n}]$. Since A_{n-1} is a subgroup of A_n, $Q(A_n,k) \leqslant 1 - (1/n)^k$. Then $Q(A_n,k)^{n!/8} \to 0$ as $n \to 0$, and hence $Q(A_n^{n!/8},k) \to 0$ by Proposition 9. □

REMARKS. Many more examples of the above types can be readily obtained. The following ones are left to the reader.

(i) The probability that n elements generate $A_n^{n!/8}$ approaches 1 as $n \to \infty$.

(ii) The probability that two elements generate A_n^n approaches e^{-1} as $n \to \infty$; while the probability that three elements generate A_n^n approaches 1 as $n \to \infty$. Here, a better bound is needed for $P(A_n)$, whose proof uses the classification of finite simple groups ([5]; cf. Proposition 13(i) below).

6. Generation of profinite groups

If F is a profinite group, one can ask for the probability that a k-tuple of elements of F 'generates' F. Here, probability is in terms of the normalized Haar measure on F^k, and 'generates' refers to generating a dense subgroup. The following result answers a question posed in [12, Problem 16.16(2)].

Let $\hat{F}_l$ denote the free profinite group on l generators.

PROPOSITION 11. (i) *For any $l \geqslant 2$ and k, the probability that k elements generate $\hat{F}_l$ is* 0.

(ii) *More generally, the probability that k elements generate an open subgroup* (i.e., *a closed subgroup of finite index*) *of $\hat{F}_l$ is also* 0.

Proof. Since $\hat{F}_2$ is a homomorphic image of $\hat{F}_l$ it suffices to consider the case $l = 2$.

(i) By Example 2 in Section 5, $A_n^{n!/8}$ is a quotient of $\hat{F}_2$ while the probability of k elements generating $A_n^{n!/8}$ approaches 0 as $n \to \infty$. Thus, (i) holds.

(ii) If H is an open subgroup of $\hat{F}_l$ then $H \cong \hat{F}_m$ with $m = 1 + |\hat{F}_l : H|(l-1)$ [12, 15.27]. We are only interested in the case in which H is generated by k elements, so that $1 + |\hat{F}_l : H|(l-1) \leqslant k$. There are only finitely many open subgroups $H_1, \ldots, H_s$ whose index in $\hat{F}_l$ is at most $(k-1)/(l-1)$ [12, 15.1]. Consequently,

$$\Pr(k \text{ elements generate a subgroup of finite index in } \hat{F}_l)$$

$$\leqslant \sum_{i=1}^{s} \Pr(k \text{ elements generate } H_i) = \sum_{i=1}^{s} 0 = 0$$

since part (i) can be applied to each of the free profinite groups H_i. □

Note that the preceding proof did not use the classification of finite simple groups: the proof of (i) used only elementary properties of A_n.

The preceding result should be compared to the situation in the abelian case (see [12, 16.15] for the case $l = 1$):

PROPOSITION 12. *Let $\hat{A}_l \cong \hat{\mathbb{Z}}^l$ be the free profinite abelian group on l generators. Then, for $k \geqslant l$,*

(i) $\Pr(k \text{ elements generate } \hat{A}_l) = \begin{cases} 0 & \text{if } k = l \\ \prod_{i=k-l+1}^{k} \zeta(i)^{-1} > 0 & \text{if } k > l \end{cases}$

where ζ is the usual zeta function; and

(ii) $\Pr(k \text{ elements generate a subgroup of finite index in } \hat{A}_l) =$

$$\begin{cases} 0 & \text{if } k = l \\ 1 & \text{if } k > l. \end{cases}$$

Proof. For each prime p let E_p be the set of k-tuples in $\hat{A}_l^k$ whose projections to $\mathbb{Z}_p^l$ generate $\mathbb{Z}_p^l$ (or equivalently, whose projections to $\mathbb{F}_p^l$ generate $\mathbb{F}_p^l$). Then $\{E_p \mid p \text{ prime}\}$ consists of independent sets, and $\mu(E_p)$ is the probability that k vectors in $\mathbb{F}_p^l$ span that space. The latter probability is the same as the probability that l vectors in $\mathbb{F}_p^k$ are linearly independent (using the equality of row and column rank), and hence

$$\mu(E_p) = \frac{p^k - 1}{p^k}\frac{p^k - p}{p^k}\cdots\frac{p^k - p^{l-1}}{p^k}$$
$$= (1 - p^{-k})(1 - p^{-(k-1)})\cdots(1 - p^{-(k-l+1)}).$$

By independence, $\mu(\bigcap E_p) = \Pi_p \mu(E_p)$, which $= \Pi_{i=k-l+1}^{k} \zeta(i)^{-1}$ if $k > l$ and $=0$ if $k = l$. This proves (i). Moreover, this shows that, if $\bar{E}_p$ denotes the complement of E_p, then $\Sigma \mu(\bar{E}_p)$ converges if $k > l$ and is ∞ if $k = l$. By the Borel–Cantelli lemma [12, 16.7], it follows that $\Pr(x \in \hat{A}_l^k$ is in E_p for almost all $p)$ is 1 if $k > l$ and is 0 if $k = l$. This completes the case $k = l$ since x can generate a subgroup of finite index in $\hat{A}_l$ only if x is in E_p for almost all p.

Now let $k > l$. We first claim that almost every k-tuple of elements of $\mathbb{Z}_p^l$ generates a subgroup of finite index. Indeed, for every subgroup H of index p^n in $\mathbb{Z}_p^l$ consider $H^k \leqslant (\mathbb{Z}_p^l)^k$. Then $\mu(H^k) = 1/p^{nk}$ while the number $c(p^n)$ of such subgroups H grows polynomially, in fact $c(p^n) \leqslant M(p^n)^l$ for some constant M [15]. Hence, letting H range over all subgroups H of finite index in $\mathbb{Z}_p^l$ we have

$$\sum \mu(H) = \sum_{n=1}^{\infty} \frac{c(p^n)}{p^{nk}} \leqslant \sum_{n=1}^{\infty} \frac{M(p^n)^l}{p^{nk}} < \infty \quad \text{since } k > l.$$

Again using the Borel–Cantelli lemma we deduce that $\mu\{k\text{-tuples of elements of } \mathbb{Z}_p^l \text{ lying in infinitely many subgroups } H \text{ of finite index in } \mathbb{Z}_p^l\} = 0$. This implies the claim since every closed subgroup of infinite index in a profinite group is contained in infinitely many subgroups of finite index [12, p. 3].

Let B_p be the set of k-tuples in $\hat{A}_l^k = \hat{\mathbb{Z}}^{lk}$ whose projections to $\mathbb{Z}_p^l$ generate a subgroup of finite index in $\mathbb{Z}_p^l$. By the previous paragraph, $\mu(B_p) = 1$, and hence $\mu(\bigcap_p B_p) = 1$ as well.

At this point we know that almost every k-tuple x of elements of $\hat{A}_l$ has the properties that (i) for almost every prime p, the projection of x into $\mathbb{Z}_p^l$ generates $\mathbb{Z}_p^l$, and (ii) for every prime p, this projection of x generates a subgroup of finite index in $\mathbb{Z}_p^l$. These two properties are equivalent to saying that x generates a subgroup of finite index in $\hat{A}_l$. □

7. More profinite groups

Finally, we turn to an entirely different type of question concerning the probability of generating suitable profinite groups. Whereas the last two sections were independent of the theorem – and hence of the classification of finite simple groups – we will now once again use that theorem. As in Section 5, we will use information concerning the rate of convergence of $P(G)$ to 0.

Let $\mathscr{F}_A$ consist of a representative of each isomorphism class of nonabelian finite simple groups; and let $\mathscr{F}_C$ consist of a representative of each isomorphism class of finite simple alternating or classical groups. We will need the following quantitative version of the theorem and the theorem in [11]:

PROPOSITION 13. *If $G \in \mathscr{F}_C$, then $P(G)$ behaves as follows*:

(i) $P(A_n) = n^{-1} + O(n^{-2})$; *and*

(ii) *If G is a classical group over $\mathbb{F}_q$ in dimension n, then* $P(G) = O(n^3(\log q)^2 q^{-l(G)})$, *while* $P(\mathrm{PSL}(2,q)) \geqslant q^{-1} - 2q^{-2}$.

Proof. (i) This is due to Babai [5], using the classification of finite simple groups. (NB – The following weaker version of this, obtained in [6] using nineteenth-century group theory together with number-theoretic estimates, suffices below: for each $\varepsilon > 0$, $P(A_n) < n^{-1+\varepsilon}$ for all sufficiently large n.)

(ii) The first part follows from an examination of the estimates occurring in the proof of the theorem (see the remarks at the end of Sections 2 and 3). For the second part proceed as in Section 5, Example 1. □

We will consider (unrestricted) products $P = \Pi_{G \in \mathscr{U}} G$ of subsets $\mathscr{U}$ of $\mathscr{F}_A$. Each such product P is a compact group, with Haar measure μ satisfying $\mu((S_G)_G) = \Pi_{G \in \mathscr{U}} |S_G|/|G|$ whenever the subsets $S_G \subseteq G$ satisfy $S_G = G$ for almost all $G \in \mathscr{U}$.

Throughout the remainder of this section, when we consider the case $\mathscr{U} = \mathscr{F}_A$ we will always *assume*:

($) *For every finite simple group G of Lie type defined over $\mathbb{F}_q$,* $P(G) = O(l(G)^3(\log q)^2 q^{-l(G)})$.

By Proposition 13, ($) is already known to be true in the case of classical groups; and in fact it is also known for all the cases discussed in Section 4.

We will consider the probability of generating a dense subgroup of P using two or three elements of G.

PROPOSITION 14. *Let P be the product of all the members of $\mathscr{F}_C$, or of $\mathscr{F}_A$ assuming ($). Then*

(i) $\Pr(g, h \in P$ *generate a dense subgroup of* $P) = 0$; *and*

(ii) $\Pr(g, h, k \in P$ *generate a dense subgroup of* $P) \neq 0, 1$.

PROPOSITION 15. *Let P be the product of all the members of $\mathcal{F}_C$, or of $\mathcal{F}_A$ assuming (\$), but excluding the alternating groups and those of the form* PSL(2, p) *with p prime. Then* $\Pr(g, h \in P$ *generate a dense subgroup of* $P) \neq 0, 1$.

Proof of Propositions 14 *and* 15. Consider $g, h \in P$. It is easy to check that $\langle g, h\rangle$ is dense if and only if g and h project onto a pair of generators of each factor in the definition of P. Thus, if $T_P \subseteq P \times P$ is the set of all such pairs (g, h), then $T_P = \Pi_G T_G$ where T_G is defined similarly for $G \in \mathcal{F}_A$. Then $\mu(T_P) = \Pi_G(1 - P(G))$, and so $\mu(T_P) = 0$ if and only if $\Sigma_G P(G)$ diverges.

Now Proposition 13 shows that, in Proposition 14(i), $\Sigma_G P(G)$ has a subsum $\geqslant \Sigma n^{-1}$ and hence diverges; whereas in Proposition 15, $\Sigma_G P(G)$ converges (by Proposition 13, since we are avoiding part (i) there, while $\Sigma_G n^3(\log q)^2 q^{-l(G)}$ converges provided that G is restricted so that q is not a prime when $n = 2l(G) = 2$). The proof of Proposition 14(ii) is similar: it is only necessary to check that

$$\Pr(g, h, k \in \mathrm{PSL}(2, q) \text{ do not generate } \mathrm{PSL}(2, q)) = O(q^{-2})$$

and

$$\Pr(g, h, k \in A_n \text{ do not generate } A_n) = O(n^{-3/2}).$$

In fact, since $\Pr(g, h, k \in G$ do not generate $G) \leqslant P(G)^2$, Proposition 13(ii) implies the first of these inequalities; while the second follows either from Proposition 13(i), or from the less difficult result from [6] mentioned in the proof of Proposition 13(i) (namely, use $\varepsilon = \frac{1}{4}$). □

REFERENCES

1. Aschbacher, M., 'On the maximal subgroups of the finite classical groups', *Invent. Math.* **76** (1984), 469–514.
2. Aschbacher, M., 'Chevalley groups of type $G_2(q)$ as the group of a trilinear form', *J. Algebra* **109** (1987), 193–259.
3. Aschbacher, M., 'The 27-dimensional module for E_6' I-IV. I: *Invent. Math.* **89** (1987), 159–195; II: *J. London Math. Soc.* **37** (1988) 275–293; III: *Trans. Amer. Math. Soc.* (to appear); IV: *J. Algebra* (to appear).
4. Aschbacher, M., 'The maximal subgroups of E_6' (to appear).
5. Babai, L., 'The probability of generating the symmetric group', *J. Combin. Theory* (*A*) **52** (1989), 148–153.
6. Bovey, J. D., The probability that some power of a permutation has small degree, *Bull. London. Math. Soc.* **12** (1980), 47–51.
7. Carter, R., *Simple Groups of Lie Type*, Wiley, London; New York; Sydney; Toronto, 1972.
8. Carter, R., 'Conjugacy classes in the Weyl group', *Compositio Math.* **25** (1972), 1–59.
9. Cooperstein, B. N., 'Maximal subgroups of $G_2(2^n)$', *J. Algebra* **70** (1981), 23–36.
10. Dickson, L. E., *Linear Groups, with an Exposition of Galois Theory*, Dover, New York, 1958.

11. Dixon, J. D., 'The probability of generating the symmetric group', *Math. Z.* **110** (1969), 199–205.
12. Fried, M. D. and Jarden, M., *Field Arithmetic*, Springer, Berlin; Heidelberg, 1986.
13. Gorenstein, D., *Finite Groups*, Harper and Row, New York, 1968.
14. Hall, P., 'The Eulerian function of a group', *Quart. J. Math.* **7** (1936), 134–151.
15. Ilani, I., 'Counting finite index subgroups and the P. Hall enumeration principle' (to appear in *Israel J. Math.*).
16. Kleidman, P. B., 'The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups', *J. Algebra* **110** (1987), 173–242.
17. Kleidman, P. B., 'The maximal subgroups of the finite Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups', *J. Algebra* **115** (1988), 182–199.
18. Kleidman, P. B., '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.
19. Kleidman, P. B., 'The maximal subgroups of automorphism groups of $E_6(q)$ inducing a graph automorphism' (to appear).
20. Landazuri, V. and Seitz, G. M., 'On the minimal degrees of projective representations of the finite Chevalley groups', *J. Algebra* **32** (1974), 418–443.
21. Liebeck, M. W., 'On the order of maximal subgroups of the finite classical groups', *Proc. London Math. Soc.* **50** (1985), 426–446.
22. Liebeck, M. W. and Seitz, G. M., 'Maximal subgroups of exceptional groups of Lie type, finite and algebraic', *Geom. Dedicata* **35** (1990), 353–387.
23. Lang, S. and Weil, A., 'Number of points of varieties in finite fields', *Amer. J. Math.* **76** (1954), 819–827.
24. Meier, D. and Wiegold, J., 'Growth sequences in finite groups, V', *J. Austral. Math. Soc.* **31** (1981), 374–375.
25. Seitz, G. M., 'The root subgroups for maximal tori in finite groups of Lie type', *Pacific J. Math.* **106** (1983), 153–244.
26. Steinberg, R., 'Representations of algebraic groups', *Nagoya Math. J.* **22** (1963), 33–56.
27. Suzuki, M., 'On a class of doubly transitive groups', *Ann. of Math.* **75** (1962), 105–145.
28. Wagner, A., 'An observation on the degrees of projective representations of the symmetric and alternating groups over an arbitrary field', *Arch. Math.* **29** (1977), 583–589.
29. Wiegold, J., 'Growth sequences of finite groups', *J. Austral. Math. Soc.* **17** (1974), 133–141.

Authors' addresses:

William M. Kantor,
Department of Mathematics,
University of Oregon,
Eugene, OR 97403,
U.S.A.

Alexander Lubotzky,
Department of Mathematics,
The Hebrew University,
Jerusalem,
Israel.

(Received, November 14, 1989)