RANDOM GENERATION OF FINITE SIMPLE GROUPS BY p-REGULAR OR p-SINGULAR ELEMENTS

BY

ANER SHALEV*
Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: shalev@math.huji.ac.il

ABSTRACT

Let p be a fixed prime and let G be a finite simple group. It is shown that two randomly chosen elements of G of orders prime to p generate G with probability tending to 1 as $|G| \to \infty$. This answers a question of Kantor. Some related results are also established.

1. Introduction

Let G be a finite simple group. A conjecture of J. D. Dixon, which is now a theorem (cf. [D], [KaLu], [LiSh1]), states that the probability that two randomly chosen elements x, y of G generate G tends to 1 as $|G| \to \infty$. Recently Bill Kantor asked whether a similar result holds if we pick at random two elements of odd order. He also considered other versions of the problem, such as random generation by two elements of even order, or by an element of even order and an element of odd order. In this paper we answer these questions. In fact we prove a bit more. Recall that for a prime p and a group element x we say that x is p-singular if its order is divisible by p, and that x is p-regular if its order is not divisible by p. The group $PSL_n(q)$ will also be denoted by $L_n(q)$.

* Partially supported by a grant from the Israel Science Foundation, administered by the Israel Academy of Science and Humanities.
Received July 14, 2000

THEOREM 1.1: *Let p be a fixed prime and let G be a finite simple group. Then:*

(i) *The probability that two randomly chosen p-regular elements of G generate G tends to 1 as $|G| \to \infty$.*

(ii) *Suppose p divides $|G|$, and if $p = 2$ suppose $G \neq L_2(q)$ with q even. Then the probability that two randomly chosen p-singular elements of G generate G tends to 1 as $|G| \to \infty$.*

(iii) *Suppose p divides $|G|$. Then the probability that a randomly chosen p-regular element of G and a randomly chosen p-singular element of G generate G tends to 1 as $|G| \to \infty$.*

The exception in part (ii) above is genuine. Indeed, the elements of even order in $L_2(2^k)$ are involutions, and two involutions always generate a proper (dihedral) subgroup.

For other results on random generation by elements of restricted orders see [LiSh2], [LiSh3]. We note that the methods used here seem to be applicable in other contexts, such as random generation by nth powers, etc. Indeed, we first obtain a random generation result for any "large" subset S of a finite simple group G (see Corollaries 2.3 and 2.4 below). We then show that this result already gives rise to many instances of Theorem 1.1. The remaining cases are dealt with using a more detailed analysis.

ACKNOWLEDGEMENT: I am grateful to Bill Kantor for useful discussions, and to the Institute for Advanced Studies at the Hebrew University for its kind hospitality during Spring Semester 2000, when the program on Asymptotic Group Theory took place.

2. Proofs

Let p be a fixed prime, and let $c, c_1, c_2, \ldots$ denote positive constants. Let G be a finite simple group, and let $m(G)$ denote the minimal index of a proper subgroup of G. Let $X_n(q)$ denote a finite simple group of Lie type of rank n over a field with q elements.

LEMMA 2.1: *Let $G = X_n(q)$ be sufficiently large. Then:*

(i) $m(G) \geq q^n$.

(ii) *If $m(G) \leq cq^2$ then G is one of $L_2(q), L_3(q)$ or the Suzuki group $Sz(q)$.*

(iii) *If $m(G) \leq cq$ then $G = L_2(q)$.*

For classical groups this follows from Table 5.2.A of [KL]. For exceptional groups this follows from [LiSa] (see also Lemma 6.4 of [LiSh3]).

Let $Q(G)$ denote the proportion of non-generating pairs among all pairs of elements of G.

LEMMA 2.2: *There exist a constant c such that $Q(G) \leq cm(G)^{-1}$ for all finite simple group G.*

This follows from [Ba], [Ka], [LiSh3] (where more refined estimates are obtained).

For a subset S of G let $Q_S(G)$ denote the probability that two randomly chosen elements from S do not generate G. We write $f >> g$ for functions f, g if the ratio f/g tends to infinity.

COROLLARY 2.3: *Let S be a subset of a finite simple group G. Then $Q_S(G) \leq c|G|^2 m(G)^{-1}|S|^{-2}$. Consequently, if $|S|/|G| >> m(G)^{-1/2}$, then $Q_S(G) \to 0$.*

Proof: Among all the $|S|^2$ pairs of elements of S, the number of non-generating pairs is obviously at most $|G|^2 Q(G)$. Hence $Q_S(G) \leq |G|^2 Q(G)|S|^{-2}$. The first assertion now follows by applying Lemma 2.2, whereas the second assertion follows from the first. ∎

COROLLARY 2.4: *Let G be a finite simple group and let $S \subseteq G$. Suppose either $G = A_n$ and $|S|/|G| >> n^{-1/2}$, or $G = X_n(q)$ and $|S|/|G| >> q^{-n/2}$. Then $Q_S(G) \to 0$.*

Proof: This follows by combining Lemmas 2.1 and 2.3 and the equality $m(A_n) = n$. ∎

Fix a prime p. Given G let R be the set of p-regular elements of G, and let S be the set of p-singular elements of G. Set $Q_{p'}(G) = Q_R(G)$ and $Q_p(G) = Q_S(G)$. In addition, denote by $Q_{p,p'}(G)$ the probability that a randomly chosen element of S and a randomly chosen element of R do not generate G. Our aim is to show that $Q_p(G), Q_{p'}(G), Q_{p,p'}(G) \to 0$ as $|G| \to \infty$.

Set $\mu_{p'}(G) = |R|/|G|$ and $\mu_p(G) = |S|/|G|$. Clearly $\mu_p(G) + \mu_{p'}(G) = 1$.

LEMMA 2.5: *Let p be a fixed prime. Then there are positive constants c_1, c_2, c_3 (depending on p) such that*

(i) $c_1 n^{-1/p} \leq \mu_{p'}(A_n) \leq c_2 n^{-1/p}$,

(ii) $\mu_{p'}(X_n(q)) \geq c_3 n^{-1}$.

Indeed, part (i) follows from [ET] and [BLNPS], and part (ii) from [NiP] and [BPS].

COROLLARY 2.6: *If $(G,p) \neq (A_n, 2)$ then $Q_{p'}(G) \to 0$ as $|G| \to \infty$.*

Proof: This follows by combining 2.4 and 2.5, since $c_1 n^{-1/p} >> n^{-1/2}$ for odd p, and $c_3 n^{-1} >> q^{-n/2}$. ∎

LEMMA 2.7: *Let $\mathcal{M}$ be a set of representatives for the conjugacy classes of the maximal subgroups of G. Then:*

(i) $Q_{p'}(G) \leq \sum_{M \in \mathcal{M}} (\mu_{p'}(M)/\mu_{p'}(G))^2 |G:M|^{-1}$.
(ii) $Q_p(G) \leq \sum_{M \in \mathcal{M}} (\mu_p(M)/\mu_p(G))^2 |G:M|^{-1}$.
(iii) $Q_{p,p'}(G) \leq \sum_{M \in \mathcal{M}} \mu_p(M)\mu_{p'}(M)\mu_p(G)^{-1}\mu_{p'}(G)^{-1}|G:M|^{-1}$.

Proof: If two p-regular elements x, y of G do not generate G then they lie in some maximal subgroup M of G, and the probability of this (given M) is $(\mu_{p'}(M)|M|/\mu_{p'}(G)|G|)^2$. Summing over all maximal subgroups M we obtain

$$Q_{p'}(G) \leq \sum_M (\mu_{p'}(M)|M|/\mu_{p'}(G)|G|)^2.$$

Part (i) follows since each M has $|G:M|$ conjugate subgroups, each contributing the same term to the sum. The proofs of parts (ii) and (iii) are similar. ∎

LEMMA 2.8: *$Q_{2'}(A_n) \to 0$ as $n \to \infty$.*

Proof: Let $G = A_n$ and let $\mathcal{M}$ be as above. Part (i) of Lemma 2.7 yields

$$Q_{2'}(G) \leq (\mu_{2'}(A_{n-1})/\mu_{2'}(A_n))^2 \cdot n^{-1} + \sum_{A_{n-1} \not\cong M \in \mathcal{M}} (\mu_{2'}(M)/\mu_{2'}(G))^2 |G:M|^{-1}.$$

By Lemma 2.5(i) the first summand of the right hand side is bounded above by $(c_2(n-1)^{-1/2}/c_1 n^{-1/2})^2 \cdot n^{-1} = O(n^{-1})$, whereas the second summand is bounded above by $\sum_{A_{n-1} \not\cong M \in \mathcal{M}} (1/\mu_{2'}(G))^2 |G:M|^{-1}$ which in turn is bounded above by $cn \cdot \sum_{A_{n-1} \not\cong M \in \mathcal{M}} |G:M|^{-1}$. It follows from the arguments in Babai [Ba] (see also [Ka]) that

$$\sum_{A_{n-1} \not\cong M \in \mathcal{M}} |G:M|^{-1} = O(n^{-2}).$$

Putting everything together we obtain $Q_{2'}(G) = O(n^{-1})$. The result follows. ∎

The proof of Theorem 1.1(i) is now complete.

In order to deal with p-singular elements suppose p divides $|G|$. Then we have

LEMMA 2.9: *Let $G = X_n(q)$, where $q = r^k$, r prime.*

(i) *If $r \neq p$ then $\mu_p(G) \geq p^{-2}$.*

(ii) *If $r = p$ then $\mu_p(G) \geq cq^{-1}$.*

This is proved in [IKS].

Note that $\mu_p(A_n) = 1 - \mu_{p'}(A_n) \geq 1 - c_2 n^{-1/p} \to 1$ as $n \to \infty$.

LEMMA 2.10: *Suppose G is alternating or a Lie type group in characteristic $\neq p$. Then $Q_p(G) \to 0$ as $|G| \to \infty$.*

Proof: In both cases $\mu_p(G)$ is bounded below by some positive constant (possibly depending on p), so the conclusion follows from 2.4. ∎

LEMMA 2.11: *Suppose G is a Lie type group in characteristic p, and assume $G \neq L_2(q), L_3(q), Sz(q)$. Then $Q_p(G) \to 0$ as $|G| \to \infty$.*

Proof: Let $G = X_n(q)$ where $q = p^k$. Suppose $Q_p(G) \geq \epsilon$ for some fixed $\epsilon > 0$. We have to show that $|G|$ is bounded (in terms of ϵ). By Lemma 2.3 we have $c|G|^2 m(G)^{-1}|S|^{-2} \geq \epsilon$ where S is the set of p-singular elements of G. This yields

$$m(G) \leq c_4(|G|/|S|)^2 = c_4\mu_p(G)^{-2}.$$

Applying Lemma 2.9(ii) it follows that $m(G) \leq c_5 q^2$. Since G is not one of $L_2(q), L_3(q), Sz(q)$, it follows from Lemma 2.1(ii) that $|G|$ is bounded. ∎

We now deal with the remaining groups, using information on their subgroup structure and Lemma 2.7.

LEMMA 2.12: *Let $p = 2$ and $G = Sz(q)$. Then $Q_p(G) \to 0$ as $|G| \to \infty$.*

Proof: By [Su] the maximal subgroups of G up to conjugacy are M_1 of order $q^2(q-1)$, M_2 (dihedral) of order $2(q-1)$, M_3 of order $4(q + \sqrt{2q} + 1)$, M_4 of order $4(q - \sqrt{2q} + 1)$, as well as the subfield subgroups $M_{5,r} := Sz(q^{1/r})$ where $r \geq 3$ ranges over the prime divisors of $k := \log_2 q$ (if k is composite).

Consider the upper bound for $Q_p(G)$ in Lemma 2.7(ii). Let $M = M_1$. Then it is known [Su] that M has a normal 2-subgroup Q of order q^2 and index $q-1$ such that any $a \in M \setminus Q$ acts fixed point freely on Q. It follows that every element $a \in M \setminus Q$ is 2-regular, since for some odd t we have $a^t \in Q$, hence $a^t \in C_Q(a) = 1$. We see that the 2-singular elements of M are precisely the non-trivial elements of Q, hence

$$\mu_2(M) = (|Q|-1)/|M| = (q+1)/q^2 \leq 2/q.$$

It follows that for $M = M_1$ we have

$$(\mu_p(M)/\mu_p(G))^2|G:M|^{-1} \leq ((2/q)/(c/q))^2(q^2+1)^{-1} = O(q^{-2}).$$

For the remaining maximal subgroups $M \in \mathcal{M}$ it suffices to use the inequalities $\mu_p(M) \leq 1$ and $|M| \leq q^{5/3}$ to obtain

$$(\mu_p(M)/\mu_p(G))^2|G:M|^{-1} \leq (1/(c/q))^2(q^{10/3})^{-1} = O(q^{-4/3}).$$

Noting that there are at most $\log\log q$ subfield subgroups in $\mathcal{M}$ we obtain

$$Q_p(G) \leq \sum_{M\in\mathcal{M}} (\mu_p(M)/\mu_p(G))^2|G:M|^{-1} \leq cq^{-2} + c\log\log q \cdot q^{-4/3},$$

which tends to 0 as $q \to \infty$. In fact a more careful analysis shows that $Q_p(G) = O(q^{-2})$. ∎

LEMMA 2.13: *Let $G = L_2(q)$, $q = p^k$, $p > 2$. Then $Q_p(G) \to 0$ as $|G| \to \infty$.*

Proof: Here the maximal subgroups in $\mathcal{M}$ are the parabolic subgroup M_1 of order $q(q-1)/2$, the dihedral subgroups M_2 and M_3 of order $q+1$ and $q-1$ respectively, the subfield subgroups $M_{4,r} = L_2(q^{1/r})$ for r a prime divisor of k, and some bounded number of bounded subgroups. The p-singular elements in M_1 have order p and we have $\mu_p(M_1) = (q-1)/|M_1| = 2/q$. Plugging this as well as $\mu_p(M_2) = \mu_p(M_3) = 0$ and $\mu_p(M_{4,r}) \leq c/q^{1/r}$ in Lemma 2.7(ii) we easily obtain $Q_p(G) = O(q^{-1/2})$. The result follows. ∎

Note that for $p = 2$, $q = 2^k$ and $G = L_2(q)$ the dihedral subgroups $M = D_{2(q\pm1)}$ satisfy $\mu_2(M) = 1/2$, which is why the sum in 2.7(ii) does not tend to 0.

LEMMA 2.14: *Let $G = L_3(q)$, where $q = p^k$. Then $Q_p(G) \to 0$ as $|G| \to \infty$.*

Proof: The argument is similar and is left to the reader. ∎

This completes the proof of Theorem 1.1(ii).

To prove part (iii) we need the following.

LEMMA 2.15: *With the above notation we have*

$$Q_{p,p'}(G) \leq Q(G)\mu_p(G)^{-1}\mu_{p'}(G)^{-1}.$$

Proof: This follows from $Q_{p,p'}(G) \leq Q(G)|G|^2/|R||S|$. ∎

LEMMA 2.16: *Suppose $G \neq L_2(q)$ for some pth power q. Then $Q_{p,p'}(G) \to 0$ as $|G| \to \infty$.*

Proof: Applying Lemmas 2.2 and 2.15 we obtain

$$Q_{p,p'}(G) \leq cm(G)^{-1}\mu_p(G)^{-1}\mu_{p'}(G)^{-1}.$$

For $G = A_n$ this yields $Q_{p,p'}(G) \leq cn^{-1}n^{1/p}$ which tends to 0. Let $G = X_n(q)$. If q is not a pth power then $\mu_p(G) \geq p^{-2}$ and $\mu_{p'}(G) \geq c/n$, and so $Q_{p,p'} \leq cq^{-n}p^2n \to 0$ as $|G| \to \infty$. So let q be a pth power. Then $\mu_p(G)^{-1}\mu_{p'}(G)^{-1} \leq cq$ and we obtain $Q_{p,p'}(G) \leq cm(G)^{-1}q$. Since $G \neq L_2(q)$ it follows from Lemma 2.1 that the right hand side tends to 0. ∎

LEMMA 2.17: *Let $G = L_2(q)$ where $q = p^k$. Then $Q_{p,p'}(G) \to 0$ as $|G| \to \infty$.*

Proof: This follows by applying part (iii) of Lemma 2.7. The details are straightforward and are left to the reader. ∎

The proof of Theorem 1.1 is now complete.

References

[Ba] L. Babai, *The probability of generating the symmetric group*, Journal of Combinatorial Theory, Series A **52** (1989), 148–153.

[BPS] L. Babai, P. P. Pálfy and J. Saxl, *On the number of p-regular elements in simple groups*, Preprint, 2000.

[BLNPS] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger and Á. Seress, *On the proportions of certain types of elements of finite alternating and symmetric groups*, Preprint, 2000.

[D] J. D. Dixon, *The probability of generating the symmetric group*, Mathematische Zeitschrift **110** (1969), 199–205.

[ET] P. Erdős and P. Turán, *On some problems of a statistical group theory. II*, Acta Mathematica Academiae Scientiarum Hungaricae **18** (1967), 151–163.

[IKS] I. M. Isaacs, W. M. Kantor and N. Spaltenstein, *On the probability that a random group element is p-singular*, Journal of Algebra **176** (1995), 139–181.

[Ka] W. M. Kantor, *Some topics in asymptotic group theory*, in *Groups, Combinatorics and Geometry* (M. W. Liebeck and J. Saxl, eds.), Cambridge University Press, 1992.

[KaLu] W. M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geometriae Dedicata **36** (1990), 67–87.

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

[LiSa] M. W. Liebeck and J. Saxl, *On the orders of maximal subgroups of the finite exceptional groups of Lie type,* Proceedings of the London Mathematical Society **55** (1987), 299–330.

[LiSh1] M. W. Liebeck and A. Shalev, *The probability of generating a finite simple group,* Geometriae Dedicata **56** (1995), 103–113.

[LiSh2] M. W. Liebeck and A. Shalev, *Classical groups, probabilistic methods, and the (2,3)-generation problem,* Annals of Mathematics **144** (1996), 77–125.

[LiSh3] M. W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky,* Journal of Algebra **184** (1996), 31–57.

[NiP] A. C. Niemeyer and C. E. Praeger, *A recognition algorithm for classical groups over finite fields,* Proceedings of the London Mathematical Society **77** (1998), 117–169.

[Su] M. Suzuki, *On a class of doubly transitive groups,* Annals of Mathematics **75** (1962), 105–145.