# The expected number of random elements to generate a finite group by Alexander Lubotzky*

**To John Thompson**

Let $G$ be a finite group with a minimal number of generators $d = d(G)$. If one chooses random elements from $G$ independently, and with the uniform distribution, how many should one expect to pick until the elements chosen generate $G$? Call this number $\mathcal{E}(G)$.

Carl Pomerance [Po], motivated by some algorithms for primality testing, studied the question for $G$ abelian. He showed that if $G$ is abelian, $\mathcal{E}(G) \leq d(G) + \sigma$ when $\sigma = 1 + \sum\limits_{j=2}^{\infty}(1 - \prod\limits_{t=2}^{\infty}\zeta(t)^{-1}\prod\limits_{\ell=2}^{j-1}\zeta(\ell)) = 2.118456563\ldots$ and this $\sigma$ is best possible (when $G$ runs over all finite abelian groups). He raised the question of studying $\mathcal{E}(G)$ and $\mathcal{E}(G) - d(G)$ for more general groups.

Igor Pak [P], motivated by potential applications for the Product Replacement Algorithm, studied a closely related invariant: For $k \in \mathbf{N}$, let $d_k(G) = \#\{(x_1, \ldots, x_k) \in G^k \mid \langle x_1, \ldots, x_k\rangle = G\}$, so $\frac{d_k(G)}{|G|^k}$ is the probability of $k$ random elements from $G$ to generate $G$. Pak defined

$$\mathcal{V}(G) = \min\left\{k \in \mathbf{N} \;\middle|\; \frac{d_k(G)}{|G|^k} \geq \frac{1}{e}\right\}.$$

He evaluated $\mathcal{V}(G)$ for various classes of groups $G$, and based on these and estimates in [KL] and [M], he conjectured that $\mathcal{V}(G) = O(d(G)\log\log|G|)$. He also pointed out that up to multiplication by (small) constants $\mathcal{V}(G)$ is roughly $\mathcal{E}(G)$. In particular, he showed that $\mathcal{E}(G) \leq e\mathcal{V}(G)$.

In [DLM], Detoni, Lucchini and Morini proved a weaker form of Pak's conjecture by showing that $\mathcal{V}(G) \leq d(G) + O(\log\log|G|\log\log\log|G|)$. (See there

*This work was partially supported by BSF and NSF grants

for more results in this direction).

In this paper, we answer Pomerance's question and prove Pak's conjecture, in fact in a stronger form.

**Theorem.**

$$\mathcal{V}(G) \leq d(G) + 2\log\log|G| + 4.02.$$

**Corollary.**

$$\mathcal{E}(G) \leq ed(G) + 2e\log\log|G| + 11.$$

For the proof, we introduce a third invariant for $G$: Let $m_n(G)$ denote the number of maximal subgroups of $G$ of index $n$, and let

$$\mathcal{M}(G) = \max_{n\geq 2} \frac{\log m_n(G)}{\log n}.$$

$\mathcal{M}(G)$ is actually the "polynomial degree" of the rate of growth of $m_n(G)$. This rate has been studied in recent years for finite and profinite groups by Mann, Shalev, Borovik, Liebeck and Pyber (see [M], [MS], [BLP] and the references therein). It is roughly equal to $\mathcal{V}(G)$ (see Proposition 1.2 below). Our proof follows the footsteps of these works and in particular it also depends on the classification of the finite simple groups.

In §1, we bring some relations between $\mathcal{E}(G), \mathcal{V}(G)$ and $\mathcal{M}(G)$, and in §2, the theorem is proved. When we write log we always take it in base 2.

**Acknowledgments.** We are grateful to Carl Pomerance and Igor Pak for illuminating discussions which generated our interest in the problem and to Cheryl Praeger, for a crash course she gave me on permutation groups during a walk at the Durham conference 2001, which turned out to contain the main ingredients to solve this problem. We are also grateful to Yale University for its hospitality, and to the NSF and BSF (U.S.-Israel) for their support.

## §1. Some comparisons.

Let $\mathcal{E}(G), \mathcal{V}(G)$ and $\mathcal{M}(G)$ be as in the introduction. More generally, if $G$ is a profinite group, denote by $P_k(G)$ the probability (with respect to the Haar measure $\mu$ of $G^k$) that a $k$-tuple of elements of $G$ generates $G$ topologically. Namely, $P_k(G) = \mu\{(x_1,\ldots,x_k) \in G^k \mid \overline{\langle x_1,\ldots,x_k\rangle} = G\}$. Let
$\tilde{P}_k(G) = \mu\{(x_1,\ldots,x_k) \in G^k \mid \overline{\langle x_1,\ldots,x_k\rangle} = G; \overline{\langle x_1,\ldots,x_{k-1}\rangle} \neq G\}$,

$$\mathcal{E}(G) = \sum_{k=1}^{\infty} k\tilde{P}_k(G)$$
$$\text{and } \mathcal{V}(G) = \min\{k \mid P_k(G) \geq \tfrac{1}{e}\}$$

when we agree that $\mathcal{V}(G) = \infty$ if such $k$ does not exist.

Let $m_n(G)$ be the number of maximal open subgroups of $G$ of index $n$ and

$$\mathcal{M}(G) = \sup_{n \geq 2} \frac{\log m_n(G)}{\log n}.$$

**Proposition 1.1. (Pak [P])**

$$\frac{1}{e}\mathcal{E}(G) \leq \mathcal{V}(G) \leq \frac{e}{e-1}\mathcal{E}(G).$$

This is proved by Pak for finite groups but the same proof works for profinite groups. One can also deduce the result from finite to profinite by observing that if $G = \varprojlim G_i$ then $\mathcal{E}(G) = \lim \mathcal{E}(G_i)$ and $\mathcal{V}(G) = \lim \mathcal{V}(G_i)$.

**Proposition 1.2.**

$$\mathcal{M}(G) - 3.5 \leq \mathcal{V}(G) \leq \mathcal{M}(G) + 2.02.$$

*Proof.* Let us start with the right-hand side inequality:

$$\mathcal{V}(G) = \min\left\{k \mid 1 - P_k(G) < 1 - \frac{1}{e} = \frac{e-1}{e}\right\}.$$

Now,

$$\begin{aligned} 1 - P_k(G) & \leq \sum_{M \text{ maximal}} [G:M]^{-k} \\ & = \sum_{n=2}^{\infty} m_n(G) n^{-k} \leq \sum_{n=2}^{\infty} n^{\mathcal{M}(G)-k}. \end{aligned}$$

Thus, if $k \geq \mathcal{M}(G) + 2.02$, we deduce that

$$1 - P_k(G) \leq \sum_{n=2}^{\infty} \frac{1}{n^{2.02}} = \zeta(2.02) - 1$$

which is smaller than $\frac{e-1}{e}$.

The proofs of Proposition 1.1 and half of Proposition 1.2 are elementary. On the other hand, the proof of the left-hand side inequality of Proposition 1.2, which is actually not needed in the rest of the paper, does require the following result of Pyber whose proof uses the classification of the finite simple groups.

**Theorem 1.3 (Pyber [Py])** *There exists a constant $b$ such that for every finite group $G$ and every $n \geq 2$, $G$ has at most $n^b$ core-free maximal subgroups of index $n$. In fact, $b = 2$ will do.*

Pyber's result is needed for the proof of the main theorems of this paper. Its proof uses, beside the classification, also the detailed description of core-free maximal subgroups as given in Aschbacher-Scott [AS]. Mann and Shalev show in [MS] a slightly weaker form of Theorem 1.3. In their result $b$ depends on $d = d(G)$. Their form implies a slightly weaker inequality in Proposition 1.2 and in the main theorems.

Anyway, the following proof of the left hand side of Proposition 1.2 is not more than a quantitative version of the qualitative result of Mann and Shalev which say that for a profinite group $G$, $\mathcal{V}(G) < \infty$ if and only if $\mathcal{M}(G) < \infty$. In fact, we follow closely Section 4 of [MS]:

Let now $N_i$ be an enumeration of all cores of maximal subgroups of $G$ (each core occuring only once). For each $N_i$ choose a maximal subgroup $M_i$ whose core is $N_i$. Let $C_n(G)$ be the number of the maximal subgroups of index $n$ obtained in this way. The events $M_i^k$ in $G^k$ are pairwise independent and from the (quantitative version of the) Borel-Cantelli lemma, one deduces that $\sum\limits_{n=2}^{\infty} C_n(G)n^{-k} \leq \frac{1}{P_k(G)}$ and in particular, $C_n(G) \leq \frac{n^k}{P_k(G)}$. Taking $k = \mathcal{V}(G)$ we get that

$$C_n(G) \leq e \cdot n^{\mathcal{V}(G)}.$$

Now, Pyber's Theorem (1.3) implies that

$$m_n(G) \leq C_n(G)n^b.$$

Hence, $m_n(G) \leq e \cdot n^{\mathcal{V}(G)+b}$.

It follows that

$$\mathcal{M}(G) = \sup_{n \geq 2} \frac{\log m_n(G)}{\log n} \leq \mathcal{V}(G) + b + \log e \leq \mathcal{V}(G) + 3.5.$$

This proves Proposition 1.2.

We can now restate Mann-Shalev result:

**Corollary 1.4.** For a profinite group $G$, $\mathcal{E}(G) < \infty \Leftrightarrow \mathcal{V}(G) < \infty \Leftrightarrow \mathcal{M}(G) < \infty$.

## §2. Proof of the main theorem.

We will prove the main theorem by proving the following theorem which together with Propositions 1.1 and 1.2 gives the main theorem.

**Theorem 2.1.** *Let $G$ be a finite group. Then $\mathcal{M}(G) \leq d(G) + 2\log\log|G| + 2$.*

To prove Theorem 2.1 we have to bound the number of maximal subgroups of $G$, or equivalently to bound the number of primitive permutational representations of $G$.

The following Proposition summarizes Theorem 4.3B and Theorem 4.7A of [DM] and gives us the needed information about the structure of finite primitive groups.

**Proposition 2.2.** Let $X$ be a primitive permutation group on a set $\Omega$ of size $n$. Then $X$ has at most two minimal normal subgroups $K_1$ and $K_2$, where $K_i \simeq T^k$ when $T$ is a simple group. There are three possibilities:

**(A)**: Affine case: $K = K_1 = K_2$ is a unique abelian minimal normal subgroup of order $n = p^k$ isomorphic to $(\mathbf{Z}/p\mathbf{Z})^k$. $X$ is a semi-direct product of $K$ and $X_\alpha$ - a stabilizer of $\alpha \in \Omega$. $X_\alpha$ is an irreducible subgroup of $GL_k(p)$. The centralizer of $K$ in $X$ is $K$, $C_X(K) = K$.

**(B1)**: $K = K_1 = K_2$ is a unique non-abelian minimal normal subgroup. In this case $C_X(K) = \{1\}$.

**(B2)**: $X$ has two different non-abelian minimal normal subgroups $K_1$ and $K_2$. They are isomorphic to each other, acting regularly on $\Omega, K_1 \cap K_2 = \{1\}$ and $C_X(K_i) = K_{3-i}$ for $i = 1, 2$.

Let $G$ now be a finite group and $1 = N_0 \leq N_1 \leq N_2 \leq \ldots \leq N_r = G$ a chief-series of $G$, i.e., for every $i = 1, \ldots, r$, $N_i \lhd G$ and $N_i/N_{i-1}$ is a minimal normal subgroup of $G/N_{i-1}$. The series is not uniquely defined but $r$ depends only on $G$ as well as the quotients $N_i/N_{i-1}$ as $G$-groups ([H] Theorem 8.4.5 p. 127).

Define $C_i = C_G(N_i/N_{i-1}) = \mathrm{Ker}(G \overset{\pi_i}{\to} \mathrm{Aut}(N_i/N_{i-1}))$ where $\pi_i$ is the natural action of $G$ on $N_i/N_{i-1}$. The collection of subgroups $C = \{C_i\}_{i=1}^r$ is independent of the choice of the chief series.

**Proposition 2.3.** Let $\rho : G \to \mathrm{Sym}(\Omega)$ be a primitive permutational representation and $X = \rho(G)$.

(a) If $X$ is of type A (of (2.2)) with an abelian minimal normal subgroup $K$ and $\tilde{\rho} : G \to X/K$ the composition of $\rho$ and the projection from $X$ to $X/K$, then there exist $i, 1 \leq i \leq r$, such that $\mathrm{Ker}\tilde{\rho} = C_i$

(b1) If $X$ is of type B1, then there exist $i, 1 \leq i \leq r$, such that $\mathrm{Ker}\rho = C_i$.

(b2) If $X$ is of type B2, then there exists $i$ and $j$ in $\{1, \ldots, r\}$, such that $\mathrm{Ker}\rho = C_i \cap C_j$.

*Proof.* For $i$, $1 \leq i \leq r$, $\rho(N_i)/\rho(N_{i-1})$ is either trivial or a chief factor of $X$. Moreover, if it is non-trivial then $N_i/N_{i-1}$ is isomorphic as $G$-group to $\rho(N_i)/\rho(N_{i-1})$ (where $g \in G$ acts on $\rho(N_i)/\rho(N_{i-1})$ via conjugation by $\rho(g)$).

Now, if $K$ is a minimal normal subgroup of $X$, then there exists a smallest $i$, $1 \leq i \leq r$ such that $\rho(N_i) \cap K \neq \{1\}$. For such an $i$, $\rho(N_{i-1}) \cap K = \{1\}$ and $\rho(N_i)$ must contain $K$. As $K$ is a minimal normal subgroup of $X$ and $N_i/N_{i-1}$ of $G/N_{i-1}$, $K$ is isomorphic as a $G$-group to $N_i/N_{i-1}$ (via $\rho$). This implies that $\rho(C_i) \leq C_X(K)$. In fact, it implies that $\rho(C_i) = C_X(K)$ since if $x \notin C_i$, it acts non-trivially on $N_i/N_{i-1}$ and hence $\rho(x)$ acts non-trivially on $K$. This observation and Proposition 2.2 prove all parts of Proposition 2.3.

If $M$ is a maximal subgroup of $G$, we will say that $M$ is of type $A$ (resp. $B$) if the (primitive) permutation group induced by $G$ on the coset space $G/M$ is of type $A$ (resp. $B_1$ or $B_2$) of Proposition 2.2. Let $m_n^A(G)$ (resp. $m_n^B(G)$) be the number of maximal subgroups of $G$ of type $A$ (resp. $B$) of index $n$.

Let $r_a(G)$ (resp., $r_b(G)$) be the number of abelian (resp. non-abelian) chief factors of $G$. So $r_a(G) + r_b(G) = r$.

**Claim 2.4.** $m_n^B(G) \leq \frac{1}{2}(r_b(G)+1)r_b(G)n^2$.

*Proof:* By Proposition 2.3 parts (b1) and (b2), the core of a maximal subgroup $M$ of $G$ of type $B$ is equal to $C_i \cap C_j$ for some $1 \leq i, j \leq n$ ($i$ may be equal to $j$). It is clear that in this case, $i$ and $j$ come from non-abelian chief factors, so the number of possibilities for $\{i,j\}$ is at most $\frac{1}{2}(r_b(G)+1)r_b(G)$. Given the core, there are at most $n^2$ maximal subgroups with this core, by Theorem 1.3.

We need now to bound $m_n^A(G)$, i.e., the number of affine primitive representations of $G$ of degree $n$. We saw in (2.3)(a), that a maximal subgroup $M$ of type $A$ determines a primitive representation $\rho : G \to X$ where $X$ has a unique abelian minimal normal subgroup $K$. Now, $K$ is an abelian chief factor of $X$ and hence isomorphic as a $G$-group to one of the $r_a(G)$ abelian chief factors of $G$, say $N_i/N_{i-1}$. Moreover, by Proposition 2.2(A) and Proposition 2.3(a) we know that if $\tilde{\rho} : G \to X/K$ is the induced map, then Ker$\tilde{\rho} = C_i$ and $X$ is isomorphic to the semi-direct product $N_i/N_{i-1} \rtimes G/C_i \simeq K \rtimes X/K$. The kernel of $\rho$ is not unqiuely determined by Ker$\tilde{\rho}$, but $\rho$ is a homomorphism from $G$ to $K \rtimes X/K$ whose projection to $X/K$ is the given $\tilde{\rho}$, which is determined by the choice of $i$. One can easily see that given $i$ (and $\tilde{\rho}$) $\rho$ determines (and it is determined) by a cocycle $\sigma : G \to K$, a cocycle with respect to the $G$-action on $K$. The number of these cocycles is equal to $Z^1(G,K)$ which is bounded by $|K|^{d(G)}$, since every cocycle is determined by its values on the generators.

Now, if $M$ is a maximal subgroup of type $A$ and index $n$, then by Proposition 2.2(A), the action of the minimal normal subgroup $K$ of $X = \rho(G)$ on $G/M$ is regular, in particular $|K| = n$. We therefore deduce:

**Claim 2.5.** $m_n^A(G) \leq r_a(G) \cdot n^{d(G)+2}$.

*Proof:* By the discussion above, the number of possible cores of maximal subgroups of type $A$ is at most $r_a(G)n^{d(G)}$. Given the core there are at most $n^2$ maximal subgroups of index $n$ with that core, by Theorem 1.3.

**Corollary 2.6.** $m_n(G) = m_n^A(G) + m_n^B(G) \leq$

$$\begin{aligned}&(\tfrac{1}{2}((r_b(G)+1)(r_b(G)) + r_a(G)n^{d(G)})n^2\\ &\leq r^2 n^{d(G)+2}.\end{aligned}$$

Finally as $\mathcal{M}(G) = \max\limits_n \frac{\log m_n(G)}{\log n}$, we deduce:

$$\mathcal{M}(G) \leq d(G) + 2\log r + 2.$$

As $r < \log G$, Theorem 2.1 is proved.

**Remark.** There is some "significant waste" in the proof. The contribution of the non-affine permutation representations is at most $r^2n^2$ and hence to $\mathcal{M}(G)$ it contributes at most $\frac{2\log r}{\log n} + 2$. We estimated this from above by $2\log r + 2$ which is of course ridiculous if $n$ is large. We also allow a "waste" in the second inequality of Corollary 2.6. Let's now estimate it in a slightly more careful way, keeping the notations as above and denoting $i(G)$ to be the smallest index of a proper subgroup of $G$.

Now, by Corollary 2.6,

$$m_n(G) \leq (\frac{1}{2}(r+1)r + rn^{d(G)})n^2 \leq r(r + n^{d(G)})n^2$$

and so:

$$\mathcal{M}(G) = \max_{n\geq 2} \frac{\log m_n(G)}{\log n} \leq 2 + \frac{1+\log r}{\log n} + \max(d(G), \frac{\log r}{\log n}).$$

Hence, we get:

**Corollary 2.7** $\mathcal{M}(G) \leq \frac{1+\log\log|G|}{\log i(G)} + \max(d(G), \frac{\log\log|G|}{\log i(G)}) + 2$.

So, for the sequence of groups $G_k = (A_k)^{k!/8}$ (discussed in [KL] and [P]). The main theorem as stated gives $\mathcal{V}(G_k) = O(k\log k)$. But, in fact, $i(G_k) = k$, so Corollary 2.7 shows that $\mathcal{V}(G_k) = O(k)$ - which is the correct estimate - see [P]).

The referee also showed us how the 2 can be dropped in Corollary 2.7, but as the proof needs some further analysis into the structure of primitive groups, we will not bring the details.

These improvements give a slightly sharper form of the main Theorem as:
**Corollary 2.8** $\mathcal{V}(G) \leq \frac{1+\log\log|G|}{\log i(G)} + \max(d(G), \frac{\log\log|G|}{\log i(G)}) + 2.02$.

## References

[AS] M. Aschbacher and L. Scott, Maximal subgroups of finite groups, J. Algebra 92 (1985) 44-80.

[BPS] A.V. Borovik, L. Pyber, A. Shalev, Maximal subgroups in finite and profinite groups, Trans. AMS 348 (1996), 3745-3761.

[DLM] E. Detoni, A. Lucchini and F. Morini, How many elements are needed to generate a finite group with good probability?, preprint.

[DM] J.D Dixon and B. Mortimer, Permutations Groups, Springer 1996.

[H] M. Hall, The Theory of Groups, The Macmillan Company, NY 1959.

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

[M] A. Mann, Positively finitely generated groups, Forum Math. 8 (1996) 429-459.

[MS] A. Mann, A. Shalev, Simple groups, maximal subgroups and probabilstic aspects of profinite groups, Israel J. Math. 96 (1996) 449-468.

[P] I. Pak, On probability of generating a finite group, preprint 1999.

[Po] C. Pomerance, The expected number of random elements to generate a finite abelian group. Period. Math. Hungar. **43** (2001), no. 1-2, 191-198.

[Py] L. Pyber, in preparation.

Institute of Mathematics
Hebrew University
Jerusalem 91904
ISRAEL