**Advances in Group Theory and Applications**

9 (2020), pp. 39–49 ISSN: 2499-1287
DOI: 10.32037/agta-2020-002

# Generation of Finite Groups and Maximal Subgroup Growth

Andrea Lucchini — Mariapia Moscatiello

(*Received May 8, 2019; Accepted June 22, 2019 — Communicated by F. de Giovanni*)

## Abstract

Let $G$ be a finite group and, for $n \in \mathbb{N}$, denote by $m_n(G)$ the number of maximal subgroups of $G$ with index $n$. Let

$$\mathcal{M}(G) = \sup_{n \geqslant 2} \log m_n(G)/\log n$$

and let $E_1(G)$ be the expected number of elements of $G$ which have to be drawn at random, with replacement, before a set of generators is found. Then

$$\lceil \mathcal{M}(G) \rceil - 4 \leqslant E_1(G) \leqslant \lceil \mathcal{M}(G) \rceil + 3.$$

*Mathematics Subject Classification (2010)*: 20P05
*Keywords*: waiting time; generation of finite groups

## 1 Introduction

Let $G$ be a nontrivial finite group and let $x = (x_n)_{n \in \mathbb{N}}$ be a sequence of independent, uniformly distributed $G$-valued random variables. We may define a random variable $\tau_G$ (a waiting time) by

$$\tau_G = \min\{n \geqslant 1 \mid \langle x_1, \dots, x_n \rangle = G\} \in [1, +\infty].$$

Notice that $\tau_G > n$ if and only if $\langle x_1, \dots, x_n \rangle \neq G$, so we have

$$P(\tau_G > n) = 1 - P_G(n),$$

denoting by

$$P_G(n) = \frac{|\{(g_1, \dots, g_n) \in G^n \mid \langle g_1, \dots, g_n \rangle = G\}|}{|G|^n}$$

the probability that $n$ randomly chosen elements of $G$ generate $G$. We denote by $E_1(G)$ the expectation $E(\tau_G)$ of this random variable. In other word $E_1(G)$ is the expected number of elements of $G$ which have to be drawn at random, with replacement, before a set of generators is found.

Significant estimations for the value of $E_1(G)$ have been obtained by A. Lubotzky in [5]. More precisely he estimated another related invariant, defined by I. Pak:

$$\mathcal{V}(G) = \min \left\{ k \in \mathbb{N} \;\middle|\; P_G(k) \geqslant \frac{1}{e} \right\}.$$

As it was noticed by I. Pak (see for example Proposition 1.1 of [5]), $E_1(G)$ and $\mathcal{V}(G)$ are related in the following way:

$$\frac{1}{e} \cdot E_1(G) \leqslant \mathcal{V}(G) \leqslant \frac{e}{e-1} \cdot E_1(G). \tag{1.1}$$

For $n \in \mathbb{N}$, denote by $m_n(G)$ the number of maximal subgroups of $G$ with index $n$ and let

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

Actually $\mathcal{M}(G)$ is the "polynomial degree" of the rate of growth of $m_n(G)$. This rate has been studied for finite and profinite groups by Mann, Shalev, Borovik, Jaikin-Zapirain, Liebeck, Pyber and more recently by Ballester-Bolinches, Esteban-Romero, Jiménez-Seral and Hangyang Meng (see [2],[3],[9],[10],[1]). It is roughly equal to $\mathcal{V}(G)$, indeed we have (see Proposition 1.2 of [5]):

$$\mathcal{M}(G) - 3.5 \leqslant \mathcal{V}(G) \leqslant \mathcal{M}(G) + 2.02. \tag{1.2}$$

The estimation for $E_1(G)$ given by Lubotzky is obtained combining (1.1) and (1.2):

$$(\mathcal{M}(G) - 3.5) \cdot \frac{e-1}{e} \leqslant E_1(G) \leqslant (\mathcal{M}(G) + 2.02) \cdot e. \quad (1.3)$$

However this estimation leaves open the question whether

$$|\mathcal{M}(G) - E_1(G)|$$

could be arbitrarily large. The main observation of this paper is that the arguments used in [5] can be improved and the following result can be obtained.

**Theorem 1.1** *Let* $G$ *be a finite group. Then*

$$\lceil \mathcal{M}(G) \rceil - 4 \leqslant E_1(G) \leqslant \lceil \mathcal{M}(G) \rceil + 3.$$

Other numerical invariants may be derived from $\tau_G$ starting from the higher moments

$$E(\tau_G^k) = \sum_{n \geqslant 1} n^k P(\tau_G = n).$$

In particular it is probabilistically important, when the expectation of a random variable is known, to have control over its second moment. We will denote by $E_2(G)$ the second moment $E(\tau_G^2)$ and by

$$\mathrm{var}(\tau_G) = E_2(G) - E_1(G)^2$$

the variance of $\tau_G$.

**Theorem 1.2** *Let* $G$ *be a finite group. Then*

$$\lceil \mathcal{M}(G) \rceil^2 - 8\lceil \mathcal{M}(G) \rceil + 13 \leqslant E_2(G) \leqslant \lceil \mathcal{M}(G) \rceil^2 + 6\lceil \mathcal{M}(G) \rceil + 14 + \frac{\pi^2}{3}.$$

**Corollary 1.3** $\mathrm{var}(\tau_G) \leqslant 14\lceil \mathcal{M}(G) \rceil + \frac{\pi^2}{3} - 2.$

In [7] it is proved that $E_1(G)$ and $E_2(G)$ can be directly determined using the Möbius function defined on the subgroup lattice of $G$ by setting $\mu(G) = 1$ and $\mu(H) = -\sum_{H<K} \mu(K)$ for any $H < G$. More

precisely (see Theorem 1 and Theorem 3 of [7]):

$$E_1(G) = -\sum_{H<G} \frac{\mu(H)|G|}{|G|-|H|}, \quad E_2(G) = -\sum_{H<G} \frac{\mu(H)|G|(|G|+|H|)}{(|G|-|H|)^2} \tag{1.4}$$

Combining (1.4) with Theorems 1.1 and 1.2 we deduce:

**Proposition 1.4** *For every finite group* $G$, *we have*

$$\lceil \mathcal{M}(G) \rceil - 4 \leqslant -\sum_{H<G} \frac{\mu(H)|G|}{|G|-|H|} \leqslant \lceil \mathcal{M}(G) \rceil + 3,$$

$$\lceil \mathcal{M}(G) \rceil^2 - 8\lceil \mathcal{M}(G) \rceil + 13 \leqslant -\sum_{H<G} \frac{\mu(H)|G|(|G|^2+|G||H|)}{(|G|-|H|)^2}$$

$$\leqslant \lceil \mathcal{M}(G) \rceil^2 + 6\lceil \mathcal{M}(G) \rceil + 14 + \frac{\pi^2}{3}.$$

In 1991 L.G. Kovács and Hyo-Seob Sim proved that if a finite soluble group $G$ has a family of $d$-generator subgroups whose indices have no common divisor, then $G$ can be generated by $d+1$ elements (see Theorem 2 of [4]). A probabilistic version of this theorem has been given in [8]. With the help of Theorem 1.1 we may obtain another result in this direction.

**Theorem 1.5** *Let* $G$ *be a finite soluble group. Assume that for every prime* $p$ *dividing* $|G|$, *there exists* $G_p \leqslant G$ *such that* $p$ *does not divide* $|G : G_p|$ *and* $E_1(G_p) \leqslant \rho$. *Then* $E_1(G) \leqslant \rho + 9$.

The definition of $E_1(G)$ can be extended to the case of a (topologically) finitely generated profinite group $G$. If we denote with $\mu$ the normalized Haar measure on $G$, so that $\mu(G) = 1$, the probability that $k$ random elements generate (topologically) $G$ is defined as

$$P_G(k) = \mu(\{(x_1, \dots, x_k) \in G^k | \langle x_1, \dots, x_k \rangle = G\}),$$

where $\mu$ denotes also the product measure on $G^k$. As it is proved for example in Section 6 of [7],

$$E_1(G) = \sup_{N \in \mathcal{N}} E_1(G/N),$$

where $\mathcal{N}$ is the set of the open normal subgroups of $G$. This implies that the inequalities in Theorems 1.1 and 1.2 still hold if $G$ is a finitely generated profinite group. Recall that a profinite group $G$ is said to

be positively finitely generated, PFG for short, if $P_G(k)$ is positive for some natural number $k$ and that $G$ is said to have polynomial maximal subgroup growth if $m_n(G) \leqslant \alpha n^\sigma$ for all $n$ (and for some constant $\alpha$ and $\sigma$). The profinite version of Theorem 1.1 can be considered as a quantitative version of the celebrated result of Mann and Shalev [10], saying that a profinite group is PFG if and only if it has polynomial maximal subgroup growth.

## 2 Proof of Theorem 1.1

For a real number $\eta \geqslant 1$, let us define

$$\mathcal{V}_\eta(G) = \min\left\{ k \in \mathbb{N} \;\middle|\; P_G(k) \geqslant \frac{1}{\eta} \right\}.$$

The argument used by Lubotzky to bound $\mathcal{V}(G) = \mathcal{V}_e(G)$, can be adapted to bound $\mathcal{V}_\eta(G)$, for an arbitrarily value of $\eta$. The proof is essentially the same, but for reader's convenience we prefer to give the details. In the following, when we write log we always take it in base 2.

It was proved by Pyber (see Theorem 1.3 of [5]) that there exists a constant $b$ such that for every finite group $G$ and every $n \geqslant 2$, $G$ has at most $n^b$ core-free maximal subgroups of index $n$. In fact, $b = 2$ will do.

**Lemma 2.1** $\mathcal{V}_\eta(G) \geqslant \mathcal{M}(G) - b - \log\eta \geqslant \mathcal{M}(G) - 2 - \log\eta$.

Proof — Let $N_i$ 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

$$\sum_{n=2}^{\infty} C_n(G) n^{-k} \leqslant \frac{1}{P_k(G)}$$

and in particular,

$$C_n(G) \leqslant \frac{n^k}{P_k(G)}.$$

Taking $k = \mathcal{V}_\eta(G)$ we get that

$$C_n(G) \leqslant \eta \cdot n^{\mathcal{V}_\eta(G)}.$$

Now, Pyber's Theorem implies that

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

Hence, $m_n(G) \leqslant \eta \cdot n^{\mathcal{V}_\eta(G)+b}$. It follows that

$$\mathcal{M}(G) = \sup_{n \geqslant 2} \frac{\log m_n(G)}{\log n} \leqslant \mathcal{V}_\eta(G) + b + \log \eta.$$

This concludes our proof. □

We recall the following formula (see for example (1.1) of [7]).

**Lemma 2.2** $E_1(G) = \sum_{n \geqslant 0}(1 - P_G(n))$.

**Lemma 2.3** $\lceil \mathcal{M}(G) \rceil - 4 \leqslant E_1(G)$.

Proof — By Lemma 2.1, for every positive integer $i$, we have

$$\mathcal{V}_{2^i}(G) \geqslant \mathcal{M}(G) - b - \log(2^i) \geqslant \mathcal{M}(G) - 2 - i.$$

In particular if $k = \lceil \mathcal{M}(G) \rceil - 3 - i$, then $P_G(k) < 2^{-i}$. Let $m = \lceil \mathcal{M}(G) \rceil$. It follows from Lemma 2.2 that

$$\begin{aligned} E_1(G) &\geqslant \sum_{0 \leqslant k \leqslant m-4} (1 - P_G(k)) \geqslant \sum_{0 \leqslant k \leqslant m-4} \left(1 - 2^{k-(m-3)}\right) \\ &= m - 3 - \sum_{1 \leqslant j \leqslant m-3} 2^{-j} \geqslant m - 3 - \sum_{j \geqslant 1} 2^{-j} = m - 4. \end{aligned}$$

This concludes our proof. □

**Lemma 2.4** $E_1(G) \leqslant \lceil \mathcal{M}(G) \rceil - 3$.

Proof — Let $m = \lceil \mathcal{M}(G) \rceil$ and $k = m + t$ with $t$ a positive integer. As it is noticed in the proof of Proposition 11.2.2 of [6] we have

$$1 - P_G(k) \leqslant \sum_{n \geqslant 2} \frac{m_n(G)}{n^k} \leqslant \sum_{n \geqslant 2} \frac{n^{\mathcal{M}(G)}}{n^k} \leqslant \sum_{n \geqslant 2} \frac{n^m}{n^k} \leqslant \sum_{n \geqslant 2} \frac{1}{n^t}.$$

It follows that

$$E_1(G) = \sum_{k\geqslant 0}(1-P_G(k)) \leqslant m+2+\sum_{k\geqslant m+2}(1-P_G(k))$$
$$\leqslant m+2+\sum_{u\geqslant 2}\left(\sum_{n\geqslant 2} n^{-u}\right) = m+2+\left(\sum_{n\geqslant 2}\left(\sum_{u\geqslant 2} n^{-u}\right)\right)$$
$$= m+2+\sum_{n\geqslant 2}\frac{n}{n^2(n-1)} = m+2+\left(\sum_{n\geqslant 1}\frac{1}{n(n+1)}\right) = m+3.$$

This concludes our proof. □

## 3 Proof of Theorem 1.2

We recall the following formula (see for example Lemma 18 of [7]).

**Lemma 3.1** $E_1(G)+E_2(G) = 2\sum_{n\geqslant 0}(n+1)(1-P_G(n))$.

**Lemma 3.2** $E_1(G)+E_2(G) \leqslant \lceil \mathcal{M}(G)\rceil^2 + 7\lceil \mathcal{M}(G)\rceil + 10 + \frac{\pi^2}{3}$.

Proof — Setting $m = \lceil \mathcal{M}(G)\rceil$ and using Lemma 3.1, we deduce

$$E_1(G)+E_2(G) = 2\sum_{k\geqslant 0}(k+1)(1-P_G(k))$$
$$\leqslant 2\sum_{0\leqslant k<m+2}(k+1) + 2\sum_{k\geqslant m+2}(k+1)(1-P_G(k))$$
$$= (m+2)(m+3) + 2\sum_{k\geqslant m+2}(k+1)(1-P_G(k)).$$

To conclude it suffices to estimate $\sum_{k\geqslant m+2}(k+1)(1-P_G(k))$.

$$\sum_{k\geqslant m+2}(k+1)(1-P_G(k)) \leqslant \sum_{k\geqslant m+2}(k+1)\left(\sum_{n\geqslant 2}\frac{n^m}{n^k}\right)$$
$$= \sum_{n\geqslant 2}\left(\sum_{u\geqslant 2}\frac{u+1+m}{n^u}\right) = \sum_{n\geqslant 2}\left(\sum_{u\geqslant 2}\frac{u-1}{n^u}\right) + \sum_{n\geqslant 2}\left(\sum_{u\geqslant 2}\frac{m+2}{n^u}\right)$$

$$= \sum_{n \geqslant 2} \left( \sum_{u \geqslant 1} \frac{1}{n^u} \right)^2 + \sum_{n \geqslant 2} \frac{n(m+2)}{n^2(n-1)}$$

$$= \sum_{n \geqslant 2} \left( \frac{1}{n-1} \right)^2 + m + 2 = m + 2 + \frac{\pi^2}{6}.$$

This concludes our proof. □

**Corollary 3.3** $E_2(G) \leqslant \lceil \mathcal{M}(G) \rceil^2 + 6\lceil \mathcal{M}(G) \rceil + 14 + \frac{\pi^2}{3}$.

Proof — Combining Lemma 3.2 and Lemma 2.3, we deduce

$$E_2(G) \leqslant \lceil \mathcal{M}(G) \rceil^2 + 7\lceil \mathcal{M}(G) \rceil + 10 + \frac{\pi^2}{3} - E_1(G)$$

$$\leqslant \lceil \mathcal{M}(G) \rceil^2 + 7\lceil \mathcal{M}(G) \rceil + 10 + \frac{\pi^2}{3} - (\lceil \mathcal{M}(G) \rceil - 4)$$

$$= \lceil \mathcal{M}(G) \rceil^2 + 6\lceil \mathcal{M}(G) \rceil + 14 + \frac{\pi^2}{3}.$$

This concludes our proof. □

**Lemma 3.4** $E_1(G) + E_2(G) \geqslant \lceil \mathcal{M}(G) \rceil^2 - 7\lceil \mathcal{M}(G) \rceil + 10$.

Proof — Setting $m = \lceil \mathcal{M}(G) \rceil$ and applying Lemmas 2.1 and 3.1, we obtain

$$\frac{e_1(G) + e_2(G)}{2} \geqslant \sum_{0 \leqslant k \leqslant m-4} (k+1)(1 - P_G(k))$$

$$\geqslant \sum_{0 \leqslant k \leqslant m-4} (k+1) \left( 1 - 2^{k-(m-3)} \right)$$

$$= \frac{(m-2)(m-3)}{2} - \sum_{1 \leqslant j \leqslant m-3} \frac{m-2-j}{2^j}$$

$$\geqslant \frac{(m-2)(m-3)}{2} + \sum_{1 \leqslant j \leqslant m-3} \frac{j}{2^j} - \sum_{j \geqslant 1} \frac{m-2}{2^j}$$

$$\geqslant \frac{(m-2)(m-3)}{2} - (m-2).$$

This concludes our proof. □

**Corollary 3.5** $E_2(G) \geqslant \lceil \mathcal{M}(G) \rceil^2 - 8\lceil \mathcal{M}(G) \rceil + 13$.

Proof — Combining Lemma 3.4 and Lemma 2.4, we deduce

$$\begin{aligned} E_2(G) &\geqslant \lceil \mathcal{M}(G) \rceil^2 - 7\lceil \mathcal{M}(G) \rceil + 10 - E_1(G) \\ &\geqslant \lceil \mathcal{M}(G) \rceil^2 - 7\lceil \mathcal{M}(G) \rceil + 10 - (\lceil \mathcal{M}(G) \rceil - 3) \\ &= \lceil \mathcal{M}(G) \rceil^2 - 8\lceil \mathcal{M}(G) \rceil + 13. \end{aligned}$$

This concludes our proof. □

# 4 Proof of Theorem 1.5

It can be easily seen that for every finite soluble group $G$ and every $n \geqslant 2$, $G$ has at most $n$ core-free maximal subgroups of index $n$. This means that the constant $b$ in the statement of Lemma 2.1 can be taken equal to 1 in the case of finite soluble groups and consequently we have:

**Lemma 4.1** *If $G$ is a finite soluble group, then*

$$\lceil \mathcal{M}(G) \rceil - 3 \leqslant E_1(G) \leqslant \lceil \mathcal{M}(G) \rceil + 3.$$

**Lemma 4.2** *Let $G$ be a finite soluble group. There exists a prime divisor $p$ of the order of $G$ and a positive integer $a$ such that*

$$m_{p^a}(G) = p^{a \cdot \mathcal{M}(G)}.$$

*If $H$ is a subgroup of $G$ containing a Sylow $p$-subgroup of $G$, then*

$$\mathcal{M}(G) \leqslant \mathcal{M}(H) + 3.$$

Proof — Let $m = \mathcal{M}(G)$. Since the maximal subgroups of $G$ have prime-power indices, there exists a prime divisor $p$ of the order of $G$ and a positive integer $a$ such that $m_{p^a}(G) = p^{a \cdot m}$. Let $H$ be a subgroup of $G$ containing a Sylow $p$-subgroup of $G$ and let $\mu = \mathcal{M}(H)$. It follows from (2.4) of [8] that

$$p^{a \cdot m} = m_{p^a}(G) \leqslant \sum_{b \leqslant a} p^{a+b} m_{p^b}(H) \leqslant \sum_{b \leqslant a} p^{a+b} p^{b \cdot \mu} \leqslant p^{3 \cdot a + \mu \cdot a},$$

hence $m \leqslant 3 + \mu$. □

Proof of Theorem 1.5 — By Lemma 4.2, there exists a prime divisor $p$ of $G$, such that

$$\mathcal{M}(G) \leqslant \mathcal{M}(G_p) + 3.$$

But then we deduce from Lemma 4.1, that

$$E_1(G) \leqslant \lceil \mathcal{M}(G) \rceil + 3 \leqslant \lceil \mathcal{M}(G_p) \rceil + 6 \leqslant E_1(G_p) + 9.$$

The theorem is proved. □

# REFERENCES


[1] A. Ballester-Bolinches – R. Esteban-Romero – P. Jiménez-Seral – Hangyang Meng: "Bounds on the number of maximal subgroups with applications to random generation of finite groups", preprint.

[2] A.V. Borovik – L. Pyber – A. Shalev: "Maximal subgroups in finite and profinite groups", *Trans. Amer. Math. Soc.* 348 (1996), 3745–3761.

[3] A. Jaikin-Zapirain – L. Pyber: "Random generation of finite and profinite groups and group enumeration", *Ann. Math.* 173 (2011), 769–814.

[4] L. G Kovács – Hyo-Seob Sim: "Generating finite soluble groups", *Indag. Math. (N.S.)* 2 (1991), 229–232.

[5] A. Lubotzky: "The expected number of random elements to generate a finite group", *J. Algebra* 257 (2002), 452–459.

[6] A. Lubotzky – D. Segal: "Subgroup Growth", *Birkhäuser*, Basel (2003).

[7] A. Lucchini: "The expected number of random elements to generate a finite group", *Monatsh. Math.* 181 (2016), 123-–142.

[8] A. Lucchini – M. Moscatiello: "A probabilistic version of a theorem of Laszlo Kovacs and Hyo-Seob Sim", *Int. J. Group Theory* 9 (2020), n.1, 1–6.

[9] A. Mann: "Positively finitely generated groups", *Forum Math.* 8 (1996), 429–459.

[10] A. Mann – A. Shalev: "Simple groups, maximal subgroups and probabilistic aspects of profinite groups", *Israel J. Math.* 96 (1996), 449–468.

---

Andrea Lucchini, Mariapia Moscatiello
Dipartimento di Matematica "Tullio Levi-Civita"
Università di Padova
Via Trieste, 63
35131 Padova (Italy)
e-mail: lucchini@math.unipd.it
mariapia.moscatiello@math.unipd.it