www.theoryofgroups.ir

**International Journal of Group Theory**
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (201x), pp. xx-xx.

www.ui.ac.ir

# A PROBABILISTIC VERSION OF A THEOREM OF LÁSZLÓ KOVÁCS AND HYO-SEOB SIM

ANDREA LUCCHINI* AND MARIAPIA MOSCATIELLO

Communicated by Patrizia Longobardi

Abstract. For a finite group group, denote by $\mathcal{V}(G)$ the smallest positive integer $k$ with the property that the probability of generating $G$ by $k$ randomly chosen elements is at least $1/e$. Let $G$ be a finite soluble group. Assume that for every $p \in \pi(G)$ there exists $G_p \leq G$ such that $p$ does not divide $|G : G_p|$ and $\mathcal{V}(G_p) \leq d$. Then $\mathcal{V}(G) \leq d + 7$.

## 1. Introduction

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 [4, Theorem 2]). In this short note we want to present a probabilistic version of this theorem.

For $k \in \mathbb{N}$, let $\phi_k(G)$ be the number of ordered $k$-tuples $(x_1, \ldots, x_k) \in G^k$ such that $\langle x_1, \ldots, x_k \rangle = G$, so

$$P_G(k) = \frac{\phi_k(G)}{|G|^k}$$

is the probability of $k$ random elements from $G$ to generate $G$. I. Pak defined

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

MSC(2010): Primary: 20P05; Secondary: 20D60.
Keywords: Finite soluble groups; generation of finite groups.
Received: 14 August 2018, Accepted: 20 November 2018.
∗Corresponding author.
http://dx.doi.org/10.22108/ijgt.2017.21483

.

He also pointed out that up to multiplication by (small) constants $\mathcal{V}(G)$ is roughly $\mathcal{E}(G)$, where $\mathcal{E}(G)$ denotes the expected number of elements of $G$ chosen randomly before a set of generators is found.

Assume now that a finite soluble group $G$ has a family $H_1, \dots, H_t$ of subgroups whose indices have no common divisor and such that $\mathcal{V}(H_i) \leq d$ for every $1 \leq i \leq d$. Is it true that $\mathcal{V}(G)$ can be bounded in term of $d$? We prove that the answer is affirmative.

**Theorem 1.** *Let $G$ be a finite soluble group. Assume that for every $p \in \pi(G)$ there exists $G_p \leq G$ such that $p$ does not divide $|G : G_p|$ and $\mathcal{V}(G_p) \leq d$. Then $\mathcal{V}(G) \leq d + 7$.*

## 2. A preliminary remark

Let $G$ be a finite soluble group and let $\Sigma(G)$ be the set of the maximal subgroups of $G$. For $M \in \Sigma(G)$, denote by $M_G = \bigcap_{g \in G} M^g$ the normal core of $M$ in $G$: clearly $\mathrm{soc}(G/M_G)$ is a chief factor of $G$ and $M/M_G$ is a complement of $\mathrm{soc}(G/M_G)$ in $G/M_G$. Let $\mathcal{A}(G)$ be a set of representatives of the irreducible $G$-modules that are $G$-isomorphic to some chief factor of $G$ having a complement and, for every $V \in \mathcal{A}(G)$, let $\Sigma_V(G)$ be the set of maximal subgroups $M$ of $G$ with $\mathrm{soc}(G/M_G) \cong_G V$. Recall some results by Gaschütz [2]. Let

$$R_G(A) = \bigcap_{M \in \Sigma_V(G)} M_G.$$

It turns out that $R_G(A)$ is the smallest normal subgroup contained in $C_G(A)$ with the property that $C_G(A)/R_G(A)$ is $G$-isomorphic to a direct product of copies of $A$ and it has a complement in $G/R_G(A)$. The factor group $C_G(A)/R_G(A)$ is called the $A$-crown of $G$. The non-negative integer $\delta_G(A)$ defined by $C_G(A)/R_G(A) \cong_G A^{\delta_G(A)}$ is called the $A$-rank of $G$ and it coincides with the number of complemented factors in any chief series of $G$ that are $G$-isomorphic to $A$ (see for example [1, Section 1.3]). In particular $G/R_G(A) \cong A^{\delta_G(A)} \rtimes H$, with $H \cong G/C_G(A)$. Now set $q_G(V) = |\operatorname{End}_G V|$, $\epsilon_G(V) = 0$ if $V$ is a trivial $G$-module, 1 otherwise. We have

$$|\Sigma_V(G)| = \frac{\left(q_G(V)^{\delta_G(V)} - 1\right) |V|^{\epsilon_G(V)}}{q_G(V) - 1}. \tag{2.1}$$

Now assume that $H$ is a subgroup of $G$ containing a Sylow $p$-subgroup of $G$. We want to compare $\Sigma_p(G)$ and $\Sigma_p(H)$, where, for a finite soluble group $X$, $\Sigma_p(X)$ denotes the set of the maximal subgroups of $G$ whose index is a $p$-power. Let $\mathcal{A}_p(G)$ be the set of the irreducible $G$-modules $V \in \mathcal{A}(G)$ whose order is a $p$-power.

Fix $V \in \mathcal{A}_p(G)$, let $\delta = \delta_G(V)$, $q = q_G(V)$, $R = R_G(V)$. Moreover set $\overline{G} = G/R$ and $\overline{H} = HR/R$. We have

$$\overline{G} \cong V^\delta \rtimes X \text{ with } X \leq \operatorname{Aut} V.$$

Since $\overline{H}$ contains a Sylow $p$-subgroup of $\overline{G}$, $V^\delta \leq \overline{H}$ and, by the Dedeking law,

$$\overline{H} = \overline{G} \cap \overline{H} = V^\delta X \cap \overline{H} = V^\delta (X \cap \overline{H}),$$

hence

$$\overline{H} \cong V^\delta \rtimes Y \text{ with } Y = X \cap \overline{H}.$$

Now let $U$ be an irreducible $H$-module that can be obtained as an $H$-epimorphic image of $V$ (viewed as an $H$-module) and define

$$\Omega_U := \{Z \leq_H V \mid V/Z \cong_H U\}, \quad J_U := \bigcap_{Z\in\Omega_U} Z.$$

There exists $t \in \mathbb{N}$ such that $V/J_U \cong_H U^t$ and $\delta^* := \delta_H(U) \geq t \cdot \delta$. Notice that if $Z \in \Omega_U$ and $\alpha \in F = \operatorname{End}_G V$, then $Z^{\alpha h} = Z^{h\alpha} = Z^\alpha$ for every $h \in H$, i.e. $Z^\alpha \leq_H V$. Moreover, if $\alpha \neq 0$, then the map

$$V/Z \to V/Z^\alpha$$

$$v + Z \mapsto v^\alpha + Z^\alpha$$

is an $H$-isomorphism, so $V/Z \cong_H V/Z^\alpha$ and $Z^\alpha \in \Omega_U$. It follows that $J_U$ is $F$-invariant and there is a ring homomorphism

$$F \to \operatorname{End}_H(V/J_U) \cong \operatorname{End}_H(U^t) \cong M_{t\times t}(\operatorname{End}_H U).$$

Let $r = |\operatorname{End}_H U|$ and suppose $F^* = \langle a\rangle$. We have that $\langle a\rangle \leq \mathrm{GL}(t, r)$ and this implies $|a| \leq r^t - 1$. In particular

$$q \leq r^t. \tag{2.2}$$

Notice that

$$|\Sigma_U(H)| = \frac{r^{\delta^*} - 1}{r-1}|U|^{\epsilon_U} \geq \frac{r^{t\cdot\delta} - 1}{r-1}|U|^{\epsilon_U} + \frac{r^b - 1}{r-1}|U|^{\epsilon_U} \tag{2.3}$$

where $b := \delta^* - t \cdot \delta$. Set

$$\mu_V := |\Sigma_V(G)|, \quad \mu_{V,U} := \frac{r^{t\cdot\delta} - 1}{r-1}|U|^{\epsilon_U}.$$

We have

$$\frac{\mu_V}{|V|} = \frac{(q^\delta - 1)|V|^{\epsilon_V}}{(q-1)|V|} \leq \frac{q^\delta - 1}{q-1} \leq q^\delta - 1 \leq r^{\delta\cdot t} - 1 \leq \frac{(r^{t\cdot\delta} - 1)|U|}{r-1} \leq |U|\mu_{V,U}. \tag{2.4}$$

## 3. Proof of Theorem 1

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

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

**Lemma 2.** *If $G$ is a finite soluble group, then $\mathcal{M}(G) \leq \mathcal{V}(G) + 2.5$.*

*Proof.* By [5, Proposition 1.2], there exists a constant $\gamma$ such that $\mathcal{M}(G) \leq \mathcal{V}(G) + \gamma$ for every finite group $G$. From the proof of [5, Proposition 1.2] it turns out that $\gamma \leq b + \log_2 e$, where $b$ must be chosen such that, for every finite group $X$ and every $n \geq 2$, $X$ has at most $n^b$ core-free maximal subgroups of index $n$. As it is noticed in [5, Theorem 1.3], $b = 2$ will do. However it can be easily seen that for every finite soluble group $X$ and every $n \geq 2$, $X$ has at most $n$ core-free maximal subgroups of index $n$. So if we restrict our attention to the soluble case, we can take $b = 1$ and consequently $\mathcal{M}(G) \leq \mathcal{V}(G) + 1 + \log_2 e \leq \mathcal{V}(G) + 2.5$. □

http://dx.doi.org/10.22108/ijgt.2018.112531.1496

*Proof of Theorem 1.* Set

$$a_G(t)=\sum_{n\geq 2}\frac{m_n(G)}{n^t},\quad a_{G,p}(t)=\sum_{u\geq 1}\frac{m_{p^u}(G)}{p^{u\cdot t}},\quad b_p(t)=\sum_{u\geq 1}\frac{m_{p^u}(G_p)}{p^{u\cdot t}}.$$

For every $V\in\mathcal{A}_p(G)$, let $U\in\mathcal{A}_p(G_p)$ be an irreducible $G_p$-module that can be obtained as a $G_p$-epimorphic image of $V$. By (2.4), for $t\geq 1$, we have

$$a_{G,p}(t)=\sum_{V\in\mathcal{A}_p(G)}\frac{\mu_V}{|V|^t}\leq\sum_{V\in\mathcal{A}_p(G)}\frac{|U|\mu_{V,U}}{|V|^{t-1}}\leq\sum_{V\in\mathcal{A}_p(G)}\frac{\mu_{V,U}}{|U|^{t-2}}\leq b_p(t-2).$$

By Lemma 2,

$$\mathcal{M}(G_p)\leq\mathcal{V}(G_p)+\gamma\leq d+2.5=c.$$

It follows

$$\frac{\log(m_{p^u}(G_p))}{\log(p^u)}\leq c,$$

and consequently

$$m_{p^u}(G_p)\leq p^{u\cdot c}.$$

We deduce

$$a_G(t)=\sum_p a_{G,p}(t)\leq\sum_p b_p(t-2)\leq\sum_n\frac{n^c}{n^{t-2}}.$$

It follows

$$1-P_G(t)\leq\sum_{M\text{ maximal}}[G:M]^{-t}\leq\sum_{n\geq 2}\frac{m_n(G)}{n^t}=a_G(t)\leq\sum_{n\geq 2}n^{c+2-t}.$$

Thus, if $t\geq c+4.02$, we deduce that

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

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

## 4. An open question

A generalization of the theorem of L.G. Kovács and Hyo-Seob Sim to arbitrary finite group is given in [7]: if a finite group $G$ has a family of $d$-generator subgroups whose indices have no common divisor, then $G$ can be generated by $d+2$ elements. So a natural question is whether there is an analogous of Theorem 1 for arbitrary finite groups. This is a difficult question. Denote by $\Lambda_p(G)$, or respectively $\Lambda_{\text{nonab}}(G)$, the set of the maximal subgroups $M$ of $G$ with the property that the socle of $G/M_G$ is an abelian $p$-group, or respectively a nonabelian group. Assume that for every $p\in\pi(G)$ there exists $G_p\leq G$ such that $p$ does not divide $|G:G_p|$ and $\mathcal{V}(G_p)\leq d$. In order to prove an analogous of Theorem 1 we would need to deduce from this hypothesis a bound on the number of maximal subgroups of $G$ of a given index. Imitating the arguments of the proof of Theorem 1, the assumption $\mathcal{V}(G_p)\leq d$ can be used to estimate the number of maximal subgroups in $\Lambda_p(G)$ in terms of $d$, but it remains the problem of getting an efficient estimation of the number of the maximal subgroups in $\Lambda_{\text{nonab}}(G)$.

http://dx.doi.org/10.22108/ijgt.2018.112531.1496

We think that it could be possible to use for this purpose the assumption $\mathcal{V}(G_2) \leq d$. An evidence that this could work is that in [6] it is showed that the number of maximal subgroups in $\Lambda_{\mathrm{nonab}}(G)$ of index $n$ in $G$ can be bounded in terms of the cardinality $d_2(G)$ of a minimal generating set of a Sylow 2-subgroup of $G$. We would need a similar result, using a subgroup of odd index instead of a Sylow 2-subgroup. In the remaining part of this section we want to discuss a question in the context of profinite groups in which a similar question arises, i.e. whether the role of a 2-Sylow subgroup can be played by an arbitrary subgroup of odd index.

A profinite group $G$, being a compact topological group, can be seen as a probability space. 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 $G^k$. A profinite group $G$ is said to be positively finitely generated, PFG for short, if $P_G(k)$ is positive for some natural number $k$. Not all finitely generated profinite groups are PFG (for example if $\hat{F}_d$ is the free profinite group of rank $d \geq 2$ then $P_{\hat{F}_d}(t) = 0$ for every $t \geq d$, see for example [3])

**Proposition 3.** *Let $G$ be a finitely generated profinite group. If the 2-Sylow subgroups of $G$ are finitely generated, then $G$ is PFG.*

*Proof.* Let $h = d_2(G)$ be the smallest cardinaly of a (topologically) generating set of a 2-Sylow subgroup of $G$. By [6, Lemma 4 (3)] (indeed a consequence of the Tate's $p$-nilpotency criterion), for every open normal subgroup $N$ of $G$, a chief series of $G/N$ contains at most $h-1$ non-abelian factors. This implies that $G$ is virtually pro-soluble, and consequently $G$ is $PFG$ by [8, Theorem 10]. □

We don't know whether the previous result remains true if we only assume that there is a closed subgroup of $G$ which is of odd index and PFG. So we conclude this section with the following open question: *is it true that if a finitely generated profinite group $G$ contains a PFG closed subgroup of odd index, then $G$ is PFG?*

## References


[1] A. Ballester-Bolinches and L. M. Ezquerro, Classes of finite groups, Mathematics and Its Applications (Springer), **584**, Springer, Dordrecht, 2006.

[2] W. Gaschütz, Praefrattinigruppen, *Arch. Mat.*, **13** (1962) 418–426.

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

[4] L. G Kovács and 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. Lucchini, A bound on the expected number of random elements to generate a finite group all of whose Sylow subgroups are $d$-generated, *Arch. Math. (Basel)*, **107** (2016) 18.

[7] A. Lucchini, On groups with $d$-generator subgroups of coprime index, *Comm. Algebra*, **28** (2000) 1875–1880.

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

**Andrea Lucchini**

*Dipartimento di Matematica Tullio Levi-Civita, Via Trieste 63, 35121 Padova, Italy*

lucchini@math.unipd.it

**Mariapia Moscatiello**

*Dipartimento di Matematica Tullio Levi-Civita, Via Trieste 63, 35121 Padova, Italy*

mariapia.moscatiello@math.unipd.it

http://dx.doi.org/10.22108/ijgt.2018.112531.1496