J. Austral. Math. Soc. **71** (2001), 177–185

ON THE PROBABILITY OF GENERATING A MINIMAL *d*-GENERATED GROUP

F. DALLA VOLTA, A. LUCCHINI and F. MORINI

To Laci Kovács on his 65th birthday

(Received 9 January 2001; revised 15 June 2001)

Communicated by R. A. Bryce

Abstract

We consider finite groups with the property that any proper factor can be generated by a smaller number of elements than the group itself. We study some problems related with the probability of generating these groups with a given number of elements.

2000 *Mathematics subject classification*: primary 20B05, 20P05.

1. Introduction

We denote by $\mathscr{L}$ the set of finite groups L with the following properties: L has a unique minimal normal subgroup, say M, and if M is abelian then M has a complement in L. Let $L_0 = L/M$ and for any positive integer t define $L_t = \{(l_1, \dots, l_t) \in L^t \mid l_1 \equiv \dots \equiv l_t \mod M\}$.

Denote by $d(G)$ the minimal number of generators of a finite group G; in [2] it is proved that for any nontrivial finite group G there exists $L \in \mathscr{L}$ and a positive integer t such that L_t is an epimorphic image of G and $d(G) = d(L_t) > d(L_{t-1})$. In particular, if G is a *minimal d-generated group* (meaning by this expression that $d(G) = d$ but $d(G/N) < d$ whenever N is a nontrivial normal subgroup of G) then $G \cong L_t$ for a suitable choice of $L \in \mathscr{L}$ and $t \in \mathbb{N}$. This motivates our interest in the generation properties of groups L_t; results in this direction can be applied to obtain more general results on the generation of finite groups.

© 2001 Australian Mathematical Society 0263-6115/2001 \$A2.00 + 0.00

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

For any finite group G, let $\phi_G(s)$ denote the number of s-bases, that is, ordered s-tuples $(g_1, \ldots, g_s)$ of elements of G that generate G. The number $P_G(s) = \phi_G(s)/|G|^s$ gives the probability that s randomly chosen elements of G generate G. Recently Pak [10] introduced the following interesting conjecture: *given a real number α with $0 < \alpha < 1$ there exists an absolute constant β such that for any finite group G, if $s \geq \beta d(G) \log\log |G|$ then $P_G(s) \geq \alpha$.*

One of the aims of this paper is to analyse the behaviour of groups L_t with respect to this conjecture. We give an evidence for the conjecture proving that if s is large enough with respect to $d(L_t) \log\log |L_t|$ and the probability of generating L_0 with s element is high, then the probability of generating L_t with s elements is also high. To state this result in a more precise way we recall a definition. If G is a finite group and N is a normal subgroup of G, let $P_{G,N}(s) = P_G(s)/P_{G/N}(s)$. This number is the probability that an s-tuple generates G, given that it generates G modulo N. If $L \in \mathscr{L}$ and $M = \operatorname{soc} L$ then $\operatorname{soc} L_t \cong M^t$ and $L_t/\operatorname{soc} L_t \cong L_0$. Therefore, $P_{L_t}(s) = P_{L_0}(s) P_{L_t, \operatorname{soc} L_t}(s)$. Our main result is the following:

THEOREM 1. *Given a real number α with $0 < \alpha < 1$ there exist two absolute constants β_1 and β_2 such that for any $L \in \mathscr{L}$ and any $t \in \mathbb{N}$*

(a) *if $\operatorname{soc} L$ is abelian and $s \geq \beta_1 + d(L_t)$, then $P_{L_t, \operatorname{soc} L_t}(s) \geq \alpha$;*
(b) *if $\operatorname{soc} L$ is non abelian and $s \geq \beta_2 \log(t+1)$, then $P_{L_t, \operatorname{soc} L_t}(s) \geq \alpha$.*

This is a consequence of two more precise results. Let $\mathscr{L}_{\text{ab}}$ be the set of finite groups $L \in \mathscr{L}$ satisfying the property that $\operatorname{soc} L$ is abelian and let $\mathscr{L}_{\text{nonab}} = \mathscr{L} \setminus \mathscr{L}_{\text{ab}}$.

THEOREM 2. *For any $L \in \mathscr{L}_{\text{ab}}$ and any $t, u \in \mathbb{N}$*

$$P_{L_t, \operatorname{soc} L_t}(d(L_t) + u) \geq 1 - 2^{-u}.$$

THEOREM 3. *There exist two positive real numbers η_1 and η_2 such that for any $L \in \mathscr{L}_{\text{nonab}}$ and any $t, u \in \mathbb{N}$, if $P_{L_0}(u) > 0$ then*

$$P_{L_t, \operatorname{soc} L_t}(u) \geq 1 - \frac{\eta_1 t^2}{2^{\eta_2 u}}.$$

The second problem that we want to discuss in this paper is the following: suppose $X, Y \in \mathscr{L}$ with $\operatorname{soc} X = \operatorname{soc} Y$ and let $t \in \mathbb{N}$; can we say something about $d(Y_t)$ if we know $d(X_t)$? A partial answer follows from [7, Proposition 1]: if $X, Y \in \mathscr{L}_{\text{nonab}}$, $\operatorname{soc} X = \operatorname{soc} Y$ and $X \leq Y$ then, for any $t \in \mathbb{N}$, $d(Y_t) \leq \max(d(Y_0), d(X_t) + 1)$. In this paper we prove a more general result.

THEOREM 4. *There exists a positive integer r with the following property: for any pair of groups $X, Y \in \mathscr{L}_{\text{nonab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$ and any non negative integer t, $d(Y_t) \leq \max(d(Y_0), d(X_t) + r)$.*

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

Note that one cannot expect to bound $d(Y_t)$ only as a function of $d(X_t)$ but independently from $d(Y_0)$. As we will show in Section 4, for any $t, u \in \mathbb{N}$, there exists a pair X, Y of groups in $\mathscr{L}_{\text{nonab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$, $d(X_t) = 2$, $d(Y_t) \geq d(Y_0) = u$. It is also possible to construct examples with $d(Y_t) > \max(d(Y_0), d(X_t))$ while we know no example with $d(Y_t) > \max(d(Y_0), d(X_t) + 1)$. Therefore we can conjecture that one can take $r = 1$ in Theorem 4. We prove that this is true asymptotically.

THEOREM 5. *There exists a positive real number ζ with the following property: for any pair of groups $X, Y \in \mathscr{L}_{\text{nonab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$ and any nonnegative integer t, if $|\operatorname{soc} X| \geq \zeta$, then $d(Y_t) \leq \max(d(Y_0), d(X_t) + 1)$.*

There are no similar results for pairs X, Y of groups in $\mathscr{L}_{\text{ab}}$. In Section 4, for any positive integers n, u, we construct $X, Y \in \mathscr{L}_{\text{ab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$, $d(X_0) = 2$, $d(X_{nu}) = u + 1$, $d(Y_0) = 1$, $d(Y_{nu}) = nu + 1$.

2. Preliminary results

In this section we describe how the number $P_{L_t}(s)$ can be computed.

First assume that $L \in \mathscr{L}_{\text{ab}}$. In this case the socle M of L has a complement H in L. Of course H is isomorphic to an irreducible subgroup of $\operatorname{Aut} M$. Define the numbers q_L, r_L, s_L and θ_L as follows: $q_L = |\operatorname{End}_H M|$, $q_L^{r_L} = |M|$, $q_L^{s_L} = |\mathrm{H}^1(H, M)|$, $\theta_L = 0$ or 1 according as M is trivial or not. Moreover, let $h_{L,t} = \theta_L + \lceil (t + s_L)/r_L \rceil$, where $\lceil x \rceil$ denotes the smallest integer greater or equal x. From [5, Lemma 2] it follows:

PROPOSITION 6. *If $L \in \mathscr{L}_{\text{ab}}$, then for any $s, t \in \mathbb{N}$*

$$P_{L_t}(s) = P_{L_0}(s) \prod_{0 \leq i \leq t-1} \left(1 - q_L^{r_L(\theta_L - s) + s_L + i}\right).$$

In particular, $d(L_t) = \max(d(L_0), h_{L,t})$.

If $L \in \mathscr{L}_{\text{nonab}}$ and $M = \operatorname{soc} L$, we may identify L with a subgroup of $\operatorname{Aut} M$. Let $\gamma_L = |C_{\operatorname{Aut} M}(L/M)|$ and for any $s \in \mathbb{N}$ define $\psi_L(s) = \phi_L(s)/\gamma_L \phi_{L/M}(s)$. The number $\psi_L(s)$ plays an important role in the computation of $P_{L_t, \operatorname{soc} L_t}(s)$. The following result generalises a formula ([6, Proposition 9]) about the probability of generating a direct product of isomorphic non abelian finite simple groups.

PROPOSITION 7. *If $L \in \mathscr{L}_{\text{nonab}}$, then for any $s, t \in \mathbb{N}$ with $s \geq d(L_0)$,*

$$P_{L_t}(s) = P_{L_0}(s) P_{L, \operatorname{soc} L}(s)^t \prod_{1 \leq i \leq t-1} \left(1 - \frac{i}{\psi_L(s)}\right).$$

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

PROOF. Let $M = \operatorname{soc} L$ and $C_L = C_{\mathrm{Aut}\,M}(L/M)$. As it is proved in [2] the group L_t is generated by s elements $g_1 = (x_{11}, \dots, x_{1t}), \dots, g_s = (x_{s1}, \dots, x_{st})$ if and only if:

(a) for $1 \le i \le s$, $(x_{1i}, \dots, x_{si})$ is an s-basis of L;
(b) if $1 \le i < j \le t$, $(x_{1j}, \dots, x_{sj}) \notin \Gamma_i = (x_{1i}, \dots, x_{si})^{C_L}$.

So, to choose $g_1, \dots, g_s$ generating L_t we first choose an s-basis $(x_{11}, \dots, x_{s1})$ of L, and this can be done in exactly $\phi_L(s)$ different ways. Let $\Omega_{x_{11},\dots,x_{s1}} = \{(y_1, \dots, y_s) \in L \mid y_i \equiv x_{i1} \mod M, 1 \le i \le s, \text{ and } \langle y_1, \dots, y_s\rangle = L\}$. If $i > 1$, $(x_{1i}, \dots, x_{si}) \in \Omega_{x_{11},\dots,x_{s1}} \setminus (\Gamma_1 \cup \dots \cup \Gamma_{i-1})$. By a result of Gaschütz [4] $|\Omega_{x_{11},\dots,x_{s1}}| = \phi_L(s)/\phi_{L/M}(s)$. Moreover, the sets Γ_i, $1 \le i \le t$, are pairwise disjoint and, being $\langle x_{1i}, \dots, x_{si}\rangle = L$, it must be $|\Gamma_i| = |C_L| = \gamma_L$. Therefore, if $i > 1$, $(x_{1i}, \dots, x_{si})$ can be chosen in exactly $[\phi_L(s)/\phi_{L/M}(s)] - (i-1)\gamma_L$ different ways. So we have

$$\begin{aligned} P_{L_t}(s) &= \frac{\phi_L(s)}{|L_t|^s} \prod_{1 \le i \le t-1} \left(\frac{\phi_L(s)}{\phi_{L/M}(s)} - i\gamma_L \right) \\ &= P_L(s) P_{L,\operatorname{soc} L}(-s)^{t-1} \prod_{1 \le i \le t-1} \left(1 - \frac{i}{\psi_L(s)} \right) \\ &= P_{L_0}(s) P_{L,\operatorname{soc} L}(s)^t \prod_{1 \le i \le t-1} \left(1 - \frac{i}{\psi_L(s)} \right). \end{aligned}$$ □

COROLLARY 8. *Assume $L \in \mathscr{L}_{\mathrm{nonab}}$, $s \ge \max(2, d(L_0))$; $d(L_t) \le s$ if and only if $t \le \psi_L(s)$.*

PROOF. Suppose $s \ge 2$ and $P_{L_0}(s) > 0$; by the main theorem in [8] $d(L) = \max(2, d(L_0))$, so it follows that $P_{L,\operatorname{soc} L}(s) = P_L(s)/P_{L_0}(s) > 0$. Therefore, from Proposition 7, $P_{L_t}(s) > 0$ if and only if $1 > i/\psi_L(s)$ for $1 \le i \le t-1$ and this is equivalent to the condition $\psi_L(s) \ge t$. □

A bound for $\psi_L(s)$ can be deduced from the following result ([9, Corollary 1.2]).

PROPOSITION 9. *There exists an absolute constant γ, $0 < \gamma < 1$, such that for any $L \in \mathscr{L}_{\mathrm{nonab}}$ and any integer $s \ge 2$ we have $\phi_L(s) \ge \gamma \phi_{L_0}(s) |\operatorname{soc} L|^s$.*

PROPOSITION 10. *Suppose that $L \in \mathscr{L}_{\mathrm{nonab}}$ and that $M = \operatorname{soc} L \cong S^n$ with S a non abelian simple group. If γ is the constant which appears in the statement of Proposition 9, then for any $s \ge \max(2, d(L_0))$ we have*

$$\frac{\gamma |M|^{s-1}}{n|\operatorname{Out} S|} \le \psi_L(s) \le |M|^{s-1}.$$

PROOF. By Proposition 9, $\gamma |M|^s \le \phi_L(s)/\phi_{L/M}(s) \le |M|^s$. Moreover, from the proof of [3, Lemma 1], $|M| \le |C_L| \le n|S|^{n-1}|\operatorname{Aut} S|$. □

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

3. Proof of Theorem 1

In this section, we deal with the proofs of Theorem 2 and Theorem 3; Theorem 1 follows immediately from these two results.

First, in order to prove Theorem 2, we need the following lemma.

LEMMA 11. *For any $L \in \mathscr{L}_{\mathrm{ab}}$ and $t, u \in \mathbb{N}$,*

$$P_{L_t}(h_{L,t} + u) \geq P_{L_0}(h_{L,t} + u)(1 - q_L^{-r_L u}).$$

PROOF. By Proposition 6 and noticing that $r_L(\theta_L - h_{L,t} - u) + s_L \leq -t - r_L u$, if $h_{L,t} + u \geq d(L_0)$ we have

$$\begin{aligned} P_{L_t, \mathrm{soc}\, L_t}(h_{L,t} + u) &\geq \prod_{0 \leq i \leq t-1} \left(1 - q_L^{r_L(\theta_L - h_{L,t} - u) + s_L + i}\right) \geq \prod_{0 \leq i \leq t-1} \left(1 - q_L^{-r_L u - t + i}\right) \\ &\geq 1 - \sum_{0 \leq i \leq t-1} q_L^{-r_L u - t + i} \geq 1 - q_L^{-r_L u} \sum_{1 \leq j \leq t} q_L^{-j} \\ &\geq 1 - q_L^{-r_L u} \sum_{1 \leq j \leq \infty} q_L^{-j} \geq 1 - q_L^{-r_L u}. \end{aligned}$$ □

PROOF OF THEOREM 2. It follows immediately from Lemma 11, since, by Proposition 6, $h_{L,t} \leq d(L_t)$. □

By [1, Theorem A], if $L \in \mathscr{L}_{\mathrm{ab}}$ then $s_L < r_L$ and this implies $h_{L,t} \leq t + 1$. Therefore from Lemma 11 we also deduce:

COROLLARY 12. *For any $L \in \mathscr{L}_{\mathrm{ab}}$ and $s \in \mathbb{N}$, $P_{L_t}(s) \geq P_{L_0}(s)(1 - 2^{-(s-t-1)})$.*

Now, we are left with the non abelian case. Again, to prove Theorem 3, we start with two lemmas:

LEMMA 13. *Suppose that $L \in \mathscr{L}_{\mathrm{nonab}}$ and let $M = \mathrm{soc}\, L$. There exist two positive constants σ_1 and σ_2 such that for any $u \in \mathbb{N}$ with $u \geq \max(2, d(L_0))$,*

$$P_{L,M}(u) \geq 1 - \sigma_1 / e^{\sigma_2 u}.$$

PROOF. There exist a positive integer n and a non abelian simple group S such that $M = \mathrm{soc}\, L \cong S^n$. Denote by S_1 the subset of $S^n = M$ consisting of elements $x = (1, x_2, \ldots, x_n)$ and let $\phi_1 : N_L(S_1) \to \mathrm{Aut}\, S$ be the map induced by the conjugation action of $N_L(S_1)$ on S. Select $g_1, \ldots, g_u$ in L such that $\langle g_1, \ldots, g_u, M \rangle = L$. From [9, Lemma 2.12] it follows:

$$\frac{\phi_L(u)}{\phi_{L/M}(u)} \geq |\Omega_1| - |M|^{3/2} - |M|^{u/2 + 19/20},$$

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

where $\Omega_1 = \{(m_1, \dots, m_u) \in M^u \mid (N_{\langle g_1 m_1, \dots, g_u m_u \rangle}(S_1))\phi_1 \geq S\}$. For any $1 \leq i < j \leq u$, define $\Delta_{i,j} = \{(x, y) \in M^2 \mid (N_{\langle g_i x, g_j y \rangle}(S_1))\phi_1 \geq S\}$.

We can repeat the arguments used in [9, Lemma 2.10] and prove that $|\Delta_{i,j}| \geq c_s|M|^2$, where c_s is the positive constant which appears in [9, Proposition 2.7]. We note that $(m_1, \dots, m_u)$ is an element of Ω_1 if there exists at least a pair $(m_{2i+1}, m_{2i+2}) \in \Delta_{2i+1,2i+2}$, where $0 \leq i \leq [u/2] - 1$.

It follows that

$$\begin{aligned}|\Omega_1| &\geq |M|^u - \prod_{0 \leq i \leq [u/2]-1} \left(|M|^2 - |\Delta_{2i+1,2i+2}|\right) \\ &\geq |M|^u - \prod_{0 \leq i \leq [u/2]-1} \left(|M|^2 - c_s|M|^2\right) \geq |M|^u \left(1 - (1 - c_s)^{[u/2]}\right).\end{aligned}$$

So we have

$$P_{L,M}(u) \geq 1 - (1 - c_s)^{[u/2]} - \frac{|M|^{3/2}}{|M|^u} - \frac{|M|^{19/20}}{|M|^{u/2}}.$$

By [9, Proposition 2.7] we derive that $c^* = \inf_s c_s$ is a positive number. Set $\eta = 1 - c^*$. Then we have

$$(1 - c_s)^{[u/2]} \leq \eta^{[u/2]} \leq \eta^{u/2-1}.$$

Moreover, $|M| \geq 60 \geq e^4$ and $u \geq 2$ imply that

$$|M|^{3/2-u} \leq e^{-u/2}, \qquad |M|^{19/20-u/2} \leq e^{19/5-2u} \leq e^{4/5-u/2}.$$

Set $\sigma_1 = \eta^{-1} + 1 + e^{4/5}$ and $\sigma_2 = \min(1/2, -\log \eta/2)$ and conclude

$$\begin{aligned}P_{L,M}(u) &\geq 1 - \eta^{-1}\eta^{u/2} - e^{-u/2} - e^{4/5}e^{-u/2} \\ &\geq 1 - \eta^{-1}e^{-u\sigma_2} - e^{-u\sigma_2} - e^{4/5}e^{-u\sigma_2} \geq 1 - \sigma_1 e^{-u\sigma_2}.\end{aligned}$$

□

LEMMA 14. *Suppose that $L \in \mathcal{L}_{\text{nonab}}$ and that $M = \operatorname{soc} L \cong S^n$ with S a non abelian simple group. For any $t, u \in \mathbb{N}$ with $u \geq 2$*

$$\prod_{1 \leq i \leq t-1} \left(1 - \frac{i}{\psi_L(u)}\right) \geq 1 - \frac{t^2}{\gamma 2^{u-2}},$$

where γ is the constant which appears in the statement of Proposition 9.

PROOF. By Proposition 10 and noticing that $n|\operatorname{Out} S| \leq |S^n| = |M|$ we have

$$\begin{aligned}\prod_{1 \leq i \leq t-1} \left(1 - \frac{i}{\psi_L(u)}\right) &\geq 1 - \frac{\sum_{1 \leq i \leq t-1} i}{\psi_L(u)} \geq 1 - \frac{(t-1)^2}{\psi_L(u)} \\ &\geq 1 - \frac{(t-1)^2 n|\operatorname{Out} S|}{\gamma|M|^{u-1}} \geq 1 - \frac{(t-1)^2}{\gamma|M|^{u-2}} \geq 1 - \frac{t^2}{\gamma 2^{u-2}}.\end{aligned}$$

□

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

PROOF OF THEOREM 3. It follows immediately from Lemma 13, Lemma 14 and Proposition 7. Precisely, noticing that $\sigma_2 u \leq u-1$ we have

$$P_{L,M}(u)^t \geq 1 - \frac{\sigma_1 t}{2^{\sigma_2 u}},$$
$$\prod_{1 \leq i \leq t-1} \left(1 - \frac{i}{\psi_L(u)}\right) \geq 1 - \frac{2\gamma^{-1}t^2}{2^{u-1}} \geq 1 - \frac{2\gamma^{-1}t^2}{2^{\sigma_2 u}}$$

and hence

$$P_{L_t, \operatorname{soc} L_t}(u) \geq 1 - \frac{2\gamma^{-1}t^2 + \sigma_1 t}{2^{\sigma_2 u}} \geq 1 - \frac{(\sigma_1 + 2\gamma^{-1})t^2}{2^{\sigma_2 u}}. \qquad \square$$

4. Proof of Theorem 4 and Theorem 5

In this section we consider two groups X and $Y \in \mathcal{L}_{\mathrm{nonab}}$ such that $\operatorname{soc} X = \operatorname{soc} Y$. It seems interesting to compare $d(X_t)$ and $d(Y_t)$. As already observed in the introduction, $X \leq Y$ implies $d(Y_t) \leq \max(d(Y_0), d(X_t) + 1)$ ([7]).

One cannot expect to have $d(Y_t) \leq \max(d(Y_0), d(X_t))$ for any pair of groups $X, Y \in \mathcal{L}_{\mathrm{nonab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$. For example, let $X = \mathrm{PGL}(2,7)$, $Y = \mathrm{PSL}(2,7)$; it can be computed that $\psi_X(2) = 69$ and $\psi_Y(2) = 57$, hence, by Corollary 8, $d(Y_{58}) = 3$ while $d(X_{58}) = 2$. However, we conjecture that $d(Y_t) \leq \max(d(Y_0), d(X_t) + 1)$. From the proof of Theorem 4, one can deduce that to prove this conjecture if suffices to show that $\gamma \geq 1/\sqrt{60}$, where γ is the constant which appears in the statement of Proposition 9.

We explicitly observe that, in general, it is not true neither that if $X \geq Y$ then $d(X_t) \geq d(Y_t)$ (see the previous example) nor the converse. If we take $Y = \mathrm{PSU}(3,3)$ and $X = \mathrm{Aut}(Y)$, we obtain $\psi_Y(2) = 2784$ and $\psi_X(2) = 2772$, so that $2 = d(Y_{2773}) < d(X_{2773}) = 3$.

LEMMA 15. *Let $X, Y \in \mathcal{L}_{\mathrm{nonab}}$, and assume $\operatorname{soc} X = \operatorname{soc} Y \cong S^n$ with S a finite non abelian simple group, and let $r, t \in \mathbb{N}$. If $d(Y_t) > \max(d(Y_0), d(X_t) + r)$ then $n|\operatorname{Out} S|/|S|^{rn} > \gamma$, where γ is the constant which appears in the statement of Proposition* 9.

PROOF. Since $\max(2, d(X_0)) \leq d(X_t)$, by Corollary 8 we have $t \leq \psi_X(d(X_t))$. On the other hand, again by Corollary 8, $d(Y_t) > \max(d(Y_0), d(X_t) + r)$ implies $t > \psi_Y(d(X_t) + r)$. Using Proposition 10 we deduce

$$\frac{\gamma |S|^{n(d(X_t)+r-1)}}{n|\operatorname{Out} S|} \leq \psi_Y(d(X_t) + r) < t \leq \psi_X(d(X_t)) \leq |S|^{n(d(X_t)-1)}$$

which implies $\gamma |S|^{rn} < n|\operatorname{Out} S|$. $\square$

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

PROOF OF THEOREM 4. Let r be the smallest integer satisfying $r \geq -\log_{60}\gamma + 1/2$. Suppose by contradiction that there exist $X, Y \in \mathscr{L}_{\mathrm{nonab}}$ and $t \in \mathbb{N}$ such that $\operatorname{soc} X = \operatorname{soc} Y$ and $d(Y_t) > \max(d(Y_0), d(X_t) + r)$. By Lemma 15, if $\operatorname{soc} X = S^n$ with S a non abelian simple group, then $\gamma < n|\operatorname{Out} S|/|S|^{rn}$. On the other hand, $|\operatorname{Out} S| \leq \sqrt{|S|}$ (see [9, Proposition 2.6]) and $|S| \geq 60$, so

$$\gamma < \frac{n|\operatorname{Out} S|}{|S|^{rn}} \leq \frac{|\operatorname{Out} S|}{|S|^r} \leq \frac{\sqrt{|S|}}{|S|^r} \leq 60^{1/2-r},$$

in contradiction with the choice of r. □

LEMMA 16. *Let $M = S^n$ be a direct product of isomorphic non abelian simple groups, then* $\lim_{|M|\to\infty} n|\operatorname{Out} S|/|S|^n = 0$.

PROOF. By [9, Proposition 2.6]

$$\frac{n|\operatorname{Out} S|}{|S|^n} \leq \frac{n\sqrt{|S|}}{|S|^n} \leq \frac{\sqrt{|S|^n}}{|S|^n} \leq \frac{1}{\sqrt{|M|}}.$$ □

PROOF OF THEOREM 5. By Lemma 16 there exists ζ such that if $M = S^n$ is a direct product of isomorphic non abelian simple groups and $|M| \geq \zeta$, then $n|\operatorname{Out} S|/|M| \leq \gamma$. Suppose by contradiction that there exist $X, Y \in \mathscr{L}_{\mathrm{nonab}}$ and $t \in \mathbb{N}$ satisfying $\operatorname{soc} X = \operatorname{soc} Y \cong S^n$, $|S^n| \geq \zeta$ and $d(Y_t) > \max(d(Y_0), d(X_t) + 1)$. By Lemma 15, $\gamma < n|\operatorname{Out} S|/|S|^n$, against the choice of ζ. □

We have proved that if $X, Y \in \mathscr{L}_{\mathrm{nonab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$, then $d(Y_t)$ can be bounded in terms of $d(X_t)$ and $d(Y_0)$. The next result shows that it is impossible to bound $d(Y_t)$ from the knowledge of $d(X_t)$ but independently from $d(Y_0)$.

PROPOSITION 17. *For any $t, u \in \mathbb{N}$, there exists a pair X, Y of groups in $\mathscr{L}_{\mathrm{nonab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$, $d(X_t) = 2$, $d(Y_t) \geq d(Y_0) = u$.*

PROOF. Let A be an elementary abelian 2-group of rank u and let S be a finite non abelian simple group with $|S| \geq (2^u t/\gamma)^2$; A can be viewed as a regular permutation group of degree 2^u. Consider the wreath products $X = S \wr \operatorname{Sym}(2^u)$ and $Y = S \wr A$. Of course $X, Y \in \mathscr{L}_{\mathrm{nonab}}$ and $\operatorname{soc} X = \operatorname{soc} Y = S^{2^u}$. By Proposition 10

$$\psi_X(2) \geq \frac{\gamma|S|^{2^u}}{2^u|\operatorname{Out} S|} \geq \frac{\gamma|S|^{2^u}}{2^u\sqrt{|S|}} \geq \frac{\gamma\sqrt{|S|}}{2^u} \geq t,$$

hence, by Corollary 8, $d(X_t) \leq 2$. On the other hand, $d(Y_t) \geq d(Y_0) = u$. □

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

Finally we note that the previous results don't remain true for pairs of groups in $\mathcal{L}_{\mathrm{ab}}$. Indeed, given $n \in \mathbb{N}$ there exist $X, Y \in \mathcal{L}_{\mathrm{ab}}$ with $\operatorname{soc} X = \operatorname{soc} Y$, $\max(d(X_0), d(Y_0)) \leq 2$ but $d(Y_{un}) - d(X_{un}) = u(n-1)$ for any positive integer u. Let p be an odd prime and let V be a vector space of dimension n over the field $\mathrm{GF}(p)$. Moreover, let $H_1 = \mathrm{GL}(n, p)$ and let H_2 be the subgroup of $\mathrm{GL}(n, p)$ generated by a Singer cycle of order $p^n - 1$. Take the semidirect products $X = VH_1$ and $Y = VH_2$. Note that $X, Y \in \mathcal{L}_{\mathrm{ab}}$ with $\operatorname{soc} X = \operatorname{soc} Y = V$ and that $d(X_0) = d(H_1) = 2$, $d(Y_0) = d(H_2) = 1$. Since $\mathrm{End}_{H_1} V = \mathrm{GF}(p)$ and $\mathrm{End}_{H_2} V = \mathrm{GF}(p^n)$, we have $r_X = n$ and $r_Y = 1$. Moreover, $\mathrm{H}^1(H_1, V) = \mathrm{H}^1(H_2, V) = 0$ so $s_X = s_Y = 0$. For any positive integer u, from Proposition 6, we deduce $d(X_{nu}) = h_{X,nu} = 1 + u$, $d(Y_{nu}) = h_{Y,nu} = 1 + nu$.

References

[1] M. Aschbacher and R. Guralnick, 'Some applications of the first cohomology group', *J. Algebra* **90** (1984), 446–460.

[2] F. Dalla Volta and A. Lucchini, 'Finite groups that need more generators than any proper quotient', *J. Austral. Math. Soc. Ser. A* **64** (1998), 82–91.

[3] ———, 'The smallest group with non zero presentation rank', *J. Group Theory* **2** (1999), 147–155.

[4] W. Gaschütz, 'Zu einem von B. H. und H. Neumann gestellten Problem', *Math. Nachr.* **14** (1955), 249–252.

[5] K. W. Gruenberg and K. W. Roggenkamp, 'Decomposition of the relation modules of a finite group', *J. London Math. Soc. (2)* **12** (1976), 262–266.

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

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

[8] A. Lucchini and F. Menegazzo, 'Generators for finite groups with a unique minimal normal subgroup', *Rend. Sem. Mat. Univ. Padova* **98** (1997), 173–191.

[9] A. Lucchini and F. Morini, 'On the probability of generating finite groups with a unique minimal normal subgroup', *Pacific. J. Math.* to appear.

[10] I. Pak, 'On the probability of generating a finite group', preprint, 2000.

Dipartimento di Matematica e Applicazioni
Università di Milano - Bicocca
Via Bicocca Degli Arcimboldi 8
20126 Milano
Italy

Dipartimento di Matematica
Università di Brescia
Via Valotti 9
25133 Brescia
Italy

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press

https://doi.org/10.1017/S1446788700002822 Published online by Cambridge University Press