Pacific Journal of Mathematics

ON THE PROBABILITY OF GENERATING FINITE GROUPS WITH A UNIQUE MINIMAL NORMAL SUBGROUP

Andrea Lucchini and Fiorenza Morini

Volume 203 No. 2 April 2002

PACIFIC JOURNAL OF MATHEMATICS
Vol. 203, No. 2, 2002

ON THE PROBABILITY OF GENERATING FINITE GROUPS WITH A UNIQUE MINIMAL NORMAL SUBGROUP

Andrea Lucchini and Fiorenza Morini

Assume that a finite group G has a unique minimal normal subgroup, say N. We prove that if the order of N is large enough then the following is true: If d randomly chosen elements generate G modulo N, then these elements almost certainly generate G itself.

1. Introduction.

For any finite group G, let $d(G)$ be the smallest cardinality of a generating set of G and let $\phi_G(d)$ denote the number of d-basis, that is, ordered d-tuples $(g_1, \dots, g_d)$ of elements of G that generate G. The number $P_G(d) = \frac{\phi_G(d)}{|G|^d}$ gives the probability that d randomly chosen elements of G generate G.

Suppose that N is a normal subgroup of G with $d(G/N) \leq d$ and choose $g_1, \dots, g_d$ such that $G = \langle g_1, \dots, g_d, N\rangle$. It was noticed by Gaschütz [**10**] that the cardinality of the set $\Omega_{g_1,\dots,g_d} = \{(n_1, \dots, n_d) \in N^d \mid \langle g_1 n_1, \dots, g_d n_d\rangle = G\}$ is independent on the choice of $g_1, \dots, g_d$; namely $|\Omega_{g_1,\dots,g_d}| = \frac{\phi_G(d)}{\phi_{G/N}(d)}$. Let $P_{G,N}(d) = \frac{P_G(d)}{P_{G/N}(d)} = \frac{\phi_G(d)}{\phi_{G/N}(d)|N|^d}$; this number is the probability that a d-tuple generates G, given that it generates G modulo N. By the previous remark $P_{G,N}(d)$ is also the probability that, given $g_1, \dots, g_d$ generating G modulo N, d randomly chosen elements $n_1, \dots, n_d$ of N satisfy the condition $G = \langle g_1 n_1, \dots, g_d n_d\rangle$.

In the last years many results have been proved about the probability of generating finite simple groups. By a classical result of Dixon [**9**] two elements chosen at random from the symmetric group $\mathrm{Sym}(n)$ will almost certainly generate a subgroup containing the alternating group $\mathrm{Alt}(n)$. Kantor and Lubotzky [**14**] proved an analogous result for classical groups and for small exceptional groups. Liebeck and Shalev [**15**] finished the proof of the following theorem: *If S is a finite nonabelian simple group and G is an almost simple group with $S \leq G \leq \mathrm{Aut}\, S$, then the probability $P(G)$ that two randomly chosen elements of G generate a subgroup containing S tends*

to 1 as $|S| \to \infty$. From the proof of this theorem it can be easily deduced a stronger result (see Proposition 2.7):

$$\min_{h_1,h_2 \in \operatorname{Aut} S} P_{\langle S,h_1,h_2\rangle,S}(2) \to 1 \text{ as } |S| \to \infty.$$

Note that the previous sentence can be viewed as a slight generalisation of the theorem of Liebeck and Shalev about the asymptotic behaviour of $P(G)$; indeed $P(G)$ coincides with the average $\sum_{(x,y)\in G^2} \frac{P_{\langle x,y,S\rangle,S}(2)}{|G|^2}$.

In this paper we want to study $P_{G,N}(d)$ in the more general case when N is the unique minimal normal subgroup of G. The main result is the following.

Theorem 1.1. *Assume that a finite group G has a unique minimal normal subgroup N and that $d \geq d(G)$. Then $P_{G,N}(d) \to 1$ as $|N| \to \infty$.*

In [**17**] it was proved that if G is a noncyclic finite group with a unique minimal normal subgroup N, then $d(G) = \max\{2, d(G/N)\}$. Combining this result with the previous theorem we deduce:

Corollary 1.2. *There exists an absolute constant γ such that if G is a noncyclic finite group with a unique minimal normal subgroup N and $d \geq \max\{2, d(G/N)\}$, then $\frac{\phi_G(d)}{\phi_{G/N}(d)} \geq \gamma |N|^d$.*

Our interest in computing $\frac{\phi_G(d)}{\phi_{G/N}(d)}$ for a finite group G with a unique minimal normal subgroup N is motivated by the following considerations. Let $G_0 = G/N$ and for any positive integer t define $G_t = \left\{(g_1, \dots, g_t) \in G^t \;\middle|\; g_1 \equiv \cdots \equiv g_t \bmod N\right\}$. In [**8**] it is proved that for any nontrivial finite group H there exist a finite group G with a unique minimal normal subgroup and an integer t such that G_t is an epimorphic image of H and $d(H) = d(G_t) > d(G_{t-1})$. Hence results on the generation of groups G_t allow us to prove more general results on the generation of finite groups. On the other hand to compute $d(G_t)$ we need to know $\phi_G(d)/\phi_{G/N}(d)$ ([**8**] Theorem 2.7) and this can be bounded using Corollary 1.2.

An example of how Corollary 1.2 can be applied to solve questions about the generation of finite groups is described in Section 3. Suppose that p and q are distinct primes, let P be a nontrivial p-group, Q a nontrivial q-group and assume that $d(Q) \leq d(P) = d$. By [**16**] Theorem C, any finite group H containing P and Q and generated by them can be generated by $d + 2$ elements. Moreover from the results in [**4**] it can be easily deduced that $d(P \wr Q) = d + 1$. Let $P \amalg Q$ be the profinite free product of P and Q, i.e., the completion of the free product $P * Q$ in the profinite topology, and let $dt(P \amalg Q)$ be the smallest cardinality of a topological generating set for $P \amalg Q$; $dt(P \amalg Q) = \max_H d(H)$ where H runs over the set of finite epimorphic images of $P * Q$ so, by the previous remarks, $d + 1 \leq dt(P \amalg Q) \leq d + 2$.

It remains open the question to determine the exact value of $dt(P \amalg Q)$. In this paper we solve this problem when d is large enough, proving:

Theorem 1.3. *Let γ be the constant which appears in Corollary* 1.2. *Suppose that p and q are two distinct primes, P is a nontrivial finite p-group, Q is a nontrivial finite q-group. If $\max\{d(P), d(Q)\} \geq 1 - \log_3 \gamma$, then $dt(P \amalg Q) = \max\{d(P), d(Q)\} + 1$.*

This follows from:

Theorem 1.4. *Let γ be the constant which appears in Corollary* 1.2. *Suppose that $d \geq 1 - \log_3 \gamma$ and that p and q are two distinct primes. If P is a p-group, Q is q-group, and P and Q can be generated by d elements then $d(H) \leq d + 1$ for any finite group H generated by P and Q.*

2. Proof of Theorem 1.1.

Suppose that G is a finite group with a unique minimal normal subgroup, N and let $d(G) \leq d$. We have to prove that $\frac{\phi_G(d)}{\phi_{G/N}(d)|N|^d} \to 1$ as $|N| \to \infty$.

We first recall a result due to Gaschütz [**10**]:

Proposition 2.1. *Let U be a normal subgroup of a finite group H and let $h_1, \ldots, h_m \in H$ be such that $H = \langle h_1, \ldots, h_m, U\rangle$. If $d(H) \leq m$, then there exist elements $u_1, \ldots, u_m$ of U such that $H = \langle h_1u_1, \ldots, h_mu_m\rangle$. Moreover the cardinality of the set $\Omega_{h_1,\ldots,h_m} = \{(u_1, \ldots, u_m) \in U^m \mid H = \langle h_1u_1, \ldots, h_mu_m\rangle\}$ is independent of the choice of $h_1, \ldots, h_m$ and it is equal to $\frac{\phi_H(m)}{\phi_{H/U}(m)}$.*

We choose d elements $g_1, \ldots, g_d$ generating G, and consider the set $\Omega = \Omega_{g_1,\ldots,g_d} = \{(n_1, \ldots, n_d) \in N^d \mid \langle g_1n_1, \ldots, g_dn_d\rangle = G\}$. Our aim is to show that $\frac{|\Omega|}{|N|^d} = \frac{\phi_G(d)}{\phi_{G/N}(d)|N|^d} \to 1$ as $|N| \to \infty$.

Suppose that N is abelian. If N lies in the Frattini subgroup, then $\frac{\phi_G(d)}{\phi_{G/N}(d)} = |N|^d$. Otherwise N has a complement, K say. The kernel of the action of K on N is a normal subgroup of G, so by the uniqueness of N that kernel must be trivial, the action must be faithful. So, by [**13**] Theorem B, $|\,\mathrm{H}^1(K, N)| \leq |N|^{\frac{2}{3}}$. If G is cyclic then $G{=}N$ has prime order and $\frac{\phi_G(d)}{\phi_{G/N}(d)} = |N|^d - 1$. If G is noncyclic then $d \geq 2$ and, by [**11**], $\frac{\phi_G(d)}{\phi_{G/N}(d)} = |N|^d - |N||\,\mathrm{H}^1(K, N)| \geq |N|^d - |N|^{\frac{5}{3}}$. In both the cases $\frac{\phi_G(d)}{\phi_{G/N}(d)|N|^d} \to 1$ as $|N| \to \infty$.

For the remaining part of this section we assume that N is a nonabelian minimal normal subgroup of G, so $N = S^n$, where S is a nonabelian simple group; furthermore, the hypothesis that N is the unique minimal normal

subgroup of G implies that $G \leq \operatorname{Aut} S^n = \operatorname{Aut} S \wr \operatorname{Sym}(n)$ (the wreath product of $\operatorname{Aut} S$ with the symmetric group of degree n). So the elements of G are of the kind $g = (h_1, \dots, h_n)\sigma$, with $h_i \in \operatorname{Aut} S$ and $\sigma \in \operatorname{Sym}(n)$. The map $\pi : G \to \operatorname{Sym}(n)$ which sends $g = (h_1, \dots, h_n)\sigma$ to σ is a homomorphism; since N is a minimal normal subgroup of G, $G\pi$ is a transitive subgroup of $\operatorname{Sym}(n)$. Let $\Gamma = (\operatorname{Aut} S)^n$ be the base of the wreath product $\operatorname{Aut} S \wr \operatorname{Sym}(n)$ and let $\pi_i : \Gamma \to \operatorname{Aut} S$ be the projection on the i-th factor. Moreover for any $1 \leq i \leq n$ denote with S_i the subset of $S^n = N$ consisting of the elements $x = (x_1, \dots, x_n)$ with $x_j = 1$ for each $j \neq i$. Set $N_i = N_G(S_i)$ and let $\phi_i : N_i \to \operatorname{Aut} S$ be the map induced by the conjugation action of N_i on S.

If $w = (n_1, \dots, n_d)$ is an element of N^d we denote by H_w the subgroup $\langle g_1 n_1, \dots, g_d n_d \rangle$ of G. We will make a frequent use of the following remarks:

Lemma 2.2. *Given a subgroup H of G, let $\Omega_H = \{w \in N^d \mid H_w \leq H\}$. Then $|\Omega_H| \leq |H \cap N|^d$.*

Proof. Suppose that $w = (n_1, \dots, n_d)$ and $\overline{w} = (\overline{n}_1, \dots, \overline{n}_d)$ are two elements of Ω_H. Then $(g_i n_i)^{-1}(g_i \overline{n}_i) = n_i^{-1}\overline{n}_i \in H \cap N$ for $1 \leq i \leq d$.

Lemma 2.3. *Suppose that M_1 and M_2 are two different maximal subgroups of G. If $M_1 \cap N = M_2 \cap N$ then either $M_1 \geq N$ or $M_1 \cap N = 1$.*

Proof. If $M_1 \cap N = M_2 \cap N$ then $M_1 \cap N$ is a normal subgroup of $\langle M_1, M_2 \rangle = G$; by the minimality of N either $M_1 \cap N = N$ or $M_1 \cap N = 1$.

To prove the theorem we need some preliminary results, concerning the cardinality of the following subsets of N^d:

$$\begin{aligned}
\Omega_1 &= \{w \in N^d \mid (N_1 \cap H_w)\phi_1 \geq S\},\\
\Omega_2 &= \{w \in N^d \mid H_w \cap N = 1\},\\
\Omega_3 &= \{w \in N^d \mid H_w \cap \Gamma = 1\},\\
\Omega_4 &= \{w \in N^d \mid H_w \neq G \text{ and } (H_w \cap N)\pi_1 = S\},\\
\Omega_5 &= \{w \in N^d \mid H_w \cap N \neq 1 \text{ and } (H_w \cap N)\pi_1 \neq S\}.
\end{aligned}$$

To study these subsets we need the following results, which depend on the classification of finite simple groups:

Proposition 2.4 (Borovik, Pyber and Shalev, Theorem 1.4 [**3**])**.** *There exists an absolute constant $c > 0$ such that a finite group H has at most $|H|^c$ maximal solvable subgroups.*

Proposition 2.5 (Babai, Goodman and Pyber, Prop. 2.10 [**2**])**.** *There exists an absolute constant $\alpha < 1$ such that, for any nonabelian finite simple group S, every solvable subgroup of S has order at most $|S|^\alpha$.*

Proposition 2.6. *If S is a finite nonabelian simple group then $|\operatorname{Out} S| \leq \sqrt{|S|}$.*

Proof. Compare the values of $|S|$ and $|\operatorname{Out} S|$ given in [**6**] Tables 5 and 6.

Proposition 2.7. *If S is a finite nonabelian simple group then there exists a positive constant c_s such that $P_{\langle S,h_1,h_2\rangle,S}(2) \geq c_s$ for every pair of elements h_1, h_2 in $\operatorname{Aut} S$. Moreover $c_s \to 1$ as $|S| \to \infty$.*

Proof. By [**7**] Theorem 1, for any $h_1, h_2 \in \operatorname{Aut} S$ there are $s_1, s_2 \in S$ with $\langle h_1, h_2, S\rangle = \langle h_1 s_1, h_2 s_2\rangle$; hence $P_{\langle S,h_1,h_2\rangle,S}(2) > 0$. Therefore

$$c_s = \min_{h_1,h_2 \in \operatorname{Aut} S} P_{\langle S,h_1,h_2\rangle,S}(2) > 0.$$

It remains to prove that $c_s \to 1$ as $|S| \to \infty$. Given a pair (h_1, h_2) of elements of $\operatorname{Aut} S$, consider the subgroup $G = \langle S, h_1, h_2\rangle$ of $\operatorname{Aut} S$. Let $\mathcal{M}$ be the set of subgroups of G which are maximal with respect to not containing S; by [**14**] and [**15**]

$$\sum_{M \in \mathcal{M}} |G : M|^{-2} \text{ tends to 0 as } |S| \to \infty.$$

On the other hand it follows from a result due to Gaschütz ([**11**], Satz 1) that

$$P_{G,S}(2) \geq 1 - \sum_{M \in \mathcal{M}^*} |G : M|^{-2}$$

where $\mathcal{M}^*$ is the set of maximal subgroups of G not containing S. As $\mathcal{M}^* \subseteq \mathcal{M}$

$$P_{G,S}(2) \geq 1 - \sum_{M \in \mathcal{M}^*} |G : M|^{-2} \geq 1 - \sum_{M \in \mathcal{M}} |G : M|^{-2},$$

hence $P_{G,S}(2) \to 1$ as $|S| \to \infty$.

Now we can start to study the subsets Ω_i, $1 \leq i \leq 5$.

Lemma 2.8. *Let α and c be the constants which appear in the statements of Proposition* 2.4 *and Proposition* 2.5*; then*

(a) $|\Omega_2| \leq \min\{|N|^5, |S|^\alpha |\operatorname{Aut} S|^c |N|^{1+\alpha(d-1)+\frac{1-\alpha}{2}}\}$,
(b) $|\Omega_3| \leq |N|^{\frac{3}{2}}$.

Proof. a) First of all, we observe that by Lemma 2.2 for each complement H of N there is at most a unique $w \in N^d$ such that $H_w = H$, thus the cardinality of Ω_2 can be bounded by the number of complements of N in G.

Denote $K = S_2 \times \cdots \times S_n$ and notice that $N_G(K)$ is isomorphic to a subgroup of $\operatorname{Aut} S \times (\operatorname{Aut} S \wr \operatorname{Sym}(n-1))$ and $N_G(K)/K$ to a subgroup of $\operatorname{Aut} S \times (\operatorname{Out} S \wr \operatorname{Sym}(n-1))$.

To estimate the cardinality of the set of complements of N in G we apply the following result, proved by Gross and Kovács ([**12**] Corollary 4.4) and by Aschbacher and Scott ([**1**] Theorem 2): G splits over N if and only if $N_G(K)/K$ splits over $N/K \cong S$ and there is a one-to-one correspondence

between the coniugacy classes of complements of N in G and of N/K in $N_G(K)/K$.

Suppose that $N_G(K)/K$ splits over N/K. It is well-known that the number of complements of N/K in $N_G(K)/K$ equals the cardinality of the set $\mathrm{Der}(Y, N/K)$ of derivations from a complement Y of N/K in $N_G(K)/K$ to N/K. Since $\delta \in \mathrm{Der}(Y, N/K)$ is uniquely determined from the knowledge of $y_1^\delta, \dots, y_s^\delta$ with $\langle y_1, \dots, y_s\rangle = Y$, we obtain that $|\mathrm{Der}(Y, N/K)| \leq |S|^{d(Y)}$. Therefore our aim is now to bound $d(Y)$.

First of all, we notice that $Y \leq \mathrm{Out}\, S \times (\mathrm{Out}\, S \wr \mathrm{Sym}(n-1))$ and, in particular, there is an homomorphism $\overline{\pi}$ from Y to $\mathrm{Sym}(n-1)$ with $\ker\overline{\pi} \leq (\mathrm{Out}\, S)^n$. Now $d(Y) \leq d(Y\overline{\pi}) + d(\ker\overline{\pi})$. It turns out to be $d(Y\overline{\pi}) \leq n-1$, since every subgroup of $\mathrm{Sym}(n-1)$ can be generated by $n-1$ elements, and $d(\ker\overline{\pi}) \leq 3n$ because any subgroup of $\mathrm{Out}\, S$ can be generated by 3 elements [**7**]. Thus, $d(Y) \leq 4n-1$ and, consequently, $|\mathrm{Der}(Y, N/K)| \leq |S|^{4n-1} < |N|^4$. Therefore, by the theorem of Gross and Kovács, Aschbacher and Scott, the coniugacy classes of complements of N in G are at most $|N|^4$.

It is clear that every complement X of N in G has index $|N|$ and so there are at most $|N|$ coniugates of X in G. Using these facts we conclude that the number of complements of N in G is at most $|N|^5$ and hence $|\Omega_2| \leq |N|^5$.

To obtain the second bound of $|\Omega_2|$ we will use again the theorem proved by Gross and Kovács, Aschbacher and Scott, but in this case we will estimate the number of complements of $N/K \cong S$ in $N_G(K)/K$ as follows.

Define $t = n(d-1)+1$; since $d(G) \leq d$ and $|G : N_G(K)| = n$, from the Nielsen-Schreier Theorem we deduce $d(N_G(K)) \leq t$. A permutation group of degree $s > 3$ can be generated by $[\frac{s}{2}]$ elements, where $[\frac{s}{2}]$ denotes the integer part of $\frac{s}{2}$ (this is a theorem by P.M. Neumann, announced in [**18**]; a proof has been published in [**5**]). In particular, since $N_G(K)\pi \leq \mathrm{Sym}(n-1)$, $d(N_G(K)\pi) \leq [\frac{n}{2}]$. Note that $K \leq N_G(K) \cap \ker\pi$ and that $\frac{N_G(K)\cap\ker\pi}{K}$ is a normal subgroup of $\frac{N_G(K)}{K}$ with $d\left(\frac{N_G(K)/K}{N_G(K)\cap\ker\pi/K}\right) = d(N_G(K)\pi) \leq [\frac{n}{2}]$. Take $\alpha_1, \dots, \alpha_{[\frac{n}{2}]}$ generating $\frac{N_G(K)}{K}$ modulo $\frac{N_G(K)\cap\ker\pi}{K}$. Since $d(N_G(K)/K) \leq d(N_G(K)) \leq t$, by Proposition 2.1, there exist $\beta_1, \dots, \beta_t \in \frac{N_G(K)\cap\ker\pi}{K}$ such that $\frac{N_G(K)}{K} = \left\langle \alpha_1\beta_1, \dots, \alpha_{[\frac{n}{2}]}\beta_{[\frac{n}{2}]}, \beta_{[\frac{n}{2}]+1} \dots, \beta_t \right\rangle$. Let $u = t - [\frac{n}{2}]$ and take $\gamma_1 = \beta_{[\frac{n}{2}]+1}, \dots, \gamma_u = \beta_t$, $\gamma_{u+1} = \alpha_1\beta_1, \dots, \gamma_t = \alpha_{[\frac{n}{2}]}\beta_{[\frac{n}{2}]}$; $\frac{N_G(K)}{K} = \langle\gamma_1, \dots, \gamma_t\rangle$ and $\gamma_i \in \frac{N_G(K)\cap\ker\pi}{K}$ for every $i \leq u$.

Now assume that $N_G(K)/K$ splits over N/K. For any complement Y of N/K in $N_G(K)/K$ there is a map $\delta : \{\gamma_1, \dots, \gamma_t\} \to N/K \cong S$ such that $Y = \langle\gamma_1\gamma_1^\delta, \dots, \gamma_u\gamma_u^\delta, \dots, \gamma_t\gamma_t^\delta\rangle$. Consider the subgroup $\overline{Y} = \langle\gamma_1\gamma_1^\delta, \dots, \gamma_u\gamma_u^\delta\rangle$ of Y; if we identify $N_G(K)/K$ with a subgroup of $\mathrm{Aut}\, S \times (\mathrm{Out}\, S \wr \mathrm{Sym}(n-1))$, we have $\overline{Y} \leq \mathrm{Aut}\, S \times (\mathrm{Out}\, S)^{n-1}$; in particular the elements γ_i's, $1 \leq i \leq u$, can be written in the form $\gamma_i = (h_i, k_i)$ with $h_i \in \mathrm{Aut}\, S$ and $k_i \in (\mathrm{Out}\, S)^{n-1}$;

moreover, if $x_i \in S$ is the image of γ_i under δ, $\gamma_i\gamma_i^\delta = (h_i x_i, k_i)$. Let ρ_1 and ρ_2 be the projections of $\overline{Y}$ onto $\operatorname{Aut} S$ and $(\operatorname{Out} S)^{n-1}$, respectively. Since the third term $(\operatorname{Out} S)^{(3)}$ of the derived series of $\operatorname{Out} S$ is trivial, it turns out to be $\overline{Y}^{(3)} \leq S \cap Y = 1$ and, as consequence, $\overline{Y}^{(3)} = 1$. Notice also that $\overline{Y}^{(3)}$ is isomorphic to $\overline{Y}^{(3)}\rho_1 = \langle h_1 x_1, \dots, h_u x_u \rangle^{(3)}$; this implies that the elements $x_1, \dots, x_u$ must be chosen in such a way as to make $\langle h_1 x_1, \dots, h_u x_u \rangle$ a solvable subgroup of $\operatorname{Aut} S$. Hence the next step is to estimate the number of the suitable choices for $x_1, \dots, x_u \in S$. Of course, $h_1 x_1, \dots, h_u x_u$ must belong to R, a maximal solvable subgroup of $\operatorname{Aut} S$. By Proposition 2.4, $\operatorname{Aut} S$ has at most $|\operatorname{Aut} S|^c$ maximal solvable subgroups. Moreover, fixed a maximal solvable subgroup R of $\operatorname{Aut} S$, the number of $(x_1, \dots, x_u) \in S^u$ such that $(h_1 x_1, \dots, h_u x_u) \in R^u$ is at most $|R \cap S|^u$ and such number can be bounded by $|S|^{\alpha u}$ using Proposition 2.5.

At this point we can state that the number of the choices for the suitable elements $x_1, \dots, x_u$ of S is at most $|S|^{\alpha u}|\operatorname{Aut} S|^c$.

Finally, since it is possible to choice γ_i^δ, $i > u$, in at most $|S|$ different ways the complements of S in $N_G(K)/K$ are at most

$$|S|^{\alpha u - u + t}|\operatorname{Aut} S|^c, \text{ where } \alpha u - u + t \leq n(\alpha(d-1) + \tfrac{1-\alpha}{2}) + \alpha.$$

At this point of the proof we can repeat the same arguments used for the first bound of $|\Omega_2|$ and conclude that

$$|\Omega_2| \leq |N||S|^{n(\alpha(d-1)+\frac{1-\alpha}{2})}|S|^\alpha|\operatorname{Aut} S|^c \leq |N|^{1+\alpha(d-1)+\frac{1-\alpha}{2}}|S|^\alpha|\operatorname{Aut} S|^c.$$

b) Notice that if $G \cap \Gamma > N$ then, for any $w \in N^d$, $G \cap \Gamma = H_w N \cap \Gamma = N(\Gamma \cap H_w) > N$, hence $H_w \cap \Gamma \neq 1$. But then $\Omega_3 \neq \emptyset$ implies $G \cap \Gamma = N$ and $\Omega_3 = \{w \in N^d \mid H_w \cap N = 1\}$. Therefore, the cardinality of Ω_3 can be bounded estimating again the number of complements of N in G. Precisely, we can repeat the same arguments used above to prove $|\Omega_2| \leq |N|^5$. But in this case because of $G \cap \Gamma = N$ any complement of N/K in $N_G(K)/K$ turns out to be isomorphic to a subgroup of $\operatorname{Sym}(n-1)$ and, in particular, $d(Y) \leq [\frac{n}{2}]$. It follows $|\operatorname{Der}(Y, N/K)| \leq |S|^{\frac{n}{2}}$ and arguing from analogy with the previous case we deduce that

$$|\Omega_3| \leq |N||S|^{\frac{n}{2}} \leq |N|^{\frac{3}{2}}.$$

Lemma 2.9. $|\Omega_4| \leq |N|^{\frac{d}{2}+\frac{19}{20}}$.

Proof. Let $w \in \Omega_4$. Notice that $H_w \cap N$ is a normal subgroup of H_w and $G\pi = (H_w)\pi$ is a transitive subgroup of $\operatorname{Sym}(n)$; this implies $(H_w \cap N)\pi_i = S$ for each $1 \leq i \leq n$. But then, there exists a maximal subgroup M of G containing H_w such that $(M \cap N)\pi_i = S$ for every $1 \leq i \leq n$. This means that $M \cap N = \prod_{B \in \Phi} D_B$, where Φ is an imprimitive system of $G\pi$ and, for every block $B \in \Phi$, D_B is a full diagonal subgroup of $\prod_{j \in B} S_j$ (that is,

if $B = \{i_1, \dots, i_r\}$, there exists $\Psi = (\varphi_2, \dots, \varphi_r) \in (\operatorname{Aut} S)^{r-1}$ such that $D_B = \{(x, x^{\varphi_2}, \dots, x^{\varphi_r}) \mid x \in S\} \leq S_{i_1} \times \cdots \times S_{i_r})$.

In the following, we will denote with $\mathcal{D}$ the set $\{\prod_{B\in\Phi} D_B \mid \Phi \text{ an imprimitive system of } G\pi\}$. By Lemma 2.2 if M is a maximal subgroup of G with $M \cap N = U \in \mathcal{D}$ then the number of $w \in N^d$ with $H_w \leq M$ is at most $|U|^d$. Moreover, by Lemma 2.3, for every $U \in \mathcal{D}$ there exists at most a unique maximal subgroup M of G satisfying $M \cap N = U$. Therefore

$$|\Omega_4| \leq \sum_{U\in\mathcal{D}} |U|^d$$

so we have to estimate $\sum_{U\in\mathcal{D}} |U|^d$.

Using again that $G\pi$ acts transitively on $\{1, \dots, n\}$, every element $U = D_{B_1} \times \cdots \times D_{B_t}$ of $\mathcal{D}$ can be uniquely determined only from the knowledge of $B = B_1$, the block which contains 1, and $\Psi_1, \dots, \Psi_t$. Note that $|U| = |S|^t$ and $\Psi_i \in (\operatorname{Aut} S)^{|B|-1}$, $1 \leq i \leq t$. As $t = \frac{n}{|B|} \leq \frac{n}{2}$ and, by Proposition 2.6, $|\operatorname{Aut} S| \leq |S|^{\frac{3}{2}}$

$$\sum_{U\in\mathcal{D}} |U|^d = \sum_B |S|^{\frac{nd}{|B|}} |\operatorname{Aut} S|^{n-\frac{n}{|B|}} \leq \sum_B |S|^{\frac{n}{2}d+\frac{3}{4}n} = \sum_B |N|^{\frac{d}{2}+\frac{3}{4}}.$$

The different choices for B are at most 2^{n-1} and $2^{n-1} \leq (60^{\frac{1}{5}})^n \leq |S|^{\frac{n}{5}} \leq |N|^{\frac{1}{5}}$. So we conclude

$$|\Omega_4| \leq \sum_B |N|^{\frac{d}{2}+\frac{3}{4}} \leq 2^{n-1}|N|^{\frac{d}{2}+\frac{3}{4}} \leq |N|^{\frac{d}{2}+\frac{19}{20}}.$$

Lemma 2.10. $|\Omega_1| \geq c_s|N|^d$.

Proof. Define $\Delta_1 = \{(n_1, n_2) \in N^2 \mid (N_{\langle g_1 n_1, g_2 n_2\rangle}(S_1))\phi_1 \geq S\}$.

Of course, $|\Omega_1| \geq |\Delta_1||N|^{d-2}$, therefore the proof is concluded if we will show that $|\Delta_1| \geq c_s|N|^2$. Let $g_1 = (\alpha_1, \dots, \alpha_n)\rho$ and $g_2 = (\beta_1, \dots, \beta_n)\sigma$ with $\rho, \sigma \in \operatorname{Sym}(n)$ and $\alpha_i, \beta_i \in \operatorname{Aut} S$. Consider ρ and σ as products of disjoint cycles (including cycles of length 1) and consider in particular the cycles $(r_1, \dots, r_t)$ and $(s_1, \dots, s_u)$ with $r_1 = s_1 = 1$ of ρ and σ respectively.

Suppose $n_1 = (x_1, \dots, x_n) \in N$ and $n_2 = (y_1, \dots, y_n) \in N$, and define $\bar{g}_1 = g_1 n_1$ and $\bar{g}_2 = g_2 n_2$. It turns out to be $\bar{g}_1^t, \bar{g}_2^u \in N_1$, $(\bar{g}_1^t)\phi_1 = h_1 x_1$ and $(\bar{g}_2^u)\phi_1 = h_2 y_1$ with $h_1 = \alpha_{r_1} x_{r_2} \alpha_{r_2} \dots x_{r_t} \alpha_{r_t}$, $h_2 = \beta_{s_1} y_{s_2} \beta_{s_2} \dots y_{s_t} \beta_{s_t}$.

We notice that in order to find $(n_1, n_2) \in \Delta_1$, we can choose $x_2, \dots, x_n$ and $y_2, \dots, y_n$ arbitrarily, while x_1, y_1 must be selected in such a way as to make $\langle h_1 x_1, h_2 y_1\rangle = \langle h_1, h_2, S\rangle \geq S$. By Proposition 2.7 there exist at least $c_s|S|^2$ ways to choose the elements $x_1, y_1 \in S$, so we conclude that $|\Delta_1| \geq c_s|N|^2$.

Lemma 2.11. $\Omega_1 \setminus (\Omega_3 \cup \Omega_4) \subseteq \Omega$.

Proof. Suppose that $w \in \Omega_1 \setminus (\Omega_3 \cup \Omega_4)$. As $w \in \Omega_1 \setminus \Omega_3$, $(H_w \cap \Gamma)\pi_1$ is a nontrivial subgroup of $\operatorname{Aut} S$ normalized by $(N_1 \cap H_w)\phi_1 \geq S$, therefore $(H_w \cap N)\pi_1 = S$; on the other hand $w \notin \Omega_4$, so $H_w = G$.

Lemma 2.12. $\frac{|\Omega|}{|N|^d} \to 1$ *as* $|S| \to \infty$.

Proof. By Lemmas 2.8, 2.9, 2.10 and 2.11

$$\frac{|\Omega|}{|N|^d} \geq \frac{|\Omega_1| - |\Omega_3| - |\Omega_4|}{|N|^d} \geq c_s - \frac{|N|^{\frac{3}{2}}}{|N|^d} - \frac{|N|^{\frac{d}{2}+\frac{19}{20}}}{|N|^d}.$$

Since $d \geq 2$, by Proposition 2.7 we conclude

$$\frac{|\Omega|}{|N|^d} \geq c_s - \frac{1}{|N|^{\frac{1}{2}}} - \frac{1}{|N|^{\frac{1}{20}}} \geq c_s - \frac{2}{|S|^{\frac{1}{20}}} \to 1 \text{ as } |S| \to \infty.$$

We have to prove that $\frac{|\Omega|}{|N|^d} \to 1$ when $|N| = |S|^n \to \infty$. By the previous lemma this is true if $|S| \to \infty$. It remains to discuss the case when $|S|$ is bounded, say $|S| \leq \mu$, and $n \to \infty$.

Lemma 2.13. *Let* ϵ *and* μ *be two positive real numbers. There exists* n_1 *such that if* $n \geq n_1$ *and* $|S| \leq \mu$ *then* $\frac{|\Omega_2|}{|N|^d} \leq \frac{\epsilon}{3}$.

Proof. By Lemma 2.8 and Proposition 2.6, and noticing that $|S| \geq 60$, we deduce

$$\frac{|\Omega_2|}{|N|^d} \leq \frac{|S|^\alpha |\operatorname{Aut} S|^c |N|^{1+\alpha(d-1)+\frac{1-\alpha}{2}}}{|N|^d} \leq \mu^{\alpha+\frac{3c}{2}} |N|^{(1-\alpha)(\frac{3}{2}-d)}$$
$$\leq \frac{\mu^{\alpha+\frac{3c}{2}}}{60^{(1-\alpha)(d-\frac{3}{2})n}}$$

and this bound tends to 0 as n tends to infinity, since $d \geq 2$.

Lemma 2.14. *Let* ϵ *and* μ *be two positive real numbers. There exists* n_2 *such that if* $n \geq n_2$ *and* $|S| \leq \mu$ *then* $\frac{|\Omega_5|}{|N|^d} \leq \frac{\epsilon}{3}$.

Proof. Denote by $\mathcal{M}$ the set of all maximal subgroups of G such that $1 < (M \cap N)\pi_1 < S$. For each $w \in \Omega_5$, there exists a maximal subgroup $M \in \mathcal{M}$ such that $H_w \leq M$. By Lemma 2.2, selected $M \in \mathcal{M}$, the elements w of N^d such that $H_w \leq M$ are at most $|M \cap N|^d$, so it follows

$$|\Omega_5| \leq \sum_{M \in \mathcal{M}} |M \cap N|^d.$$

Define $H = (M \cap N)\pi_1$. For any $1 \leq i \leq n$, G contains an element of the form $(\alpha_{1i}, \ldots, \alpha_{ni})\sigma$ with $1\sigma = i$. Since $G = MN$, there are $x_{1i}, \ldots, x_{ni}$ in S such that $(\alpha_{1i}x_{1i}, \ldots, \alpha_{ni}x_{ni})\sigma \in M$ and this implies

$$(M \cap N)\pi_i = ((M \cap N)\pi_1)^{\alpha_{1i}x_{1i}} = (H^{\alpha_{1i}})^{x_{1i}}.$$

Set $X = (M \cap N)\pi_1 \times \cdots \times (M \cap N)\pi_n$; since $M \cap N \leq X$ and M normalizes X, we have $M \leq MX < G$. Therefore, by the maximality of M, it turns out to be

$$M \cap N = H \times H^{\alpha_{12}x_{12}} \times \cdots \times H^{\alpha_{1n}x_{1n}}.$$

By Lemma 2.3, if $M_1, M_2 \in \mathcal{M}$ with $M_1 \neq M_2$ then $M_1 \cap N \neq M_2 \cap N$. It follows

$$|\Omega_5| \leq \sum_{H,x_{12},\ldots,x_{1n}} |H \times H^{\alpha_{12}x_{12}} \times \cdots \times H^{\alpha_{1n}x_{1n}}|^d$$

where H runs in the set of proper subgroups of S and x_{1i}, $2 \leq i \leq n$, is a coset representative of $N_S(H^{\alpha_{1i}})$ in S. Hence x_{1i} can be chosen in at most $|S : N_S(H^{\alpha_{1i}})| \leq |S : H|$ different ways and

$$|\Omega_5| \leq \sum_{H<S} |H|^{nd} \frac{|S|^{n-1}}{|H|^{n-1}}.$$

In particular

$$\frac{|\Omega_5|}{|N|^d} \leq \sum_{H<S} \left(\frac{|H|}{|S|}\right)^{n(d-1)+1}.$$

Notice that $H < S$ and so $\frac{|H|}{|S|} \leq \frac{1}{2}$. Moreover, since $|S| \leq \mu$, the number of subgroups of S can be bounded by an integer δ (i.e., $\delta = 2^\mu$). At this point we can conclude that

$$\frac{|\Omega_5|}{|N|^d} \leq \frac{\delta}{2^{n(d-1)+1}}$$

and such bound tends to 0 as n tends to infinity, since $d \geq 2$.

Lemma 2.15. *Let ϵ and μ be two positive real numbers. There exists n_3 such that if $n \geq n_3$ and $|S| \leq \mu$ then $\frac{|\Omega_4|}{|N|^d} \leq \frac{\epsilon}{3}$.*

Proof. This is an immediate consequence of Lemma 2.9.

Now we can complete the proof of our theorem. We are assuming that $N = S^n$ for a suitable nonabelian simple group S and a suitable integer n. We have to show that if ϵ is a fixed positive real number then there exists an integer ν such that $\frac{|\Omega|}{|N|^d} \geq 1 - \epsilon$ if $|N| \geq \nu$.

By Lemma 2.12 there exists μ such that $\frac{|\Omega|}{|N|^d} \geq 1 - \epsilon$ if $|S| \geq \mu$. For these choices of ϵ and μ take n_1, n_2 and n_3 as in Lemmas 2.13, 2.14, 2.15 and let $\nu = \mu^{\max\{n_1,n_2,n_3\}}$. Suppose $|N| = |S|^n \geq \nu$. If $|S| \geq \mu$ then $\frac{|\Omega|}{|N|^d} \geq 1 - \epsilon$ by the definition of μ. Otherwise it must be $n \geq \max\{n_1, n_2, n_3\}$. In that case, since $N^d \setminus (\Omega_2 \cup \Omega_4 \cup \Omega_5) \subseteq \Omega$, applying Lemmas 2.13, 2.14, 2.15 we deduce

$$\frac{|\Omega|}{|N|^d} \geq 1 - \frac{|\Omega_2|}{|N|^d} - \frac{|\Omega_4|}{|N|^d} - \frac{|\Omega_5|}{|N|^d} \geq 1 - \epsilon.$$

3. Proof of Theorem 1.4.

To prove Theorem 1.4 we apply the same arguments that have already been used to prove Theorem 9 in [**16**]; so we give only a sketch of the proof, omitting some details that can be found in [**16**].

Suppose that H is a minimal counterexample. There exist a finite group G with a unique minimal normal subgroup N and an integer $t \geq 2$ such that $H \cong G_t$; moreover N is nonabelian. Let $C = C_{\mathrm{Aut}\, G}(G/N)$ denote the group of those automorphisms of G that act trivially on G/N. By [**8**] Theorem 2.7 and Corollary 1.2, $d(G_t) > d+1$ implies

$$t > \frac{\phi_G(d+1)}{|C|\phi_{G/N}(d+1)} \geq \frac{\gamma |N|^{d+1}}{|C|}. \tag{1}$$

By hypothesis $G_t = \langle P, Q\rangle$ and $P = \langle \alpha_1, \ldots, \alpha_d\rangle$, $Q = \langle \beta_1, \ldots, \beta_d\rangle$. Denote by $\pi_1 : G^t \to G$ the projection onto the first factor and let $a_i = \alpha_i \pi_1$, $b_j = \beta_j \pi_1, 1 \leq i, j \leq d$. Let Δ be the set of elements $(x_1, ..., x_d, y_1, ..., y_d)$ in G^{2d} such that $\langle x_1, \ldots, x_d, y_1, \ldots, y_d\rangle = G$, $\langle x_1, \ldots, x_d\rangle$ is a p-group, $\langle y_1, \ldots, y_d\rangle$ is a q-group, $x_i \equiv a_i \mod N$ and $y_j \equiv b_j \mod N, 1 \leq i, j \leq d$. As it is noted in Section 2 of [**16**], $G_t = \langle P, Q\rangle$ implies $t \leq \frac{|\Delta|}{|C|}$. By the proof of [**16**] Lemma 6, $|\Delta| \leq |N||N|_p^{d-1}|N||N|_q^{d-1}$. The normal subgroup N is a direct product of isomorphic nonabelian simple groups, so $|N|$ is divided by at least three different primes and by 4; in particular $|N|_p|N|_q \leq \frac{|N|}{3}$. We deduce

$$t \leq \frac{|N|^{d+1}}{3^{d-1}|C|}. \tag{2}$$

Comparing (1) and (2) we conclude $\gamma < \frac{1}{3^{d-1}}$ which is false since $d \geq 1 - \log_3 \gamma$.

References

[1] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra, **92** (1985), 44-80, MR 86m:20029, Zbl 0549.20011.

[2] L. Babai, A.J. Goodman and L. Pyber, *Groups without faithful transitive permutation representations of small degree*, J. Algebra, **195** (1997), 1-29, MR 98g:20005, Zbl 0886.20020.

[3] A.V. Borovik, L. Pyber and A. Shalev, *Maximal subgroups in finite and profinite groups*, Trans. Amer. Math. Soc., **348** (1996), 3745-3761, MR 96m:20046, Zbl 0866.20018.

[4] K. Buzási and L.G. Kovács, *The minimal number of generators of wreath products of nilpotent groups*, Contemp. Math., **93** (1989), 115-121, MR 90d:20050, Zbl 0675.20023.

[5] P.J. Cameron, R. Solomon and A. Turull, *Chains of subgroups in symmetric groups*, J. Algebra, **127** (1989), 340-352, MR 91a:20008, Zbl 0683.20004.

[6] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985, MR 88g:20025, Zbl 0568.20001.

[7] F. Dalla Volta and A. Lucchini, *Generation of almost simple groups*, J. Algebra, **178** (1995), 194-223, MR 97a:20022, Zbl 0839.20021.

[8] 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, MR 99a:20030, Zbl 0902.20013.

[9] J.D. Dixon, *The probability of generating the symmetric group*, Math. Z., **110** (1969), 199-205, MR 40 #4985, Zbl 0176.29901.

[10] W. Gaschütz, *Zu einem von B. H. und H. Neumann gestellten Problem*, Math. Nachr., **14** (1955), 249-252, MR 18,790b, Zbl 0071.25202.

[11] ———, *Die Eulersche Funktion endlicher auflösbarer Gruppen*, Illinois J. Math., **3** (1959), 469-476, MR 21 #6393, Zbl 0093.25002.

[12] F. Gross and L.G. Kovács, *On normal subgroups which are direct products*, J. Algebra, **90** (1984), 133-168, MR 86a:20021, Zbl 0594.20018.

[13] R. Guralnick, *Generation of simple groups*, J. Algebra, **103** (1986), 381-401, MR 87j:20029, Zbl 0601.20013.

[14] W. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata, **36** (1990), 67-87, MR 91j:20041, Zbl 0718.20011.

[15] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata, **56** (1995), 103-113, MR 96h:20116, Zbl 0836.20068.

[16] A. Lucchini, *On the number of generators of finite images of free products of finite groups*, J. Algebra, **245**(**2**) (2001), 552-561, CMP 1 863 891.

[17] A. Lucchini and F. Menegazzo, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Sem. Mat. Univ. Padova, **98** (1997), 173-191, MR 98m:20034, Zbl 0895.20027.

[18] A. McIver and P.M. Neumann, *Enumerating finite groups*, Quart. J. Math. Oxford Ser. (2), **38** (1987), 473-488, MR 89a:11097, Zbl 0627.20014.

Dipartimento di Matematica
Università di Brescia
Via Valotti 9, 25133 Brescia, Italy
E-mail address: lucchini@bsing.ing.unibs.it

Dipartimento di Matematica
Università di Brescia
Via Valotti 9, 25133 Brescia, Italy
E-mail address: morini@bsing.ing.unibs.it