ISRAEL JOURNAL OF MATHEMATICS **132** (2002), 29–44

HOW MANY ELEMENTS ARE NEEDED TO GENERATE A FINITE GROUP WITH GOOD PROBABILITY?

BY

ELOISA DETOMI, ANDREA LUCCHINI AND FIORENZA MORINI

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

ABSTRACT

We prove that for any real number $0 < \alpha < 1$, there exists a constant c_α such that the probability of generating a finite group G with $[d(G) + c_\alpha \log\log|G| \log\log\log|G|]$ elements is at least α.

1. Introduction

For any finite group G, let $d(G)$ be the smallest cardinality of a generating set of G and let $\phi_G(t)$ denote the number of ordered t-tuples $(g_1, \ldots, g_t)$ of elements of G that generate G. The number $P_G(t) = \phi_G(t)/|G|^t$ gives the probability that t randomly chosen elements of G generate G.

The probability of generating G with $d(G)$ elements can be very small. For example $P_{\mathbb{Z}_m}(1)$, the probability of generating with one element the cyclic group of order m, tends to 0 when the number of prime divisors of m tends to infinity. This give rise to the following question: given a real number $0 < \alpha < 1$, find an integer $d_\alpha(G)$ such that $P_G(d_\alpha(G)) \geq \alpha$. It was noticed by Kantor and Lubotzky [5] that the difference $d_\alpha(G) - d(G)$ can be arbitrarily large, even with the restriction $d(G) = 2$; in other words, there exists no function $\delta\colon \mathbb{N} \to \mathbb{N}$ satisfying $d_\alpha(G) \leq \delta(d(G))$ for any finite group G. However, a bound for $d_\alpha(G)$ can be given in terms of the order of G; for example, it is easy to prove (see Pak [8], Theorem 1.1) that $d_\alpha(G) \leq \log|G| + 2 - \log(1-\alpha)$ (here, and throughout the paper, all the logarithms are on base 2). The previous bound is quite weak.

Received November 15, 2001

Pak suggested that it can be improved proving the following conjecture: *for each* $0 < \alpha < 1$, *there exists a constant* c_α *such that* $d_\alpha(G) \leq c_\alpha d(G) \log\log|G|$ *for any finite group* G.

In this paper we present evidence for this conjecture; we prove (Proposition 19) that *there exists a constant* c_α *such that for any finite group* G, $d_\alpha(G) - d(G) \leq c_\alpha \log\log|G| \log\log\log|G|$ *holds.* A slightly stronger result can be proved, replacing $\log(G)$ by the length $\lambda(G)$ of a composition series of G.

THEOREM 1: *Given a real number* $0 < \alpha < 1$, *there exists a constant* c_α *such that, for any finite group* G,

$$P_G([d(G) + c_\alpha \log\lambda(G) \log\log\lambda(G)]) \geq \alpha$$

if $\lambda(G) \geq 4$; *otherwise* $P_G([d(G) + c_\alpha]) \geq \alpha$.

This is a consequence of a more general result.

THEOREM 2: *There is a constant* c *such that if* $g(x) \to \infty$ *as* $x \to \infty$ *and* $f(x) = \log x(c\log\log x + g(x))$, *then*

$$\lim_{x\to\infty} \inf_{\substack{G \text{ s.t} \\ \lambda(G)\leq x}} P_G([d(G) + f(x)]) = 1.$$

This implies in particular that if x is large enough and $\gamma > c$, then, whenever $\lambda(G) \leq x$, $[d(G) + \gamma\log x\log\log x]$ randomly chosen elements of G almost certainly generate G.

One could expect that Theorem 2 holds under the weaker hypothesis that $f(x)$ tends to infinity as x tends to infinity. This is true ([8], Theorem 4.1) if G runs in the class of nilpotent groups, but it is not true in the general case; take $G_n = (\mathrm{Alt}(n))^{n!/8}$. Kantor and Lubotzky [5] proved that $d(G_n) = 2$ for large n; however, for any real number $0 < \alpha < 1$ there is a universal constant k_α such that $d_\alpha(G_n) \geq k_\alpha n$ if n is large enough. Since $\lambda(G_n) = n!/8$ and $\log n! \sim n\log n$, we deduce that a necessary condition for $\lim_{n\to\infty} P_{G_n}([2+f(\lambda(G_n))]) = 1$ is that asymptotically

$$f(x) \geq k\frac{\log x}{\log\log x}$$

for a suitable constant k. Finally, note that with the restriction that G is soluble, $\lim_{x\to\infty}\inf_{G \text{ s.t. } \lambda(G)\leq x} P_G([d(G) + f(x)]) = 1$ if $\lim_{x\to\infty} f(x) - \log x = \infty$ (this is an easy consequence of Corollary 11).

In section 4 we describe some applications of Theorem 2 to the case of permutation and linear groups. For example, we prove that if $\beta > 1/2$ and n is large enough then $[\beta n]$ randomly chosen elements of a permutation group G of degree n almost certainly generate G. More precisely we have the following result.

COROLLARY 3: *Given two real numbers α and β with $0 < \alpha < 1$ and $\beta > 1/2$ there exists an integer $\bar{n}$ such that if $G \leq \mathrm{Sym}(n)$ and $n \geq \bar{n}$, then $d_\alpha(G) \leq \beta n$.*

A similar result holds for linear groups.

COROLLARY 4: *Let F be a field which has finite degree over its prime subfield. Given two real numbers α and β with $0 < \alpha < 1$ and $\beta > 3/2$ there exists an integer $\bar{n}_F$ such that if G is a completely reducible subgroup of $\mathrm{GL}(n, F)$ and $n \geq \bar{n}_F$, then $d_\alpha(G) \leq \beta n$.*

2. Preliminary results

If G is a finite group and N is a normal subgroup of G, we define $P_{G,N}(t) = P_G(t)/P_{G/N}(t)$. This number is the probability that a t-tuple generates G, given that it generates G modulo N. In particular $P_{G,G}(t) = P_G(t)$. The following lemma is an immediate consequence of this definition.

LEMMA 5: *Let G be a finite group and let $1 = N_0 < N_1 < \cdots < N_l = G$ be a normal series of G of length l. Then*

$$P_G(t) = \prod_{1 \leq i \leq l} P_{G/N_{i-1}, N_i/N_{i-1}}(t).$$

Now we consider a normal series Σ: $1 = N_0 < N_1 < \cdots < N_l = G$ such that each factor is soluble or a direct product of nonabelian simple groups. We define

$$\mathcal{A}_{G,\Sigma}(t) = \prod_{\substack{i \text{ s.t.} \\ N_i/N_{i-1} \\ \text{soluble}}} P_{G/N_{i-1}, N_i/N_{i-1}}(t), \quad \mathcal{B}_{G,\Sigma}(t) = \prod_{\substack{i \text{ s.t.} \\ N_i/N_{i-1} \\ \text{nonsoluble}}} P_{G/N_{i-1}, N_i/N_{i-1}}(t).$$

Clearly, $P_G(t) = \mathcal{A}_{G,\Sigma}(t) \cdot \mathcal{B}_{G,\Sigma}(t)$.

LEMMA 6: *Let G be a finite group. If N is an abelian minimal normal subgroup of G, then*

$$P_{G,N}(t) = 1 - k/|N|^t$$

where $k = 0$ if G does not split over N, $k = |N|^{\theta_N}|H^1(G/N, N)|$ (with $\theta_N = 0$ or 1 according as N is trivial or not as a G-module) otherwise.

Proof: This formula is really Satz 2 of [4] with k being the number of complements to N in G. But if this number is nonzero, it coincides with the number of derivations of G/N in N and by definition $|\operatorname{Der}(G/N,N)| = |N|^{\theta_N}|H^1(G/N,N)|$. This completes the proof. ∎

If M is an irreducible G-module, then we define the numbers q_M, r_M and s_M as follows: $q_M = |\operatorname{End}_G M|$, $q_M^{r_M} = |M|$, $q_M^{s_M} = |H^1(G/C_G(M),M)|$. Moreover, let $\delta_G(M)$ be the number of complemented factors G-isomorphic to M in a principal series of G; in [1] the authors proved that this number is an invariant of the group G.

In the following, to simplify our notation, whenever we write $q_A{}^x$ we will mean that the value of this power is 1 if x is positive.

LEMMA 7: *Let G be a finite group. If N is an abelian minimal normal subgroup of G and G splits on N, then*

$$P_{G,N}(t) = 1 - q_N^{r_N(\theta_N - t) + s_N + \delta_G(N) - 1}.$$

Proof: In [1], Theorem (2.10), $|H^1(G/N,N)| = |H^1(G/C_G(N),N)|q_N^{\delta_{G/N}(N)}$ is proved and, since $\delta_{G/N}(N) = \delta_G(N) - 1$, by Lemma 6 we deduce that $k = q_N^{r_N\theta_N} \cdot q_N^{s_N} \cdot q_N^{\delta_G(N)-1}$, that is

$$P_{G,N}(t) = 1 - q_N^{r_N(\theta_N - t) + s_N + \delta_G(N) - 1}. \quad ∎$$

Let M be an irreducible G-module isomorphic to a complemented factor in a principal series of G. Define

$$A_{G,M}(t) = \prod_{0 \le j \le \delta_G(M)-1} (1 - q_M^{r_M(\theta_M - t) + s_M + j}).$$

THEOREM 8: *Let G be a finite group. Then $\mathcal{A}_{G,\Sigma}(t)$ does not depend on the fixed series. In particular*

$$\mathcal{A}_{G,\Sigma}(t) = \prod_{1 \le i \le \xi(G)} A_{G,M_i}(t),$$

where $M_1, \ldots, M_{\xi(G)}$, up to isomorphism, are the irreducible G-modules isomorphic to a complemented factor in a principal series of G.

Proof: We prove this theorem by induction on the order of G. Let Σ be a normal series $1 = N_0 < N_1 < \cdots < N_l = G$ such that each factor is soluble or a direct product of nonabelian simple groups. Let X be a minimal normal subgroup of G contained in N_1. If we consider Σ', the normal series of G/X defined by the subgroups XN_i/X, we note that

$$P_{G/X}(t) = P_{G/X,N_1/X}(t) \prod_{2 \le i \le l} P_{G/N_{i-1},N_i/N_{i-1}}(t).$$

Moreover, if we observe that

$$P_G(t) = P_{G,N_1}(t) \prod_{2\le i\le l} P_{G/N_{i-1},N_i/N_{i-1}}(t)$$

and

$$P_{G,N_1}(t) = P_{G/X,N_1/X}(t) \cdot P_{G,X}(t)$$

we can conclude that

$$\mathcal{A}_{G,\Sigma}(t) = \begin{cases} \mathcal{A}_{G/X,\Sigma'}(t) & \text{if } X \text{ is nonabelian or noncomplemented in } G, \\ \mathcal{A}_{G/X,\Sigma'}(t) \cdot P_{G,X}(t) & \text{otherwise.} \end{cases}$$

Moreover, in any case by inductive hypothesis we have

$$\mathcal{A}_{G/X,\Sigma'}(t) = \prod_{1\le i\le \xi(G/X)} A_{G/X,M_i}(t),$$

where $M_1, \dots, M_{\xi(G/X)}$, up to isomorphism, are the irreducible G/X-modules isomorphic to a complemented factor in a principal series of G/X.

We remark that if M is a G/X-module, then M can be considered as a G-module by setting $m^g = m^{Xt}$ if g belongs to the coset Xt. So $\{M_1, \dots, M_{\xi(G/X)}\}$ can be viewed as a set of nonisomorphic G-modules. Moreover, if M is an irreducible G-module G-isomorphic to a complemented principal factor of G, then X centralizes M and hence M can be considered as a G/X-module. If G/X has a complemented principal factor G-isomorphic to M, then $M \cong M_i$ with $1 \le i \le \xi(G/X)$; otherwise, X is abelian and complemented and $M \cong_G X$.

We observe also that if M is G-isomorphic to a complemented principal factors of G, then the numbers q_M, r_M, s_M only depend on the action of $G/C_G(M)$, so they do not change if we look at M as a module over G or over G/X.

The possible cases are the following:

(a) X is nonabelian or X is not complemented in G. In this case $\xi(G) = \xi(G/X)$ and $\{M_1, \dots, M_{\xi(G/X)}\}$ is a set of representatives for the irreducible G-modules isomorphic to a complemented principal factor of G; for $1 \le i \le \xi(G)$, we have $\delta_G(M_i) = \delta_{G/X}(M_i)$ and so $A_{G/X,M_i}(t) = A_{G,M_i}(t)$. Thus

$$\mathcal{A}_{G,\Sigma}(t) = \mathcal{A}_{G/X,\Sigma'}(t) = \prod_{1\le i\le \xi(G/X)} A_{G/X,M_i}(t) = \prod_{1\le i\le \xi(G)} A_{G,M_i}(t).$$

(b) X is abelian and complemented in G and $\delta_{G/X}(X) > 0$. Also in this case $\xi = \xi(G) = \xi(G/X)$ and $\{M_1, \dots, M_{\xi(G/X)}\}$ is a set of representatives for the irreducible G-modules isomorphic to a complemented principal factor of G; we may assume $M_\xi = X$. If $i \le \xi - 1$, then $\delta_G(M_i) = \delta_{G/X}(M_i)$ and

$A_{G/X,M_i}(t) = A_{G,M_i}(t)$. On the other hand, since X has a complement in G, $\delta_G(X) = \delta_{G/X}(X) + 1$ and, by Lemma 7,

$$P_{G,X}(t) = 1 - q_X^{r_X(\theta_X - t) + s_X + \delta_G(X) - 1}.$$

Therefore

$$\begin{aligned} A_{G,M_\xi}(t) = A_{G,X}(t) &= \prod_{0 \le j \le \delta_G(X)-1} (1 - q_X^{r_X(\theta_X - t)+s_X+j}) \\ &= \prod_{0 \le j \le \delta_{G/X}(X)} (1 - q_X^{r_X(\theta_X - t)+s_X+j}) \\ &= \left[\prod_{0 \le j \le \delta_{G/X}(X)-1} (1 - q_X^{r_X(\theta_X - t)+s_X+j}) \right] (1 - q_X^{r_X(\theta_X - t)+s_X+\delta_{G/X}(X)}) \\ &= A_{G/X,M_\xi}(t) \cdot P_{G,X}(t). \end{aligned}$$

We can conclude that

$$\begin{aligned} \mathcal{A}_{G,\Sigma}(t) = &\mathcal{A}_{G/X,\Sigma'}(t) \cdot P_{G,X}(t) = \left(\prod_{1 \le i \le \xi} A_{G/X,M_i}(t) \right) \cdot P_{G,X}(t) \\ &= \left(\prod_{1 \le i \le \xi - 1} A_{G,M_i}(t) \right) \cdot A_{G/X,M_\xi}(t) \cdot P_{G,X}(t) \\ &= \left(\prod_{1 \le i \le \xi - 1} A_{G,M_i}(t) \right) \cdot A_{G,M_\xi}(t) = \prod_{1 \le i \le \xi(G)} A_{G,M_i}(t). \end{aligned}$$

(c) X is abelian and complemented in G and $\delta_{G/X}(X) = 0$. Thus $\xi = \xi(G) = \xi(G/X) + 1$ and $\{M_1, \dots, M_{\xi(G/X)}, X\}$ is a set of representatives for the irreducible G-modules isomorphic to a complemented principal factor of G. If $i \le \xi - 1$, then $A_{G/X,M_i}(t) = A_{G,M_i}(t)$. Since $\delta_G(X) = 1$, by Lemma 7,

$$A_{G,X}(t) = 1 - q_X^{r_X(\theta_X - t) + s_X} = P_{G,X}(t).$$

Therefore

$$\mathcal{A}_{G,\Sigma}(t) = \mathcal{A}_{G/X,\Sigma'}(t) \cdot P_{G,X}(t) = \left(\prod_{1 \le i \le \xi(G/X)} A_{G/X,M_i}(t) \right) \cdot A_{G,X}(t),$$

and this concludes our proof. ∎

COROLLARY 9: *Let G be a finite group. Then $\mathcal{A}_{G,\Sigma}(t)$ and $\mathcal{B}_{G,\Sigma}(t)$ do not depend on the fixed normal series Σ.*

Proof: Since the probability $P_G(t) = \mathcal{A}_{G,\Sigma}(t) \cdot \mathcal{B}_{G,\Sigma}(t)$ is an invariant of the group G, the result follows by Theorem 8. ∎

Subsequently, we denote $\mathcal{A}_{G,\Sigma}(t)$ and $\mathcal{B}_{G,\Sigma}(t)$ by $\mathcal{A}_G(t)$ and $\mathcal{B}_G(t)$ respectively. Note that $A_{G,M}(t) > 0$ if, and only if, $t \geq h_M$, with

$$h_M = \theta_M + \left\lceil \frac{\delta_G(M) + s_M}{r_M} \right\rceil$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$. Consequently, we remark that $d(G) \geq h_M$.

Proposition 10: *If G is a finite group and M is an irreducible G-module, then*

$$A_{G,M}([d(G)+u]) \geq 1 - 1/|M|^u.$$

Proof: By the previous remark $d(G) \geq h_M$, thus

$$A_{G,M}([d(G)+u]) \geq A_{G,M}([h_M+u]) \geq \prod_{0 \leq j \leq \delta_G(M)-1} (1 - q_M^{r_M(\theta_M - h_M - u) + s_M + j}).$$

But, by the definition of h_M, it follows that $r_M(\theta_M - h_M - u) + s_M \leq -\delta_G(M) - r_M u$, hence

$$\begin{aligned}\prod_{0 \leq j \leq \delta_G(M)-1} (1 - q_M^{r_M(\theta_M - h_M - u) + s_M + j}) &\geq \prod_{0 \leq j \leq \delta_G(M)-1} (1 - q_M^{-r_M u - \delta_G(M) + j}) \\ &\geq 1 - \sum_{0 \leq j \leq \delta_G(M)-1} q_M^{-r_M u - \delta_G(M) + j} \geq 1 - q_M^{-r_M u} \sum_{1 \leq k \leq \delta_G(M)} q_M^{-k} \\ &\geq 1 - q_M^{-r_M u} \sum_{1 \leq k \leq \infty} q_M^{-k} \geq 1 - q_M^{-r_M u} = 1 - 1/|M|^u,\end{aligned}$$

since $q_M^{r_M} = |M|$. ∎

Corollary 11: *Let G be a finite group. Then*

$$\mathcal{A}_G([d(G)+u]) \geq 1 - \xi/2^u,$$

where ξ denotes the number, up to isomorphism, of the irreducible G-modules isomorphic to a complemented factor in a principal series of G.

Proof: Theorem 8 and Proposition 10 imply

$$\begin{aligned}\mathcal{A}_G([d(G)+u]) = \prod_{1 \leq i \leq \xi} A_{G,M_i}([d(G)+u]) &\geq \prod_{1 \leq i \leq \xi} \left(1 - \frac{1}{|M_i|^u}\right) \\ &\geq 1 - \sum_{1 \leq i \leq \xi} \frac{1}{|M_i|^u} \geq 1 - \frac{\xi}{2^u},\end{aligned}$$

since $|M_i| \geq 2$ for every $i = 1, \ldots, \xi$. ∎

The previous corollary gives a bound for $\mathcal{A}(t)$. Now our aim is to bound $\mathcal{B}(t)$. First we need an auxiliary result.

LEMMA 12: *Let G be a finite group and let N be a normal subgroup of G. Then*

$$P_{G,N}(t) \geq P_N(t - d(G/N)).$$

Proof: By definition,

$$P_{G,N}(t) = \frac{\phi_G(t)}{\phi_{G/N}(t)|N|^t}.$$

Choose $g_1, \ldots, g_t$ such that $G = \langle g_1, \ldots, g_t, N\rangle$; it was noticed by Gaschütz [3] that the cardinality of the set

$$\Omega_{g_1,\ldots,g_t} = \{(n_1, \ldots, n_t) \in N^t \mid \langle g_1 n_1, \ldots, g_t n_t\rangle = G\}$$

is independent of the choice of $g_1, \ldots, g_t$, namely

$$|\Omega_{g_1,\ldots,g_t}| = \frac{\phi_G(t)}{\phi_{G/N}(t)}.$$

In particular, given $r = d(G/N)$ and fixed $g_1, \ldots, g_r$ such that $\langle g_1, \ldots, g_r, N\rangle = G$, we consider

$$\Omega_{g_1,\ldots,g_r,1,\ldots,1}.$$

If $\langle x_{r+1}, \ldots, x_t\rangle = N$, then

$$(y_1, \ldots, y_r, x_{r+1}, \ldots, x_t) \in \Omega_{g_1,\ldots,g_r,1,\ldots,1}$$

for any $y_1, \ldots, y_r \in N$. We conclude that

$$\frac{\phi_G(t)}{\phi_{G/N}(t)} \geq |N|^r \phi_N(t-r) \quad \text{and} \quad P_{G,N}(t) \geq \frac{\phi_N(t-r)}{|N|^{t-r}}.$$ ∎

LEMMA 13: *Let G be a finite group. If u, v are positive integers and $u \geq v$, then*

$$P_G(u) \geq 1 - (1 - P_G(v))^{[u/v]}.$$

Proof: Let $n = [u/v]$. Since $u \geq nv$ it is sufficient to prove that

$$P_G(nv) \geq 1 - (1 - P_G(v))^n.$$

Observe that if a (nv)-tuple, say $x_1, \ldots, x_{nv}$, does not generate G, then, in particular,

$$\langle x_1, \ldots, x_v\rangle \neq G, \quad \langle x_{v+1}, \ldots, x_{2v}\rangle \neq G, \quad \ldots, \quad \langle x_{(n-1)v+1}, \ldots, x_{nv}\rangle \neq G.$$

Therefore,

$$|\{\text{nongenerating } (nv)\text{-tuples}\}| \le |\{\text{nongenerating } v\text{-tuples}\}|^n,$$

and we conclude that

$$\begin{aligned} 1 - P_G(nv) &= \frac{|\{\text{nongenerating } (nv)\text{-tuples}\}|}{|G|^{nv}} \\ &\le \frac{|\{\text{nongenerating } v\text{-tuples}\}|^n}{|G|^{nv}} = (1 - P_G(v))^n. \quad \blacksquare \end{aligned}$$

To bound $\mathcal{B}_G(t)$, we combine the two previous lemmas with a deep result on the probability of generating direct products of simple groups, recently proved by Igor Pak.

THEOREM 14 (Pak, [8, Prop. 7.1]p): *There exists a constant δ such that, if a finite group G is a direct product of nonabelian simple groups and m is the maximal number of isomorphic copies of each group involved, then, for every integer $t \ge \delta \max\{\log m, 1\}$,*

$$P_G(t) \ge 1/e.$$

In particular,

$$P_G([\delta \max\{\log m, 1\}] + 1) \ge 1/e.$$

COROLLARY 15: *If a finite group G is a direct product of nonabelian simple groups and m is the maximal number of isomorphic copies of each group involved, then, for every integer u greater than $v = [\delta \max\{\log m, 1\}] + 1$,*

$$P_G(u) \ge 1 - \eta^{u/v-1},$$

where $\eta = 1 - 1/e$ and δ is the constant defined in Theorem 14.

Proof: By Pak's Theorem (14), $P_G(v) \ge 1/e$, so that $1 - P_G(v) \le 1 - 1/e = \eta < 1$. Thus, by Lemma 13, we conclude that

$$P_G(u) \ge 1 - (1 - P_G(v))^{[u/v]} \ge 1 - \eta^{u/v-1}. \quad \blacksquare$$

LEMMA 16: *Let G be a finite group and let $1 = N_0 < N_1 < \cdots < N_l = G$ be a normal series such that each factor N_j/N_{j-1} is either soluble or a direct product of nonabelian simple groups, and in the latter case let m_j be the maximal number of isomorphic copies of each simple group involved. Set m= $\max\{m_j\}$, $v = [\delta \max\{\log m, 1\}] + 1$ and $\eta = 1 - 1/e$. Then, for every integer $u \ge v$, we get*

$$\mathcal{B}_G(d(G) + u) \ge 1 - s\, \eta^{u/v-1},$$

where s is the number of nonsoluble factors in the series.

Proof: Let N_j/N_{j-1} be a direct product of nonabelian simple groups. Set $v_j = [\delta \max\{\log m_j, 1\}] + 1$. By definition, $m \geq m_j$ and $v \geq v_j$.

By Lemma 12 and Corollary 15, for every integer $u \geq v$ we get

$$P_{G/N_{j-1},N_j/N_{j-1}}(d(G)+u) \geq P_{N_j/N_{j-1}}(u) \geq 1 - \eta^{u/v_j - 1}.$$

As $v \geq v_j$ and $\eta < 1$, it follows that

$$P_{G/N_{j-1},N_j/N_{j-1}}(d(G)+u) \geq 1 - \eta^{u/v-1}.$$

Since this holds for every nonsoluble factor N_j/N_{j-1} of the series defined above, by the definition of $\mathcal{B}_G$ we conclude that

$$\begin{aligned} \mathcal{B}_G(d(G)+u) &= \prod_{\substack{j \text{ s.t.} \\ N_j/N_{j-1} \\ \text{nonsoluble}}} P_{G/N_{j-1},N_j/N_{j-1}}(d(G)+u) \\ &\geq (1-\eta^{u/v-1})^s \geq 1 - s\eta^{u/v-1}. \end{aligned}$$ ∎

3. The main result

To prove Theorem 1 and Theorem 2 we will apply Corollary 11 and Lemma 16. The bound for $\mathcal{B}_G(t)$ given by Lemma 16 depends on the normal series of G which is chosen. For our aim it is useful to consider the normal series of G described in the following lemma.

Proposition 17: *Let G be a finite group. We define recursively the normal series*

$$1 = Y_0 \leq X_1 < Y_1 \leq X_2 < Y_2 \leq \cdots \leq X_s < Y_s \leq X_{s+1} = G$$

by setting $Y_0 = 1$ and

$$\begin{aligned} X_i/Y_{i-1} &= R(G/Y_{i-1}) \quad \text{(soluble radical of } G/Y_{i-1}) \\ Y_i/X_i &= \operatorname{soc}(G/X_i) \quad \text{(socle of } G/X_i). \end{aligned}$$

Then, Y_i/X_i is a direct product of l_i nonabelian simple groups, where

$$l_{i+1} \leq l_i/2$$

for $i = 1, \ldots, s-1$. In particular $l_1 \geq l_i$, for every i, and

$$s \leq \log l_1 + 1.$$

Proof: As the series is defined recursively, it is sufficient to prove that $l_2 \leq l_1/2$. By definition, X_1 is the soluble radical of G, so that $\overline{Y} = Y_1/X_1$ is a direct product of l_1 nonabelian simple groups, say $\overline{S}_1, \ldots, \overline{S}_{l_1}$.

Now, $\overline{G} = G/X_1$ acts by conjugation on the l_1 subgroups $\overline{S}_i$ and the kernel of this action is $\overline{N} = N/X_1 = \bigcap_{i=1}^{l_1} N_{\overline{G}}(\overline{S}_i)$. Thus, G/N is isomorphic to a subgroup of $\mathrm{Sym}(l_1)$.

Moreover, $\overline{N}$ acts by conjugation on the elements of $\overline{Y}_1$, fixing every subgroup $\overline{S}_i$. As $\overline{Y}_1 = \mathrm{soc}(\overline{G})$ and $Z(\overline{Y}_1) = 1$, it follows that $\overline{N}$ is isomorphic to a subgroup of $\prod_{i=1}^{l_1} \mathrm{Aut}(\overline{S}_i)$. In particular, N/Y_1 is isomorphic to a subgroup of $\prod_{i=1}^{l_1} \mathrm{Out}(\overline{S_i})$ and thus it is soluble, since each $\overline{S}_i$ is a nonabelian simple group. By the definition of X_2 it follows that $N \leq X_2$, so that Y_2/X_2 is isomorphic to a section of G/N and hence to a section, say Y/X, of $\mathrm{Sym}(l_1)$. As $Y/X \simeq Y_2/X_2 = \mathrm{soc}(G/X_2)$, we can write Y/X as a direct product of l_2 nonabelian simple groups, say

$$Y/X = S_1/X \times \cdots \times S_{l_2}/X.$$

Let P be a Sylow 2-subgroup of $Y \leq \mathrm{Sym}(l_1)$. Since $d(P) \leq l_1$, $|P_{ab}| = |P/P'| \leq 2^{l_1}$. Thus

$$|(PX/X)_{ab}| = |PX/P'X| = |P/P'(P \cap X)| \leq |P/P'| \leq 2^{l_1}.$$

On the other hand, PX/X is a direct product of some Sylow 2-subgroups P_i/X of S_i/X, for $i = 1, \ldots, l_2$. Since nonabelian simple groups have noncyclic Sylow 2-subgroups, we get $|(P_i/X)_{ab}| \geq 2^2$. Therefore,

$$|(PX/X)_{ab}| = \prod_{i=1}^{l_2} |(P_i/X)_{ab}| \geq 2^{2l_2},$$

so that $2^{2l_2} \leq 2^{l_1}$, and we conclude that $l_2 \leq l_1/2$. ∎

Now we can give the proof of Theorem 2.

Proof of Theorem 2: Let $\eta = 1 - 1/e$ and let δ be the constant defined in Theorem 14. We set $\alpha = -\log \eta > 0$ and define

$$c = (\delta + 1)/\alpha > 0.$$

Let f be a function such that

$$\lim_{x \to \infty} \frac{f(x)}{\log x} - c \log \log x = \infty.$$

Since, by definition, $P_G(u) = \mathcal{A}_G(u) \cdot \mathcal{B}_G(u)$ for every integer u, it is sufficient to prove that

$$\text{(a)} \qquad \lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \lambda(G)\le x}} \mathcal{A}_G([d(G)+f(x)]) = 1$$

and

$$\text{(b)} \qquad \lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \lambda(G)\le x}} \mathcal{B}_G([d(G)+f(x)]) = 1.$$

(a) By Corollary 11,

$$\mathcal{A}_G([d(G)+f(x)]) \ge 1 - \xi/2^{f(x)},$$

where ξ denotes the number, up to isomorphism, of the irreducible G-modules isomorphic to a complemented factor in a principal series of G. As $\xi \le \lambda(G) \le x$ we get that

$$\inf_{\substack{G \text{ s.t.} \\ \lambda(G)\le x}} \mathcal{A}_G([d(G)+f(x)]) \ge 1 - \frac{x}{2^{f(x)}} = 1 - 2^{-(f(x)-\log x)}.$$

Now,

$$\begin{aligned} \lim_{x\to\infty} f(x) - \log x &= \lim_{x\to\infty} \log x\left(\frac{f(x)}{\log x} - 1\right) \\ &\ge \lim_{x\to\infty} \log x\left(\frac{f(x)}{\log x} - c\log\log x - 1\right) = \infty, \end{aligned}$$

and therefore

$$\lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \lambda(G)\le x}} \mathcal{A}_G([d(G)+f(x)]) = 1 - 2^{-\infty} = 1.$$

(b) Clearly, $\lim_{x\to\infty} f(x)/\log x = \infty$, so there exists a real number $\overline{x}$ such that $[f(x)] \ge (\delta+1)\log x$ for every $x \ge \overline{x}$.

Let us fix an integer $x \ge \overline{x}$ and a group G such that $\lambda(G) \le x$. We consider the series of G defined in Proposition 17. This series has s nonsoluble factors, and each of them is a direct product of at most l_1 nonabelian simple groups. Clearly, $l_1 \le \lambda(G) \le x$. Moreover, by Proposition 17, $s \le \log\lambda(G) + 1 \le \log x + 1$.

Now, let $v = [\delta \max\{\log l_1, 1\}] + 1$. As $l_1 \le x$ and we can assume $\log x \ge 1$,

$$v \le [\delta \max\{\log x, 1\}] + 1 \le \delta \log x + 1 \le (\delta+1)\log x.$$

In particular, since $x \ge \overline{x}$, we have $[f(x)] \ge v$ and, by Lemma 16, it follows that

$$\mathcal{B}_G([d(G)+f(x)]) \ge 1 - s\eta^{[f(x)]/v-1}.$$

Note that, since $v \leq (\delta+1)\log x$,

$$\frac{[f(x)]}{v} \geq \frac{[f(x)]}{(\delta+1)\log x} \geq \frac{f(x)-1}{(\delta+1)\log x} \geq \frac{f(x)}{(\delta+1)\log x} - 1$$

so that

$$\eta^{[f(x)]/v-1} \leq \eta^{f(x)/(\delta+1)\log x - 2}.$$

Thus, for $\alpha = -\log \eta > 0$ and $c = (\delta+1)/\alpha$, since $s \leq \log x + 1$ we get

$$\begin{aligned}
\mathcal{B}_G([d(G)+f(x)]) &\geq 1 - (\log x + 1)\ \eta^{\frac{f(x)}{(\delta+1)\log x} - 2} \\
&= 1 - \eta^{-2}(\log x + 1)\ 2^{-\alpha(\frac{f(x)}{(\delta+1)\log x})} \\
&= 1 - \eta^{-2}(2^{\log\log x} + 1)\ 2^{-\frac{1}{c}\frac{f(x)}{\log x}} \\
&= 1 - \eta^{-2}(2^{-\frac{1}{c}(\frac{f(x)}{\log x} - c\log\log x)} + 2^{-\frac{1}{c}\frac{f(x)}{\log x}}).
\end{aligned}$$

Since this holds for every real number $x \geq \overline{x}$ and for every group G such that $\lambda(G) \leq x$, we conclude that

$$\begin{aligned}
\lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \lambda(G)\leq x}} \mathcal{B}_G(d(G)+f(x)) &\geq \lim_{x\to\infty} 1 - \eta^{-2}(2^{-\frac{1}{c}(\frac{f(x)}{\log x} - c\log\log x)} + 2^{-\frac{1}{c}\frac{f(x)}{\log x}}) \\
&= 1 - \eta^{-2}(2^{-\infty} + 2^{-\infty}) = 1. \qquad \blacksquare
\end{aligned}$$

Theorem 1 is a consequence of Theorem 2.

Proof of Theorem 1: Let c be the constant defined in Theorem 2 and let $g(x)$ be the function defined as $g(x) = \log x \log\log x$ if $x \geq 4$, $g(x) = 1$ otherwise. Since

$$\lim_{x\to\infty} \frac{(c+1)g(x)}{\log x} - c\log\log x = \lim_{x\to\infty} \log\log x = \infty,$$

Theorem 2 implies that

$$\lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \lambda(G)\leq x}} P_G([d(G)+(c+1)g(x)]) = 1.$$

Thus there exists a positive number x_α such that

$$\inf_{\substack{G \text{ s.t.} \\ \lambda(G)\leq x}} P_G([d(G)+(c+1)g(x)]) \geq \alpha, \quad \text{for every } x \geq x_\alpha.$$

In particular, for any group G such that $\lambda(G) \geq x_\alpha$ we have

$$P_G([d(G)+(c+1)g(\lambda(G))]) \geq \alpha,$$

and also for any group G such that $\lambda(G) \leq x_\alpha$ we have

$$P_G([d(G) + (c+1)g(x_\alpha)]) \geq \alpha.$$

Therefore, for $c_\alpha = (c+1)g(x_\alpha)$ we obtain that

$$P_G([d(G) + c_\alpha g(\lambda(G))]) \geq \begin{cases} P_G([d(G) + (c+1)g(\lambda(G))]) \geq \alpha & \text{if } \lambda(G) \geq x_\alpha, \\ P_G([d(G) + (c+1)g(x_\alpha)]) \geq \alpha & \text{if } \lambda(G) \leq x_\alpha, \end{cases}$$

since g and P_G are nondecreasing functions. ∎

COROLLARY 18: *There is a constant k such that*

(1) $\lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \log|G| \leq x}} P_G([d(G) + k \log x \log\log x]) = 1$,

(2) $\lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ |G| = x}} P_G([d(G) + k \log\log|G| \log\log\log|G|]) = 1$.

Proof: (1) Let c be the constant defined in Theorem 2. We set $k = c+1$ and $f(x) = k \log x \log\log x$. Since $\lambda(G) \leq \log|G|$, clearly

$$\{G \mid \log|G| \leq x\} \subseteq \{G \mid \lambda(G) \leq x\}.$$

Thus

$$\inf_{\substack{G \text{ s.t.} \\ \log|G| \leq x}} P_G([d(G) + f(x)]) \geq \inf_{\substack{G \text{ s.t.} \\ \lambda(G) < x}} P_G([d(G) + f(x)]),$$

and hence by Theorem 2 we conclude that

$$\lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \log|G| \leq x}} P_G([d(G) + f(x)]) \geq \lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \lambda(G) \leq x}} P_G([d(G) + f(x)]) = 1.$$

(2) Since $\{G \mid \log|G| = x\} \subseteq \{G \mid \log|G| \leq x\}$, we have

$$\begin{aligned} \lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ |G| = x}} P_G([d(G) + f(\log|G|)]) &= \lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \log|G| = x}} P_G([d(G) + f(x)]) \\ &\geq \lim_{x\to\infty} \inf_{\substack{G \text{ s.t.} \\ \log|G| \leq x}} P_G([d(G) + f(x)]) = 1. \end{aligned}$$ ∎

PROPOSITION 19: *Let $h(x)$ be a function defined as $h(x) = \log\log x \cdot \log\log\log x$ if $x \geq 16$, $h(x) = 1$ otherwise. For any real number $0 < \alpha < 1$, there exists a constant θ_α such that $P_G([d(G) + \theta_\alpha h(|G|)]) \geq \alpha$ for any finite group G.*

Proof: This follows the same lines as the proof of Theorem 1, applying Corollary 18 instead of Theorem 2. ∎

4. Permutation and linear groups

If G is a permutation or a linear group, we are able to bound $d_\alpha(G)$ with a function depending on the degree of G.

If G is a permutation group of degree n, then the length of a maximal chain in the subgroup lattice of G is at most $3n/2$ (see [2]) and this of course implies $\lambda(G) \leq 3n/2$; so from Theorem 2, one can immediately deduce the following corollary.

COROLLARY 20: *There is a constant c_1 such that, if $g(x) \to \infty$ as $x \to \infty$ and $f(x) = \log x(c_1 \log\log x + g(x))$, then*

$$\lim_{n\to\infty} \inf_{G\leq \mathrm{Sym}(n)} P_G([d(G) + f(n)]) = 1.$$

Also in this case, the previous result does not remain true if we replace $\log x(c_1 \log\log x + g(x))$ by any function $f(x)$ which tends to infinity as x tends to infinity. As we noticed in the introduction, if n is large enough, $G_n = (\mathrm{Alt}(n))^{n!/8}$ can be generated by 2 elements and can be viewed as a permutation group of degree $n \cdot n!/8$, but $\lim_{n\to\infty} P_{G_n}([2+\sqrt{n}]) = 0$ [5].

If $G \leq \mathrm{Sym}(n)$ and $n \neq 3$, then $d(G) \leq n/2$ (see [2]); so if β is a real number with $\beta > 1/2$, then

$$\lim_{n\to\infty} \frac{\beta n - d(G)}{\log n} - c_1 \log\log n = \infty.$$

Therefore we have the following result.

COROLLARY 21: *If $\beta > 1/2$ then*

$$\lim_{n\to\infty} \inf_{G\leq \mathrm{Sym}(n)} P_G([\beta n]) = 1.$$

Similar arguments can be applied for completely reducible linear groups. Namely, if F is a field which has finite degree over its prime subfield and G is a finite completely reducible subgroup of $\mathrm{GL}(n, F)$, then $\lambda(G) \leq c_F n$ for a constant c_F ([7] Theorem C) and $d(G) \leq 3n/2$ (see [6]). So we have the following corollaries.

COROLLARY 22: *Let F be a field which has finite degree over its prime subfield and let $\mathcal{X}_n$ be the set of the finite completely reducible subgroups of $\mathrm{GL}(n, F)$. There is a constant c_2 such that, if $g(x) \to \infty$ as $x \to \infty$ and $f(x) = \log x(c_2 \log\log x + g(x))$, then*

$$\lim_{n\to\infty} \inf_{G\in\mathcal{X}_n} P_G([d(G) + f(n)]) = 1.$$

COROLLARY 23: *Let F be a field which has finite degree over its prime subfield and let $\mathcal{X}_n$ be the set of the finite completely reducible subgroups of* $\mathrm{GL}(n, F)$. *If $\beta > 3/2$ then*

$$\lim_{n\to\infty} \inf_{G\in\mathcal{X}_n} P_G([\beta n]) = 1.$$

References

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

[2] P. J. Cameron, R. Solomon and A. Turull, *Chains of subgroups in symmetric groups*, Journal of Algebra **127** (1989), 340–352.

[3] W. Gaschütz, *Zu einem von B.H. und H. Neumann gestellten Problem*, Mathematische Nachrichten **14** (1955), 249–252.

[4] W. Gaschütz, *Die Eulersche Funktion endlicher auflösbarer Gruppen*, Illinois Journal of Mathematics **3** (1959), 469–476.

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

[6] L.G. Kovács and G.R. Robinson, *Generating finite completely reducible linear groups*, Proceedings of the American Mathematical Society **112** (1991), 357–364.

[7] A. Lucchini, F. Menegazzo and M. Morigi, *On the number of generators and composition length of finite linear groups*, Journal of Algebra **243** (2001), 427–447.

[8] I. Pak, *On the probability of generating a finite group*, Preprint, 2000.