J. Group Theory **14** (2011), 261–271
DOI 10.1515/JGT.2010.050

Journal of Group Theory

On profinite groups with polynomially bounded Möbius numbers

Andrea Lucchini

(Communicated by N. Boston)

1 Introduction

Let G be a finitely generated profinite group. We may define the Möbius function $\mu(H, G)$ in the lattice of the open subgroups of G by the following rules: $\mu(G, G) = 1$ and $\sum_{K \geqslant H} \mu(K, G) = 0$ if $H < G$. In [8] we started the study of the following question, proposed by Mann (see [11] and [12]): what are the groups in which $|\mu(H, G)|$ is bounded by a polynomial function in the index of H and in which the number $b_n(G)$ of subgroups H of index n satisfying $\mu(H, G) \neq 0$ grows at most polynomially in n? In this paper we will say that a profinite group G has *polynomially bounded Möbius numbers* (PBMN) if G satisfies these two properties.

The interest of this question comes from its relation to the study of the function $P(G, k)$ expressing the probability that k randomly chosen elements generate G topologically. Indeed the groups G with PBMN are precisely those for which the infinite sum

$$\sum_{H <_o G} \frac{\mu(H, G)}{|G : H|^s}$$

is absolutely convergent in some complex half-plane. When this happens, this infinite sum represents in the domain of convergence an analytic function which assumes precisely the value $P(G, k)$ at any sufficiently large positive integer k (see [12] for more details).

Since $\mu(M, G) = -1$ for any maximal subgroup M of G, we have $m_n(G) \leqslant b_n(G)$ (where $m_n(G)$ denotes the number of maximal subgroups of G with index n). In particular, if $b_n(G)$ grows polynomially, then G has polynomial maximal subgroup growth (PMSG). A theorem of Mann and Shalev [13] characterizes groups with PMSG as those which are positively finitely generated (PFG), i.e. $P(G, k) > 0$ for some choice of k. Mann conjectured that, conversely, the following holds:

Conjecture 1. If G is a PFG group, then G has PBMN.

The conjecture has been proved for particular classes of profinite groups, for example some arithmetic groups [12], finitely generated prosolvable groups [7], groups with polynomial subgroup growth [9]. In [8] we proved that in order to decide whether a finitely generated profinite group G has PBMN, it suffices to investigate the behavior of the Möbius function of the subgroup lattice of the finite monolithic groups that appear as epimorphic images of G. We need some definitions to be more precise. Let L be a finite monolithic group (i.e. a group with a unique minimal normal subgroup): we will say that L is (η_1, η_2)-*bounded* if there exist two constants η_1 and η_2 such that

(1) $b_n^*(L) \leqslant n^{\eta_1}$, where $b_n^*(L)$ denotes the number of subgroups K of L with $|L : K| = n$ and $L = K \operatorname{soc} L$;

(2) $|\mu(K, L)| \leqslant |L : K|^{\eta_2}$ for each $K \leqslant L$ with $L = K \operatorname{soc} L$.

In [8] the following is proved. Denote by $\Lambda(G)$ the set of finite monolithic groups L such that $\operatorname{soc} L$ is non-abelian and L is an epimorphic image of G. A PFG group G has PBMN if and only if there exist η_1 and η_2 such that each $L \in \Lambda(G)$ is (η_1, η_2)-bounded. In this paper we obtain a stronger reduction theorem, which requires us to deal only with almost simple groups. If L is a finite monolithic group with non-abelian socle, then $\operatorname{soc} L = S_1 \times \cdots \times S_r$, where the groups S_i are isomorphic simple groups. Let X_L be the subgroup of $\operatorname{Aut} S_1$ induced by the conjugation action of $N_G(S_1)$ on S_1. This X_L is a finite almost simple group, uniquely determined by L. Our main result is the following.

Theorem 1. *Let L be a monolithic group with non-abelian socle. If the associated almost simple group X_L is (c_1, c_2)-bounded, then L is (η_1, η_2)-bounded with $\eta_1 = 10 + 2(1 + c_1 + c_2)/r$ and $\eta_2 = 2c_2 + 8$.*

Combined with [8, Theorem 1], this implies

Corollary 2. *A PFG group has PBMN if there exist c_1 and c_2 such that X_L is (c_1, c_2)-bounded for each L in $\Lambda(G)$.*

This theorem allows us to reformulate Mann's conjecture as follows.

Conjecture 2. There exist c_1 and c_2 such that any finite almost simple group is (c_1, c_2)-bounded.

Recently, in collaboration with Valentina Colombo, we have proved that this conjecture is satisfied by the symmetric and alternating groups [3]. This implies

Corollary 3. *If G is a PFG group and, for each open normal subgroup N of G, all composition factors of G/N are either abelian or alternating groups, then G has PBMN.*

2 Monolithic groups

Let P be a finite poset. The Möbius function $\mu_P : P \times P \to \mathbb{Z}$ is defined as follows: $\mu_P(x, y) = 0$ unless $x \leqslant y$, when it is defined recursively by the equations

$$\mu_P(y, y) = 1 \quad \text{and} \quad \sum_{x \leqslant z \leqslant y} \mu_P(z, y) = 0 \quad \text{when } x < y.$$

The following is well known:

Lemma 4. *If $x \leqslant y$ then $\mu_P(x, y)$ is equal to the difference between the number of chains from x to y of even length, and the number of such chains of odd length.*

Two well-known results will play a relevant role in our discussion. One is the Möbius inversion formula. Suppose that $f, g : P \to \mathbb{Z}$ are functions such that $g(x) = \sum_{y \leqslant x} f(y)$ for all $x \in P$. Then

$$f(y) = \sum_{x \leqslant y} \mu_P(x, y) g(x) \quad \text{for all } y \in P.$$

The other is Crapo's closure theorem. A *closure map* on P is a function $^{-} : P \to P$ satisfying the following three conditions:

(a) $x \leqslant \bar{x}$ for all $x \in P$;

(b) if $x, y \in P$ with $x \leqslant y$, then $\bar{x} \leqslant \bar{y}$;

(c) $\bar{\bar{x}} = \bar{x}$ for all $x \in P$.

If $^{-}$ is a closure map on P, then $\bar{P} = \{x \in P \mid \bar{x} = x\}$ is a poset with order induced by the order on P.

Theorem 5 (Crapo's closure theorem [4]). *Let P be a finite poset and let $^{-} : P \to P$ be a closure map. Fix $x, y \in P$ such that $y \in \bar{P}$. Then*

$$\sum_{\bar{z} = y} \mu_P(x, z) = \begin{cases} \mu_{\bar{P}}(x, y) & \textit{if } x = \bar{x}, \\ 0 & \textit{otherwise}. \end{cases}$$

Denote by $\mathscr{L}(G)$ the subgroup lattice of a finite group; notice that if $H \leqslant K \leqslant G$ then $\mu_{\mathscr{L}(G)}(H, K) = \mu_{\mathscr{L}(H,K)}(H, K)$, where $\mathscr{L}(H, K)$ is the set of subgroups of K containing H. From now on, for simplicity we will write $\mu(H, K)$ instead of $\mu_{\mathscr{L}(H,K)}(H, K)$ whenever H is a subgroup of K.

Now let G be a monolithic finite group, i.e. a finite group G such that $N = \operatorname{soc} G$ is a minimal normal subgroup, and assume that N is non-abelian; so there exists a finite non-abelian simple group S such that $N = S_1 \times \cdots \times S_r$, with $S_i \cong S$ for $i = 1, \ldots, r$. Let ψ be the map from $N_G(S_1)$ to $\operatorname{Aut} S$ induced by the conjugacy action on S_1. Set

$X = \psi(N_G(S_1))$ and note that X is an almost simple group with socle $\mathrm{Inn}\, S = \psi(S_1)$. Let $T := \{t_1, \dots, t_r\}$ be a right transversal of $N_G(S_1)$ in G. The map

$$\phi_T : G \to X \wr \mathrm{Sym}(r)$$

given by

$$g \mapsto (\psi(t_1 g t_{1\pi}^{-1}), \dots, \psi(t_r g t_{r\pi}^{-1}))\pi,$$

where $\pi \in \mathrm{Sym}(r)$ satisfies $t_i g t_{i\pi}^{-1} \in N_G(S_1)$ for all $i \in \{1, \dots, r\}$, is an injective homomorphism. We will identify G with its image in $X \wr \mathrm{Sym}(r)$; in this identification, N is contained in the base subgroup X^r and S_i is a subgroup of the ith component of X^r. We will denote by $\pi_i : N \to S_i$ the projection to the ith factor.

Now define $\mathcal{B} = \{B \leqslant G \mid BN = G\}$. It is a poset, with order induced by inclusion.

Lemma 6. *For each $B \in \mathcal{B}$, there exists one and only one subgroup C satisfying*

(1) $B \leqslant C$;

(2) $C \cap N = (C \cap S_1) \times \cdots \times (C \cap S_r)$;

(3) $\psi(C \cap S_1) = \psi(N_B(S_1)) \cap \mathrm{Inn}\, S$.

Proof. Since $BN = G$, for each $i \in \{2, \dots, r\}$ there exists $b_i \in B$ with $S_i = S_1^{b_i}$. If $C \cap N = (C \cap S_1) \times \cdots \times (C \cap S_r)$ and $B \leqslant C$, then

$$\begin{aligned} C &= B(C \cap N) = B((C \cap S_1) \times \cdots \times (C \cap S_r)) \\ &= B((C \cap S_1) \times (C \cap S_1)^{b_2} \times \cdots \times (C \cap S_1)^{b_r}) \end{aligned}$$

is uniquely determined by the knowledge of $C \cap S_1$. If we add the further condition that $\psi(C \cap S_1) = \psi(N_B(S_1)) \cap \mathrm{Inn}\, S$, then we have a unique possible choice for C. Now let $Y = \psi(N_B(S_1))$ and $T = \psi^{-1}(Y \cap \mathrm{Inn}\, S) \cap S_1$. It is easy to see that B normalizes $T \times T^{b_2} \times \cdots \times T^{b_r}$ and that $C = B(T \times T^{b_2} \times \cdots \times T^{b_r})$ is the required subgroup. $\square$

For any $B \in \mathcal{B}$, we will denote by $\bar{B}$ (the *G-closure of B*) the subgroup C described by the previous lemma. Moreover, if $B_1, B_2 \in \mathcal{B}$ we will say that B_1 *is G-closed in* B_2 if $B_1 = B_2 \cap \bar{B}_1$. Suppose that $B \in \mathcal{B}$, let $Y = \psi(N_B(S_1))$ (notice that $BN = G$ implies $Y\, \mathrm{Inn}\, S = X$) and let $T = \{t_1, \dots, t_r\}$ be a right transversal of $N_B(S_1)$ in B. As $BN = G$ and $N \leqslant N_G(S_1)$, we have that $N_G(S_1) = N_B(S_1)N$ and T is also a right transversal of $N_G(S_1)$ in G. If we use precisely this transversal T in order to define our embedding $\phi_T : G \to X \wr \mathrm{Sym}(r)$, then we obtain $\phi_T(B) \leqslant Y \wr \mathrm{Sym}(r)$ and $\bar{B} = \phi_T^{-1}(Y \wr \mathrm{Sym}(r))$.

Lemma 7. *Let $B_1, B_2 \in \mathcal{B}$ with $\bar{B}_1 = B_1$, $\bar{B}_2 = B_2$ and $\psi(N_{B_1}(S_1)) = \psi(N_{B_2}(S_1))$. Then $B_2 = B_1^x$ for some $x \in E = S_2 \times \cdots \times S_r$.*

Proof. We claim that if $\psi(N_{B_1}(S_1)) = \psi(N_{B_2}(S_1)) = Y$, then $N_{B_1}(S_1)E \leqslant N_{B_2}(S_1)E$. Indeed let $g \in N_{B_1}(S)E$. Since $B_1N = B_2N$, we have also $N_{B_1}(S_1)N = N_{B_2}(S_1)N$, so there exists $s \in S_1$ such that $gs \in N_{B_2}(S_1)E$. Moreover

$$\psi(g) \in \psi(N_{B_1}(S_1)) = Y \quad \text{and} \quad \psi(gs) \in \psi(N_{B_2}(S_1)) = Y,$$

hence $\psi(s) \in Y \cap \operatorname{Inn} S$. As $B_2 = \bar{B}_2$, we must have $s \in \psi^{-1}(Y \cap \operatorname{Inn} S) \cap S_1 = S_1 \cap B_2$. Hence $g \in N_{B_2}(S)E$. By the same argument, $N_{B_2}(S_1)E \leqslant N_{B_1}(S_1)E$. This means that $N_{B_1}(S_1)E = N_{B_2}(S_1)E$ is a supplement of N/E in $N_G(S_1)/E$. By [2, Theorem 1.1.35], B_1 and B_2 are E-conjugate. □

Lemma 8. *Suppose that $B \in \mathscr{B}$ with $\bar{B} = B$ and $\psi(N_B(S_1)) = Y$. Then*

(1) $|G : B| = |X : Y|^r$, *and*

(2) $|E : N_E(B)| = |X : Y|^{r-1}$, *where* $E = S_2 \times \cdots \times S_r$.

Proof. As we noticed before, we may assume that

$$G \leqslant X \wr \operatorname{Sym}(r) \quad \text{and} \quad B = \bar{B} = (Y \wr \operatorname{Sym}(r)) \cap G.$$

Moreover, $G = BN$ implies $X = Y \operatorname{Inn} S$ and consequently

$$\begin{aligned} |G : B| &= |N : B \cap N| = |(\operatorname{Inn} S)^r : (Y \cap \operatorname{Inn} S)^r| \\ &= |\operatorname{Inn} S : (Y \cap \operatorname{Inn} S)|^r = |Y \operatorname{Inn} S : Y|^r = |X : Y|^r. \end{aligned}$$

If $k = (s_1, s_2, \ldots, s_r) \in E$ (hence $s_1 = 1$) and $b = (y_1, \ldots, y_r)\alpha \in B$, then

$$\pi_1([k, b^{-1}]) = y_1 s_{1\alpha} y_1^{-1} \in Y, \quad \text{hence } s_{1\alpha} \in Y \cap \operatorname{Inn} S.$$

Since $BN = G$, for each $i \in \{1, \ldots, r\}$ there exists $(y_1, \ldots, y_r)\alpha \in B$ with $1\alpha = i$, hence

$$\begin{gathered} N_E(B) = (\operatorname{Inn} S \cap Y)^{r-1} \quad \text{and} \\ |E : N_E(B)| = |\operatorname{Inn} S : (\operatorname{Inn} S \cap Y)|^{r-1} = |X : Y|^{r-1}. \quad \square \end{gathered}$$

If $K \in \mathscr{B}$, then $\mathscr{L}(K) \cap \mathscr{B}$ is a poset, with order induced by $\mathscr{L}(K)$, and the position $R \to \bar{R} \cap K$ defines a closure map in this poset. Moreover let

$$\mathscr{C}(K) = \{R \in \mathscr{B} \mid R \leqslant K \text{ and } R = \bar{R} \cap K\}$$

be the poset consisting of the subgroups of K that are G-closed in K. Finally, if $H \leqslant K$ and $H \in \mathscr{B}$, let

$$\mathscr{S}(H, K) = \{R \in \mathscr{B} \mid H \leqslant R \leqslant K \text{ and } \bar{R} \cap K = K\}.$$

Now let $H \in \mathscr{B}$. We define functions $f, g : \mathscr{B} \times \mathscr{B} \to \mathbb{Z}$ in the following way:

$$f(H,R) = \begin{cases} \mu(H,R) & \text{if } R \in \mathscr{S}(H,G), \\ 0 & \text{otherwise,} \end{cases}$$

$$g(H,R) = \begin{cases} \mu_{\mathscr{C}(R)}(H,R) & \text{if } R \in \mathscr{S}(H,G) \text{ and } H \text{ is } G\text{-closed in } R, \\ 0 & \text{otherwise.} \end{cases}$$

For $H \leqslant K \leqslant G$, let $\mathscr{L}(H,K)$ be the set of subgroups of K containing H. Notice that if $H \in \mathscr{B}$ and $K \in \mathscr{S}(H,G)$, then $\mathscr{S}(H,K) = \mathscr{S}(H,G) \cap \mathscr{L}(H,K)$. Indeed if $\bar{R} = G$ then $\bar{R} \cap K = K$; conversely if $\bar{R} \cap K = K$ then $K \leqslant \bar{R}$, hence $\bar{K} \leqslant \bar{\bar{R}} = \bar{R}$, but we are assuming $\bar{K} = G$, so we must have $\bar{R} = G$. But then, for $K \in \mathscr{S}(H,G)$, applying Crapo's closure theorem to the lattice $\mathscr{L}(H,K)$, we obtain

$$\sum_{R \in \mathscr{S}(H,K)} \mu(H,R) = \sum_{R \in \mathscr{S}(H,G) \cap \mathscr{L}(H,K)} \mu(H,R)$$
$$= \begin{cases} \mu_{\mathscr{C}(K)}(H,K) & \text{if } H \text{ is } G\text{-closed in } K, \\ 0 & \text{otherwise.} \end{cases}$$

This means that f and g satisfy the relation

$$g(H,K) = \sum_{R \leqslant K,\, R \in \mathscr{S}(H,G)} f(H,R)$$

and, by the Möbius inversion formula, for any $R \in \mathscr{S}(H,G)$ we have

$$f(H,R) = \sum_{K \leqslant R,\, K \in \mathscr{S}(H,G)} \mu(K,R) g(H,K).$$

Setting $R = G$, we get

Lemma 9. *If $H \in \mathscr{B}$, then*

$$\mu(H,G) = \sum_{K \in \mathscr{S}(H,G)} \mu(K,G) g(H,K).$$

In particular, $|\mu(H,G)| \leqslant \sum_{K \in \mathscr{S}(H,G)} |\mu(K,G)| \cdot |g(H,K)|$.

Lemma 10. *Let* $\mathscr{S} = \{K \in \mathscr{B} \mid \bar{K} = G\}$.

(1) $|\mathscr{S}| \leqslant 2|N|^2$.

(2) $|\mu(K,G)| \leqslant |N|^{5/2}$ *for each* $K \in \mathscr{S}$.

AUTHOR'S COPY | AUTORENEXEMPLAR

Proof. If $K \in \mathcal{S}$ then $\operatorname{Inn} S \leqslant \psi(N_K(S_1))$. Moreover $\psi(K \cap N)$ is normalized by $\psi(N_K(S_1))$, so either $\pi_1(K \cap N) = 1$ or $\pi_1(K \cap N) = S_1$. In the first case K is a complement for N in G and by [10] there are at most $|N|^2$ possibilities. In the second case there exists a partition $J_1, \dots, J_u$ of $\{1, \dots, r\}$ such that

$$K \cap N = \Delta_1 \times \cdots \times \Delta_u$$

where Δ_i is a full diagonal subgroup of S^{J_i} (see for example [2, Definition 1.1.37]). We claim that $K = N_G(K \cap N)$. Indeed, as $K \cap N \trianglelefteq K$ and $G = KN$, we have

$$N_G(K \cap N) = KN_N(K \cap N) = KN_N(\Delta_1 \times \cdots \times \Delta_u) = K(\Delta_1 \times \cdots \times \Delta_u) = K.$$

Hence K is uniquely determined by $\Delta = \Delta_1 \times \cdots \times \Delta_u$, and we have to count the possibilities for Δ. Let $\rho : G \to \operatorname{Sym}(r)$ be the homomorphism which maps g to the permutation of the set $\{S_1, \dots, S_r\}$ induced by conjugation by g and let $P = \rho(G)$. The subsets $J_1, \dots, J_u$ are the blocks of an imprimitivity system for P, so they are uniquely determined by the knowledge of J_1 and can be chosen in at most 2^r different ways. Moreover for any $J \subseteq \{1, \dots, r\}$, S^J contains precisely $|\operatorname{Aut} S|^{|J|-1}$ full diagonal subgroups. We conclude that the possibilities for Δ are at most $2^r |\operatorname{Aut} S|^{r-1} \leqslant |S|^{2r} \leqslant |N|^2$, since $4|\operatorname{Out} S| \leqslant |S|$ (see for example [1, Lemma 2.7]). Hence $|\mathcal{S}| \leqslant 2|N|^2$. This concludes the proof of (1).

Now we want to estimate $|\mu(K, G)|$ for a given $K \in \mathcal{S}$. First assume that $K \cap N \neq 1$. As before, there exists a partition $J_1, \dots, J_u$ of $\{1, \dots, r\}$ such that $K \cap N = \Delta_1 \times \cdots \times \Delta_u$ where Δ_i is a full diagonal subgroup of S^{J_i}. In order to estimate $\mu(K, G)$ we need more information on the set $\mathcal{L}(K, G)$ of subgroups of G containing K. If $U \in \mathcal{L}(K, G)$, then $U = KN \cap U = K(U \cap N)$; moreover there exists a partition $J_1^*, \dots, J_v^*$ of $\{1, \dots, r\}$ which refines $J_1, \dots, J_u$ such that $U \cap N = \Delta_1^* \times \cdots \times \Delta_v^*$ where Δ_i^* is a full diagonal subgroup of $S^{J_i^*}$. We may assume that $1 \in J_1^* \subseteq J_1$. We claim that U is uniquely determined by the knowledge of J_1^*. Since $KN = G$, we have $P = \rho(G) = \rho(K)$, so for each $i \in \{2, \dots, v\}$ there exists $x_i \in K$ such that $J_i^* = (J_1^*)^{\rho(x_i)}$. On the other hand, $U \cap N = \Delta_1^* \times \cdots \times \Delta_v^*$ is normalized by K, hence $\Delta_i^* = (\Delta_1^*)^{x_i}$ is uniquely determined by Δ_1^* for each $i \in \{2, \dots, v\}$. The full diagonal subgroup Δ_1 of S^{J_1} is uniquely identified by a family $\{\alpha_i\}_{i \in J_1, i \neq 1}$ of elements of $\operatorname{Aut} S$ (if $x \in S^{J_1}$, then $x \in \Delta_1$ if and only if $\pi_i(x) = \pi_1(x)^{\alpha_i}$). Similarly Δ_1^* is uniquely identified by a family $\{\beta_i\}_{i \in J_1^*, i \neq 1}$ of elements of $\operatorname{Aut} S$. As $\Delta_1 \leqslant K \cap N \leqslant U \cap N = \Delta_1^* \times \cdots \times \Delta_v^*$ and $J_1^* \subseteq J_1$, we must have $\beta_i = \alpha_i$ for each $i \in J_1^* \backslash \{1\}$. This completes the proof of our claim. By Lemma 4, $|\mu(K, G)|$ is bounded by the number of chains in $\mathcal{L}(G)$ connecting U to G. From what we have just seen, any of these chains is uniquely determined by a chain $\Omega_1 = J_1 \supset \Omega_2 \supset \cdots \supset \Omega_l = \{1\}$ of subsets of J_1, with $|\Omega_i|$ divisible by $|\Omega_{i+1}|$ for each $i \in \{1, \dots, l-1\}$. We claim that the number of these chains is at most $4^{|J_1|}$. Indeed we may choose $|\Omega_2|$ in at most $2^{|J_1|}$ different ways, and when Ω_2 has been chosen, by induction we have at most $4^{|J_2|} \leqslant 4^{|J_1|/2} = 2^{|J_1|}$ possibilities for the chain $\Omega_2 \supset \cdots \supset \Omega_l = \{1\}$. This leads to the conclusion

$$|\mu(K, G)| \leqslant 4^{|J_1|} \leqslant 4^r \leqslant |S|^{r/2} = |N|^{1/2}.$$

Now assume that $K \cap N = 1$. Again $|\mu(K,G)|$ is bounded by the number of chains $K_0 = K < K_1 < \cdots < K_l = G$. Since $K_1 \in \mathscr{S}$ and $K_1 \cap N \neq 1$, as we have seen before there are at most $|N|^2$ possible choices for K_1. For any choice of K_1, by the same argument as above, we have at most $|N|^{1/2}$ possible choices for the chain $K_1 < \cdots < K_l = G$. Hence $|\mu(K,G)| \leqslant |N|^{5/2}$. □

Lemma 11. *Let $H \in \mathscr{B}$ and let $Y = \psi(N_H(S_1))$. There exists a lattice isomorphism β_H from $\mathscr{L}(Y,X)$ to the lattice $\mathscr{C}(H,G)$ of G-closed subgroups of G containing H.*

Proof. Since $HN = G$, for each $i \in \{2,\dots,r\}$ there exists $h_i \in H$ with $S_i = S_1^{h_i}$. If $Z \in \mathscr{L}(Y,X)$, then $T = \psi^{-1}(Z \cap \operatorname{Inn} S) \cap S_1$ is normalized by $N_H(S_1)$; hence H normalizes $T \times T^{h_2} \times \cdots \times T^{h_r}$ and we may define $\beta_H(Z) = H(T \times T^{h_2} \times \cdots \times T^{h_r})$. Since $HN = G$, we must have $X = Y \operatorname{Inn} S$ and this can be used to prove that β_H is injective. Indeed if $\beta_H(Z_1) = \beta_H(Z_2)$, then $Z_1 \cap \operatorname{Inn} S = Z_2 \cap \operatorname{Inn} S$, which implies $Z_1 = Y(Z_1 \cap \operatorname{Inn} S) = Y(Z_2 \cap \operatorname{Inn} S) = Z_2$. It remains to prove that β_H is surjective. If $C \in \mathscr{C}(H,G)$, then $U = C \cap S_1$ is normalized by $N_H(S_1)$ and

$$\begin{aligned} C &= H(C \cap N) = H((C \cap S_1) \times \cdots \times (C \cap S_r)) \\ &= H((C \cap S_1) \times (C \cap S_1)^{h_2} \times \cdots \times (C \cap S_1)^{h_r}) = \beta_H(Z) \end{aligned}$$

with $Z = Y\psi(U)$. □

Now let $H \in \mathscr{B}$ with $Y = \psi(N_H(S_1))$ and let $K \in \mathscr{S}(H,G)$. Consider the poset $\mathscr{C}(H,K)$ of the subgroups that are G-closed in K and contain H. The map

$$\gamma_{H,K} : \mathscr{L}(Y,X) \to \mathscr{C}(H,K), \quad \gamma_{H,K}(Z) = \beta_H(Z) \cap K,$$

is surjective and satisfies

$$\gamma_{H,K}(Z_1 \cap Z_2) = \gamma_{H,K}(Z_1) \cap \gamma_{H,K}(Z_2).$$

For any $Z \in \mathscr{L}(Y,X)$, define

$$\tilde{Z} = \bigcap_{\substack{W \in \mathscr{L}(Y,X) \\ \gamma_{H,K}(W) = \gamma_{H,K}(Z)}} W.$$

Notice that $\tilde{Z}$ is the smallest element of $\mathscr{L}(Y,Z)$ with $\gamma_{H,K}(\tilde{Z}) = \gamma_{H,K}(Z)$. The map $Z \mapsto \tilde{Z}$ is a closure map in the dual poset $\mathscr{L}^*(Y,X)$. We will say that Z is $\gamma_{H,K}$-closed in X if $\tilde{Z} = Z$. The map $\gamma_{H,K}$ induces an order-preserving bijection between the subposet of the $\gamma_{H,K}$-closed subgroups of $\mathscr{L}^*(Y,X)$ and the poset $\mathscr{C}^*(H,K)$. By Crapo's closure theorem,

$$\sum_{\tilde{Z}=Y} \mu_{\mathscr{L}^*(Y,X)}(X,Z) = \mu_{\mathscr{C}^*(H,K)}(K,H).$$

By Lemma 4 if $x, y \in P$ then $\mu_{P^*}(x, y) = \mu_P(y, x)$, so we can conclude that if H is G-closed in K, then

$$\sum_{\tilde{Z}=Y} \mu(Z, X) = \mu_{\mathscr{C}(H,K)}(H, K) = g(H, K). \tag{2.1}$$

Now we are ready to prove Theorem 1. So assume that X is (c_1, c_2)-bounded, i.e. that there exist c_1 and c_2 such that

(1) $|\mu(Y, X)| \leqslant |X : Y|^{c_1}$ for each $Y \leqslant X$ with $X = Y \operatorname{Inn} S$;

(2) $b_n^*(X) \leqslant n^{c_2}$ for each $n \in \mathbb{N}$.

Lemma 12. *If $H \in \mathscr{B}$ and $K \in \mathscr{S}(H, G)$, then $|g(H, K)| \leqslant |S|^{1+c_1+c_2}$.*

Proof. If H is not G-closed in K, then $g(H, K) = 0$. Otherwise, by (2.1),

$$|g(H, K)| = \left| \sum_{Z \in \Omega} \mu(Z, X) \right| \leqslant \sum_{Z \in \Omega} |\mu(Z, X)|$$

where $\Omega = \{Z \leqslant X \mid \tilde{Z} = \psi(N_H(S_1)) \text{ and } \mu(Z, X) \neq 0\}$. Since $Z \operatorname{Inn} S = X$ for each $Z \in \Omega$, we have $|\Omega| \leqslant |S|^{1+c_2}$ and $|\mu(Z, X)| \leqslant |X : Z|^{c_1} \leqslant |S|^{c_1}$ for each $Z \in \Omega$, hence $\sum_{Z \in \Omega} |\mu(Z, X)| \leqslant |\Omega| \, |S|^{c_1} = |S|^{1+c_1+c_2}$. □

Proposition 13. *For each $H \in \mathscr{B}$, we have*

$$|\mu(H, G)| \leqslant |G : H|^{\eta_1} \quad \textit{with } \eta_1 = 10 + 2(1 + c_1 + c_2)/r.$$

Proof. Recall that the maximal subgroups of G not containing N can be classified in terms of their intersection with N as follows:

(a) maximal subgroups R with $\pi_1(R \cap N) = S$;

(b) maximal subgroups R with $1 < \pi_1(R \cap N) < S$;

(c) maximal subgroups R with $R \cap N = 1$.

We may assume that $\mu(H, G) \neq 0$. This implies that H is an intersection of maximal subgroups of G (see for example [5]). We distinguish two possibilities.

Case 1. All maximal subgroups of G containing H are of type (b). In [6] it is proved that in this case $\mu(H, G) = \mu(Y, X)$ with $Y = \psi(N_H(S_1))$ and $|G : H| = |X : Y|^r$; more precisely, it is proved that if H is an intersection of maximal subgroups of G and all the maximal subgroups of G containing H are of type (b), then H is G-closed in G, $\mathscr{S}(H, G) = \{G\}$, $\gamma_{H,G}$ is a lattice isomorphism between $\mathscr{L}(Y, X)$ and $\mathscr{C}(H, G)$ and consequently $\mu(H, G) = g(H, G) = \mu(Y, X)$. It follows

$$|\mu(H, G)| = |\mu(Y, X)| \leqslant |X : Y|^{c_1} = |G : H|^{c_1/r}.$$

Case 2. There exists a maximal subgroup M of G of type (a) or (c) containing H. In this case $|G:H| \geqslant |G:M| = |N:M\cap N| \geqslant |N|^{1/2}$. By Lemma 9

$$\mu(H,G) = \sum_{K\in\mathscr{S}(H,G)} \mu(K,G)g(H,K).$$

By Lemma 10, $|\mathscr{S}(H,G)| \leqslant 2|N|^2$. Moreover by Lemma 10 and Lemma 12, for each $K\in\mathscr{S}(H,G)$ we have $|\mu(K,G)| \leqslant |N|^{5/2}$ and $g(H,K) \leqslant |S|^{1+c_1+c_2}$. Hence

$$|\mu(H,G)| \leqslant 2|N|^{2+(5/2)+(1+c_1+c_2)/r} \leqslant 2|N|^{(9/2)+(1+c_1+c_2)/r} \leqslant |G:H|^{10+2(1+c_1+c_2)/r}.$$

This concludes our proof. □

Lemma 14. *Let* $\mathscr{N} = \{H\in\mathscr{B} \mid \mu(H,G)\neq 0\}$. *Then* $|\mathscr{N}| \leqslant |N|^{\alpha}$ *with* $\alpha = 4+c_2$.

Proof. By Lemma 9, if $H\in\mathscr{N}$, then there exists $K\in\mathscr{S}(H,G)$ with $g(H,K)\neq 0$. In particular, H is G-closed in K and this implies

$$H = \overline{H}\cap K = \beta_H(Y)\cap K = \gamma_{H,K}(Y),$$

with $Y = \psi(N_H(S_1))$. Moreover, by (2.1), there exists Z with $\mu(Z,X)\neq 0$ and $\tilde{Z} = Y$. This means that $T = \beta_H(Z)$ is a G-closed subgroup of G which satisfies

$$\psi(N_T(S_1)) = Z \quad \text{and} \quad T\cap K = \beta_H(Z)\cap K = \gamma_{H,K}(Z) = \gamma_{H,K}(Y) = H.$$

So if $g(H,K)\neq 0$ then $H = K\cap T$ for a subgroup T which is G-closed in G and satisfies $\mu(\psi(N_T(S_1)),X)\neq 0$. There are at most $|S|^{c_2+1}$ possibilities for $Z = \psi(N_T(S_1))$. Given Z, by Lemma 7, there are at most $|S|^{r-1}$ G-closed subgroups T with $\psi(N_T(S_1)) = Z$. So there are at most $|S|^{r-1}|S|^{c_2+1} = |N|\,|S|^{c_2}$ possible choices for T and at most $|\mathscr{S}| = 2|N|^2$ possible choices for K. Hence $|\mathscr{N}| \leqslant 2|N|^3|S|^{c_2} \leqslant |N|^{4+c_2}$. □

Proposition 15. $b_n^*(G) \leqslant n^{\eta_2}$ *with* $\eta_2 = 2c_2+8$.

Proof. First assume that $n < |N|^{1/2}$. As we saw in the proof of Proposition 13, if $H\in\mathscr{B}$, $\mu(H,G)\neq 0$ and $|G:H| = n$, then H is an intersection of maximal subgroups of type (b) and $n = u^r$ with $u = |X:Y|$, where $Y = \psi(N_H(S_1))$. There are $b_u^*(X) \leqslant u^{\eta_2}$ possible choices for Y and, by Lemma 7 and Lemma 8, there are precisely $|X:Y|^{r-1} = u^{r-1}$ possible choices for H with $Y = \psi(N_H(S_1))$. Hence $b_n^*(G) \leqslant b_u^*(X)u^{r-1} \leqslant u^{c_2}u^{r-1} \leqslant n^{c_2+1}$. Now assume that $n \geqslant |N|^{1/2}$. In this case, $b_n^*(G) \leqslant |\mathscr{N}| \leqslant |N|^{4+c_2} \leqslant n^{8+2c_2}$ by Lemma 14. □

References

[1] M. Aschbacher and R. Guralnick. On abelian quotients of primitive groups. *Proc. Amer. Math. Soc.* **107** (1989), 89–95.

[2] A. Ballester-Bolinches and L. M. Ezquerro. *Classes of finite groups* (Springer-Verlag, 2006).

[3] V. Colombo and A. Lucchini. On the subgroups with non-trivial Möbius number in the alternating and symmetric groups. *J. Algebra* **324** (2010), 2464–2474.

[4] H. Crapo. Möbius inversion in lattices. *Arch. Math.* (*Basel*) **19** (1968), 595–607.

[5] P. Hall. The Eulerian functions of a group. *Quart. J. Math. Oxford Ser.* **7** (1936), 134–151.

[6] P. Jiménez-Seral. Coefficients of the probabilistic function of a monolithic group. *Glasgow Math. J.* **50** (2008), 75–81.

[7] A. Lucchini. Subgroups of solvable groups with non-zero Möbius function. *J. Group Theory* **10** (2007), 633–639.

[8] A. Lucchini. On the subgroups with non-trivial Möbius number. *J. Group Theory* **13** (2010), 589–600.

[9] A. Lucchini. Profinite groups with nonabelian crowns of bounded rank and their probabilistic zeta function. *Israel J. Math.*, to appear.

[10] A. Lucchini, F. Menegazzo and M. Morigi. Complements of the socle in monolithic groups. *Groups Geom. Dyn.* **1** (2007), 585–611.

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

[12] A. Mann. A probabilistic zeta function for arithmetic groups. *Internat. J. Algebra Comput.* **15** (2005), 1053–1059.

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

Received 9 February, 2010; revised 16 June, 2010

Andrea Lucchini, Dipartimento di Matematica Pura ed Applicata, Via Trieste 63, 35121 Padova, Italy
E-mail: lucchini@math.unipd.it

AUTHOR'S COPY | AUTORENEXEMPLAR