J. Group Theory **13** (2010), 589–600
DOI 10.1515/JGT.2010.009

**Journal of Group Theory**


# On the subgroups with non-trivial Möbius number

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 rules: $\mu(G, G) = 1$ and $\sum_{K \geqslant H} \mu(K, G) = 0$ if $H < G$. In [8] and [9] Mann proposed the following problems:

(1) What are the groups in which $|\mu(H, G)|$ is bounded by a polynomial function in the index of $H$?

(2) What are the groups in which the number $b_n(G)$ of subgroups $H$ of index $n$ satisfying $\mu(H, G) \neq 0$ grows at most polynomially in $n$?

The interest of these questions is related to the study of the function $P(G, k)$ expressing the probability that $k$ randomly chosen elements generate $G$ topologically (the probability being defined via the normalized Haar measure on $G$). Indeed, as proved by Mann in [9], the groups $G$ for which $\mu(H, G)$ and $b_n(G)$ are polynomially bounded in terms of $|G : H|$ and $n$ respectively 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 $P(G, k)$ on any large enough positive integer $k$.

Since $\mu(M, G) = -1$ for any maximal subgroup $M$ of $G$, we must 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 [10] 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 $|\mu(H,G)|$ is bounded by a polynomial function in the index of $H$ and $b_n(G)$ grows at most polynomially in $n$.

He proved his conjecture when $G$ is the completion of $\Gamma(R)$ with respect to the congruence topology, with $\Gamma$ a simple algebraic group defined over $\mathbb{Z}$ and $R$ the ring of integers in some algebraic number field [9]. The conjecture has been proved in [6] for finitely generated prosolvable groups, and more recently [7] for groups with polynomial subgroup growth and for finitely generated adelic groups.

As noticed in [8, p. 447], if $H$ is an open subgroup of $G$ and $\mu(H,G) \neq 0$, then $H$ is an intersection of maximal subgroups. Moreover, for such a subgroup, $\mu(H,G)$ is the difference between the number of ways to express $H$ as an intersection of an even number of maximal subgroups and the number of ways to express it as an intersection of an odd number of maximal subgroups. This means that $b_n(G)$ is bounded in terms of the number of maximal subgroups of $G$ of index dividing $n$ and $\mu(H,G)$ can be bounded in terms of the number of maximal subgroups of $G$ containing $H$. Some interesting bounds can be obtained with these arguments (see for example [8, Theorem 21]) but even if one assumes that $G$ has PMSG, it is not known whether this implies that there is a polynomial bound for the number of maximal intersections of $G$ of index at most $n$. The results proved in [9], [6], [7] for arithmetic groups, prosolvable groups, adelic groups and groups with polynomial subgroup growth depend on the fact that in all these cases it can be proved that if $\mu(H,G) \neq 0$, then not only $H$ is an intersection of maximal subgroups, but also these maximal subgroups can be chosen with additional 'good' properties. The main result of the present paper is in this direction:

**Theorem 1.** *Assume that $G$ is a finitely generated profinite group and let $H$ be an open proper subgroup of $G$ with $\mu(H,G) \neq 0$. Then there exists a finite family $\{Y_1, \ldots, Y_t\}$ of open subgroups of $G$ with the following properties*:

(1) $H = Y_1 \cap \cdots \cap Y_t$;

(2) $|G:H| = |G:Y_1| \ldots |G:Y_t|$;

(3) *for each $i$ we have $\mu(Y_i, G) \neq 0$;*

(4) *for each $i$ either $Y_i$ is a maximal subgroup of $G$ or there exists a subgroup $K_i \leqslant Y_i$ such that $K_i \trianglelefteq G$, $G/K_i$ is a finite monolithic group with non-abelian socle, say $N_i/K_i$, and $Y_i N_i = G$.*

This result is one of the key ingredients in the proof of the following theorem which reduces the study of Conjecture 1 to finite monolithic groups (i.e. groups with a unique minimal normal subgroup) with non-abelian socle:

**Theorem 2.** *Let $G$ be a PFG group and denote by $\Lambda(G)$ the set of finite monolithic groups $L$ such that* soc $L$ *is non-abelian and $L$ is an epimorphic image of $G$. Moreover, if $L \in \Lambda(G)$, let $b_n^*(L)$ be the number of subgroups $K$ of $L$ with $|L:K| = n$, $K$* soc $L = L$ *and $\mu(K,L) \neq 0$. Then the following are equivalent*:

(1) *there exist two constants* $\gamma_1$ *and* $\gamma_2$ *such that*

$$b_n(G) \leqslant n^{\gamma_1} \quad \text{and} \quad |\mu(H,G)| \leqslant |G:H|^{\gamma_2}$$

*for each* $n \in \mathbb{N}$ *and each open subgroup* $H$ *of* $G$;

(2) *there exist two constants* $c_1$ *and* $c_2$ *such that*

$$b_n^*(L) \leqslant n^{c_1} \quad \text{and} \quad |\mu(X,L)| \leqslant |L:X|^{c_2}$$

*for each* $L \in \Lambda(G)$, *each* $n \in \mathbb{N}$ *and each* $X \leqslant L$ *with* $L = X \operatorname{soc} L$.

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

**Conjecture 2.** For any positive integer $d$ there exists a constant $c_d$ such that the following holds: if $L$ is a $d$-generated finite monolithic group and $\operatorname{soc} L$ is non-abelian, then $b_n^*(L) \leqslant n^{c_d}$ and $|\mu(X,L)| \leqslant |L:X|^{c_d}$ for each $n \in \mathbb{N}$ and each $X \leqslant L$ with $L = X \operatorname{soc} L$.

At the moment this conjecture is a completely open question. It would be interesting to start with finite simple groups. Very little is known even in this case but recently, in collaboration with Valentina Colombo, we have proved that this conjecture is satisfied by the symmetric and alternating groups. A paper with this result is in preparation.

Another consequence of Theorem 2 is:

**Corollary 3.** *Let* $G$ *be a PFG profinite group and suppose that there exists* $u \in \mathbb{N}$ *such that for each* $L \in \Lambda(G)$ *any supplement* $X$ *of* $\operatorname{soc} L$ *in* $L$ *is* $u$*-generated. Then there exist* $\gamma_1$ *and* $\gamma_2$ *such that* $b_n(G) \leqslant n^{\gamma_1}$ *and* $|\mu(H,G)| \leqslant |G:H|^{\gamma_2}$ *for each* $n \in \mathbb{N}$ *and each open subgroup* $H$ *of* $G$.

As we noted before, if $b_n(G)$ grows polynomially, then $G$ must be a PFG group. However a group $G$ in which $|\mu(H,G)|$ is bounded by a polynomial function in the index of $H$ is not necessarily PFG: an example of this situation will be presented in the final section of this paper.

## 2 Subgroups with non-trivial Möbius number

Before starting our study of the subgroups with non-trivial Möbius number, we need to recall the definition of an equivalence relation among the chief factors of a finite group $G$ that was introduced in [5].

**Definition 4.** Let $G$ be a finite group and let $X$ be a subgroup of $G$. We say that two chief factors $H_1/K_1$ and $H_2/K_2$ of $G$ are $(G,X)$-equivalent if either $H_1/K_1$ and $H_2/K_2$ are $G$-isomorphic or there exists a normal subgroup $N$ of $G$ such that

(1) $G/N$ is a primitive permutation group which contains two distinct minimal normal subgroups $M_1/N$ and $M_2/N$;

(2) there exists a subgroup $U$ of $G$ containing $XN$ such that $U/N$ is a complement of both $M_1/N$ and $M_2/N$ in $G/N$;

(3) $H_1/K_1$ is $G$-isomorphic to $M_1/N$;

(4) $H_2/K_2$ is $G$-isomorphic to $M_2/N$.

An important role in the study of $(G, X)$-equivalence is played by the normal subgroup $R_{G,X}(A)$ associated with any chief factor $A$ of $G$. It is introduced in [5, Definition 10] and it can be characterized as the intersection of the maximal subgroups $M$ of $G$ with the property that any minimal normal subgroup of $G/\mathrm{Core}_G(M)$ is $(G, X)$-equivalent to $A$.

Another definition that we recall from [5] is the following:

**Definition 5.** Let $L$ be a monolithic primitive group and let $A$ be its unique minimal normal subgroup. For each positive integer $k$, let $L^k$ be the $k$-fold product of $L$. The *crown-based power* of $L$ of size $k$ is the subgroup $L_k$ of $L^k$ defined by

$$L_k = \{(l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \bmod A\}.$$

Clearly, $\mathrm{soc}(L_k) = A^k$, $L_k/\mathrm{soc}(L_k) \cong L/A$ and the quotient group of $L_k$ over any minimal normal subgroup is isomorphic to $L_{k-1}$, for $k > 1$. Moreover, any normal subgroup of $L_k$ either contains or is contained in $\mathrm{soc}(L_k)$. Furthermore let $X$ be a subgroup of $L$ and consider the diagonal subgroup

$$\Delta(X) = \{(x, \ldots, x) \mid x \in X\} \leqslant \Delta(L) = \{(l, \ldots, l) \mid l \in L\} \leqslant L_k.$$

In [5] it is proved that the minimal normal subgroups of $L_k$ are all $(L_k, \Delta(X))$-equivalent. Moreover the following holds (see [5, Proposition 12]):

**Proposition 6.** *Let $A = U/V$ be a chief factor of $G$. Let $H \leqslant G$ and assume that either $A$ is non-abelian or that there exists a subgroup $T$ of $G$ containing $H$ such that $TU = G$ and $T \cap U = V$. Then there exist $k \in \mathbb{N}$, a monolithic primitive group $L$, a subgroup $X$ of $L$ and an epimorphism $\alpha : G \to L_k$ such that*

(1) $\ker \alpha = R_{G,H}(A)$;

(2) $H^\alpha = \Delta(X) = \{(x, \ldots, x) \mid x \in X\} \leqslant \Delta(L) = \{(l, \ldots, l) \mid l \in L\}$;

(3) $U^\alpha \cong A \cong \mathrm{soc}\, L$.

The proof of [5, Proposition 16] shows that Crapo's complement theorem implies the following result:

**Lemma 7.** *Let $N$ be a normal subgroup of a finite group $G$. Then*

$$\mu(H,G) = \mu(HN,G) \sum_{Y \in \mathscr{S}(G,H,N)} \mu(Y,G)$$

*where* $\mathscr{S}(G,H,N) := \{ Y \leqslant G \mid H \leqslant Y,\ YN = G,\ Y \cap N = H \cap N, \mu(Y,G) \neq 0\}$.

We want to apply this lemma when $\mathrm{Core}_G(H) = 1$, $\mu(H,G) \neq 0$ and $N$ is a minimal normal subgroup of $G$. In order to do that we need more information on the set $\mathscr{S}(G,H,N)$.

**Lemma 8.** *Assume that $G$ is a finite group and that $H$ is a proper subgroup of $G$ with* $\mathrm{Core}_G(H) = 1$ *and* $\mu(H,G) \neq 0$. *Let $N$ be a minimal normal subgroup of $G$ and let $R = R_{G,H}(N)$. If $Y \in \mathscr{S} = \mathscr{S}(G,H,N)$, then $R \leqslant Y$. Moreover, there exist $t \in \mathbb{N}$, a monolithic primitive group $L$ with* $\operatorname{soc} L \cong N$ *and an epimorphism $\alpha : G \to L_t$ with* $\ker \alpha = R$ *so that the following holds.*

(1) *$N^\alpha$ is a minimal normal subgroup of $L_t$.*

(2) *If $N$ is abelian, then $Y^\alpha$ is a maximal subgroup of $L_t$ and it is a complement of $N^\alpha$.*

(3) *If $N$ is non-abelian, then either $Y^\alpha$ is a maximal subgroup of $L_t$ and complements $N^\alpha$, or $Y^\alpha$ contains the subgroup $K$ generated by all minimal normal subgroups of $L_t$ that are different from $N^\alpha$.*

(4) *If there exists $Y \in \mathscr{S}$ such that $Y^\alpha$ is a maximal subgroup of $L_t$ complementing $N^\alpha$, then $H \cap N = 1$.*

(5) *Assume that $N$ is non-abelian with $\mathscr{T} = \{ Y \in \mathscr{S} \mid K \leqslant Y^\alpha \} \neq \varnothing$. Then there exist a subgroup $X$ of $L$ with $|HN : H| \geqslant |X \operatorname{soc} L : X|$ and an epimorphism $\beta : G \to L$ with $\ker \alpha \leqslant \ker \beta$ such that $Y \in \mathscr{T}$ if and only if $\ker \beta \leqslant Y$ and $Y^\beta \in \mathscr{S}(L, X, \operatorname{soc} L)$.*

*Proof.* By Lemma 7, $\mu(H,G) \neq 0$ implies that $\mathscr{S} = \mathscr{S}(G,H,N) \neq \varnothing$. Let $Y \in \mathscr{S}$. Since $\mathrm{Core}_G(H) = 1$, we have $Y \cap N = H \cap N \neq N$, hence $Y$ is a proper supplement of $N$ (and consequently it is a complement of $N$ in the particular case when $N$ is abelian). Since $\mu(Y,G) \neq 0$, $Y$ is an intersection of maximal subgroups of $G$. Moreover, as shown in the proof of [5, Theorem 19], any maximal subgroup which contains $Y$ contains $R$, hence $R \leqslant Y$. By Proposition 6, there exist a positive integer $t$, a primitive monolithic group $L$ with $\operatorname{soc} L \cong N$ and an epimorphism $\alpha : G \to L_t$ with the following properties:

- $\ker \alpha = R$;
- $N^\alpha$ is a minimal normal subgroup of $L_t$;
- there exists $X \leqslant L$ such that $H^\alpha = \Delta(X) = \{(x, \ldots, x) \mid x \in X\}$.

Moreover, since $Y \in \mathscr{S}$,

$$HR \cap NR \leqslant YR \cap NR = Y \cap NR = (Y \cap N)R = (H \cap N)R \leqslant HR \cap NR.$$

Hence $HR \cap NR = YR \cap NR$ and the following are true:

- $Y^\alpha N^\alpha = L_t$;
- $Y^\alpha \cap N^\alpha = H^\alpha \cap N^\alpha$.

If $N$ is abelian, then $Y^\alpha$ is a non-trivial supplement of the minimal normal subgroup $N^\alpha$ of $L_t$, hence $Y^\alpha$ is a complement for $N^\alpha$ and it is a maximal subgroup of $L_t$.

Assume now that $N$ is non-abelian. We have $\operatorname{soc} L_t = N_1 \times \cdots \times N_t$, where $N_1, \ldots, N_t$ are all of the minimal normal subgroups of $L_t$; moreover $N_i \cong N$ for each $i$ and we may assume that $N^\alpha = N_1$. Let $K = N_2 \times \cdots \times N_t$. We have to prove that either $Y^\alpha$ contains $K$ or $Y^\alpha$ is a maximal subgroup of $L_t$ and complements $N_1$. There is nothing to prove if $t = 1$, so let $t \geqslant 2$. In this case

$$Y^\alpha \cap N^\alpha = H^\alpha \cap N^\alpha = \Delta(X) \cap N_1 = 1,$$

hence $Y^\alpha$ is a complement of $N^\alpha$ in $L_t$. Since $R = \ker \alpha \leqslant Y$,

$$\mu(Y^\alpha, L_t) = \mu(Y, G) \neq 0,$$

which implies $Y^\alpha = M_1 \cap \cdots \cap M_r$, where, for $1 \leqslant j \leqslant r$, $M_j$ is a maximal subgroup of $L_t$ supplementing $N^\alpha$. Recall that a maximal subgroup $M$ of $L_t$ which supplements $N_1$ satisfies one of the two following properties:

(I) $\operatorname{Core}_G(M) = K$;

(II) there exists $j \in \{2, \ldots, t\}$ such that $\operatorname{Core}_G(M) = N_2 \times \cdots \times \hat{N}_j \times \cdots \times N_t$; in this case $M$ is a complement for $N_1$. More precisely, there exist $\phi \in C_{\operatorname{Aut} N}(L/N)$ and $j \in \{2, \ldots, t\}$ such that $M = \{(l_1, \ldots, l_t) \in L_t \mid l_j = l_1^\phi\}$.

If $\operatorname{Core}_G(M_i) \neq K$ for some $i$, then $M_i = Y^\alpha$ since $|L_t : Y^\alpha| = |N_1| = |L_t : M_i|$. Otherwise $K \leqslant M_1 \cap \cdots \cap M_r = Y^\alpha$. This completes the proof of (3). Note that (4) follows immediately from the fact that $Y^\alpha \cap N^\alpha = H^\alpha \cap N^\alpha$ and the observation that the restriction of $\alpha$ to $N$ is injective. It remains to prove (5). We take $\beta = \alpha$ when $t = 1$; otherwise let $\beta = \alpha\pi$, with $\pi : L_t \to L_t/K \cong L$ the canonical projection. In both cases, $H^\beta = (\Delta(X))^\pi = X$ (which implies that $|HN : H| \geqslant |X \operatorname{soc} L : X|$) and $N^\beta = \operatorname{soc} L$. If $Y \in \mathscr{T}$, then, since $K \leqslant Y^\alpha$, we have

$$\ker \beta = \alpha^{-1}(K) \leqslant Y \ker \alpha = YR = Y.$$

Moreover if $\ker \beta \leqslant Y$, then $H \leqslant Y$ if and only if $X = H^\beta \leqslant Y^\beta$, and $Y^\beta N^\beta = L^t$ if and only if $YN = G$. Finally, as the restriction of $\beta$ to $N$ is injective, $Y \cap N = H \cap N$ if and only if $Y^\beta \cap N^\beta = H^\beta \cap N^\beta$. □

*Proof of Theorem* 1. Let $U = \mathrm{Core}_G(H)$. We shall work by induction on the order of the group $G/U$. Let $N/U$ be a minimal normal subgroup of $G/U$. Since $\mu(H/U, G/U) \neq 0$, by Lemma 7 we have

$$\mu(HN/U, G/U) = \mu(HN, G) \neq 0,$$

and there exists at least one subgroup $Y/U \in \mathscr{S}(G/U, H/U, N/U)$. In particular

$$|G : Y| = |YN : Y| = |HN : H|$$

and

$$HN \cap Y = H(N \cap Y) = H(N \cap H) = H.$$

By Lemma 8, $Y$ satisfies conditions (3)–(4) of the statement. Now we are ready to construct our family $\mathscr{Y} = \{Y_1, \ldots, Y_t\}$. If $HN = G$, then $H \in \mathscr{S}(G, H, N)$ and we may take $\mathscr{Y} = \{H\}$. Otherwise, since $\mu(HN, G) \neq 0$ and $\mathrm{Core}_G(HN) \geqslant N > U$, by induction there exist $t-1$ subgroups $Y_1, \ldots, Y_{t-1}$ which satisfy conditions (3)–(4) of our statement, such that

$$Y_1 \cap \cdots \cap Y_{t-1} = HN \quad \text{and} \quad |G : Y_1| \ldots |G : Y_{t-1}| = |G : HN|.$$

The family $\{Y_1, \ldots, Y_{t-1}, Y\}$ satisfies all conditions of our statement. □

## 3 Reduction to monolithic groups

**Theorem 9.** *Suppose that $G$ is a $d$-generated profinite group, and that there exists a constant $c$ with the following property: for any epimorphic image $L$ of $G$ which is monolithic with non-abelian socle and for any $X \leqslant L$*

$$|\mu(X, L)| \leqslant |\mu(X \operatorname{soc} L, L)|\, |X \operatorname{soc} L : X|^c.$$

*Then*

$$|\mu(H, G)| \leqslant |G : H|^{\mu}$$

*for each open subgroup $H$ of $G$, where $\mu = \max(d+1, c+1)$.*

*Proof.* Let $U = \mathrm{Core}_G(H)$. We shall work by induction on the order of $G/U$. We may assume that $H \neq G$ and $\mu(H, G) \neq 0$. In this case, as in the proof of Theorem 1, let $N/U$ be a minimal normal subgroup of $G/U$ and let

$$\mathscr{S}^* = \{Y \leqslant G \mid Y/U \in \mathscr{S}(G/U, H/U, N/U)\}.$$

By Lemma 7,

$$|\mu(H,G)| = |\mu(HN,G)|\left|\sum_{Y\in\mathscr{S}^*}\mu(Y,G)\right|.$$

By induction, $|\mu(HN,G)| \leqslant |G:HN|^\mu$. So it suffices to prove that

$$\left|\sum_{Y\in\mathscr{S}^*}\mu(Y,G)\right| \leqslant |HN:H|^\mu.$$

Let $\alpha: G/U \to L_t$ and $\beta: G/U \to L$ be the epimorphisms defined in Lemma 8 (the map $\beta$ is defined only when $N/U$ is non-abelian). Set $\alpha^* = \pi\alpha: G \to L_t$, $\beta^* = \pi\beta: G \to L$ with $\pi: G \to G/U$ the canonical projection. Define

$$\mathscr{T}^* = \{Y \leqslant G \mid \ker\beta^* \leqslant Y \text{ and } Y^{\beta^*} \in \mathscr{S}(L, X, \operatorname{soc} L)\}$$

and let $\mathscr{U}^*$ be the set of subgroups $Y$ containing $\ker\alpha^*$ and with the properties that $Y^{\alpha^*}$ is a maximal subgroup of $L^t = G^{\alpha^*}$ and a complement of $N_1 = N^{\alpha^*}$. By Lemma 8, $\mathscr{S}^* = \mathscr{T}^* \cup (\mathscr{U}^* \cap \mathscr{S}^*)$; moreover, for any $Y \in \mathscr{U}^*$, $Y$ is a maximal subgroup of $G$ so $\mu(Y,G) = -1$. Therefore

$$\left|\sum_{Y\in\mathscr{S}^*}\mu(Y,G)\right| \leqslant \left|\sum_{Y\in\mathscr{T}^*}\mu(Y,G)\right| + |\mathscr{U}^*| \leqslant \left|\sum_{\mathscr{L}\in\mathscr{S}(\mathscr{L},\mathscr{X},\operatorname{soc}\mathscr{L})}\mu(Q,\mathscr{L})\right| + |\mathscr{U}^*|.$$

Moreover, by Lemma 8 (4), if $\mathscr{U}^* \cap \mathscr{S}^* \neq \varnothing$, then $|HN:H| = |N|$. In that case $\mathscr{U}^*$ is in bijective correspondence with $|\operatorname{Der}(F, N_1)|$, where $F$ is a fixed complement of $N_1$ in $L_t$. Since $G$ is $d$-generated, $L_t$ and $F$ are $d$-generated, which implies

$$|\mathscr{U}^*| = |\operatorname{Der}(F,N_1)| \leqslant |N_1|^d = |HN:H|^d.$$

If $N/U$ is abelian, then $\mathscr{S}^* \subseteq \mathscr{U}^*$, so

$$\left|\sum_{Y\in\mathscr{S}^*}\mu(Y,G)\right| \leqslant |\mathscr{U}^*| \leqslant |HN:H|^d.$$

Assume now that $N/U$ is non-abelian. By Lemma 7,

$$\mu(X\operatorname{soc}L, L)\sum_{Q\in\mathscr{S}(L,X,\operatorname{soc}L)}\mu(Q,L) = \mu(X,L).$$

Note that $0 \neq \mu(H, G)$ implies $\mu(X, L) = \mu(H \ker \beta^*, G) \neq 0$ by Lemma 7. We conclude that $\mu(X \operatorname{soc} L, L) \neq 0$, again by using Lemma 7. Therefore, by hypothesis,

$$\left| \sum_{Q \in \mathscr{S}(L, X, \operatorname{soc} L)} \mu(Q, L) \right| \leqslant |X \operatorname{soc} L : X|^c \leqslant |HN : H|^c.$$

So

$$\left| \sum_{Y \in \mathscr{S}^*} \mu(Y, G) \right| \leqslant |HN : H|^c + |HN : H|^d \leqslant |HN : H|^\mu$$

and the proof is complete. □

For a finitely generated profinite group $G$, denote by $b_n(G)$ the number of subgroups $H$ of index $n$ satisfying $\mu(H, G) \neq 0$. Moreover, if $L$ is a finite monolithic primitive group, let $b_n^*(L)$ be the number of subgroups $K$ of $L$ with $|L : K| = n$, $K \operatorname{soc} L = L$ and $\mu(K, L) \neq 0$. Finally 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 $G$.

**Theorem 10.** *Assume that $G$ is a PFG group and that there exists a constant $\gamma$ such that $b_n^*(L) \leqslant n^\gamma$ for each $n \in \mathbb{N}$ and each $L \in \Lambda(G)$. Then the sequence $\{b_n(G)\}_{n \in \mathbb{N}}$ has polynomial growth.*

*Proof.* For $n \neq 1$ we want to count the subgroups $H$ with $|G : H| = n$ and $\mu(H, G) \neq 0$. By Theorem 1, if $H$ is one of these subgroups, then there exist a factorization $n = n_1 \dots n_t$ and a family $Y_1, \dots, Y_t$ of subgroups of $G$ satisfying properties (3)–(4), with $|G : Y_i| = n_i$ and $\bigcap_{1 \leqslant i \leqslant t} Y_i = H$. There are at most $n^2$ possible choices for the factorization $n = n_1 \dots n_t$ (see [2]); we fix one of them. Since $G$ is PFG, there exists a constant $\alpha$ with $m_n(G) \leqslant n^\alpha$ for each $n \in \mathbb{N}$, since $m_n(G)$ is the number of maximal subgroups of index $n$. There are two possibilities for $Y_i$: either $Y_i$ is a maximal subgroup of $G$ or there exists a normal subgroup $K_i$ of $G$ contained in $Y_i$ such that $G/K_i \cong L_i$ is a finite monolithic group with non-abelian socle and $Y_i/K_i$ is a supplement of $\operatorname{soc}(G/K_i)$ in $G/K_i$. We have at most $n_i^\alpha$ choices for $Y_i$ in the first case. Let us bound the number of possible choices for a non-maximal subgroup $Y_i$. Note that $L_i$ has a faithful primitive permutational representation of degree $m \leqslant n_i$. Moreover, if $d$ is the smallest cardinality of a generating set of $G$, then $L_i$ is $d$-generated. It was proved by Jaikin-Zapirain and Pyber [3, Theorem 8.1] that there exists a constant $\beta$ such that for any positive integers $m$ and $d$ there are at most $m^{\beta d}$ $d$-generated primitive groups of degree $m$. So we have at most $\sum_{m \leqslant n_i} m^{\beta d} \leqslant n_i^{\beta d + 1}$ possibilities for $L_i$. Jaikin-Zapirain and Pyber proved also [3, Theorem 11.1] that if $G$ is a PFG group, then there exists a constant $\eta$ such that if $L$ is a finite monolithic primitive group and $\operatorname{soc} L$ has a faithful transitive representation of degree $m$, then there are at most $|L| m^\eta$ epimorphisms from $G$ to $L$. In particular, if $Z(L) = 1$, then there are at most $m^\eta$ normal subgroups $K$ of $G$ with $G/K \cong L$. In our case this implies that there

are at most $n_i^{\beta d+\eta+1}$ possible choices for $K_i$. When $K_i$ is fixed, the number of possibilities for $Y_i$ with $K_i \leqslant Y_i$ is at most $b^*_{n_i}(G/K_i) \leqslant n_i^{\gamma}$. Summarizing, we have at most $n_i^{\alpha} + n_i^{\beta d+\eta+\gamma+1} \leqslant n_i^{\alpha+\beta d+\eta+\gamma+2}$ possible choices for $Y_i$. But then

$$b_n(G) \leqslant n^2 \prod_{1 \leqslant i \leqslant t} n_i^{\alpha+\beta d+\eta+\gamma+2} = n^{\alpha+\beta d+\eta+\gamma+4}. \quad \square$$

*Proof of Theorem* 2. Clearly (1) implies (2), as $L$ is an epimorphic image of $G$ whenever $L \in \Lambda(G)$. Conversely if (2) holds, then, by Theorem 10, there exists $\gamma_1$ such that $b_n(G) \leqslant n^{\gamma_1}$ for each $n \in \mathbb{N}$. Assume that $G$ is $d$-generated and let $\gamma_2 = \max\{d+1, c_1+c_2+1\}$. We prove that $|\mu(H,G)| < |G:H|^{\gamma_2}$ for each open subgroup $H$ of $G$. By Theorem 9 and Lemma 7, it suffices to prove that, if $\mu(X \operatorname{soc} L, L) \neq 0$, then

$$\xi = \left| \sum_{Y \in \mathscr{S}(L, X, \operatorname{soc} L)} \mu(Y, L) \right| = \frac{|\mu(X,L)|}{|\mu(X \operatorname{soc} L, L)|} \leqslant |X \operatorname{soc} L : X|^{c_1+c_2}$$

for each $L \in \Lambda(G)$, each $n \in \mathbb{N}$ and each $X \leqslant L$. Let $\mathscr{S} = \mathscr{S}(L, X, \operatorname{soc} L)$ and $m = |X \operatorname{soc} L : X|$. If $Y \in \mathscr{S}$, then $|L:Y| = m$ and $Y \operatorname{soc} L = L$, so $|\mu(Y,L)| \leqslant m^{c_2}$ and there are at most $m^{c_1}$ possibilities for $Y \in \mathscr{S}$. But then

$$\xi \leqslant \sum_{Y \in \mathscr{S}} |\mu(L, Y)| \leqslant |\mathscr{S}| m^{c_2} \leqslant m^{c_1} m^{c_2}$$

as required. $\square$

*Proof of Corollary* 3. For a finite group $X$, the rank $\mathrm{r}(X)$ of $X$ is defined to be the smallest integer $u$ with the property that all subgroups of $X$ can be generated by $u$ elements. Assume that $\mathrm{r}(L) \leqslant u$ for each $L \in \Lambda(G)$: this implies in particular that there exists $m$ such that no $L \in \Lambda(G)$ has a section isomorphic to $\mathrm{Alt}(m)$. By [9, Corollary 2], there exists a constant $c$, which depends only on $m$ and $u$, such that if a finite group $X$ is $\mathrm{Alt}(m)$-free and $a_{n,u}(X)$ is the number of subgroups of index $n$ of $X$ that can be generated by $u$ elements, then $a_{n,u}(X) \leqslant n^c$. In particular we have $b^*_n(L) \leqslant a_{n,u}(L) \leqslant n^c$ for each $L \in \Lambda(G)$ and each $n \in \mathbb{N}$. Moreover, by [7, Lemma 18], we have $|\mu(X,L)| \leqslant n^{c+2}$ for each $L \in \Lambda(G)$ and each $X \leqslant L$ with $X \operatorname{soc} L = L$, so the conclusion follows from Theorem 2. $\square$

## 4 An example

Let $\Omega$ be the set of prime numbers $p$ with $p > 23$ and $p$ not of the form $(q^k-1)/(q-1)$ where $q$ is a prime power and $k$ is an integer.

**Lemma 11.** $|\mu(H, \mathrm{Alt}(p))| \leqslant |\mathrm{Alt}(p) : H|^2$ *for any* $p \in \Omega$ *and any* $H \leqslant \mathrm{Alt}(p)$.

*Proof.* Let $\mathscr{P}$ be the poset of partitions of $\{1,\dots,p\}$, ordered by refinement; the maximum $\hat{1}$ of $\mathscr{P}$ is $\{\{1,\dots,p\}\}$. Moreover let

$$\mathscr{P}^* = \{\sigma \in \mathscr{P} \mid \text{the orbits of some } H \leqslant \mathrm{Alt}(p) \text{ are the parts of } \sigma\}$$

(note that $\mathscr{P}^* = \mathscr{P}\backslash\mathscr{R}_1$, where $\mathscr{R}_1$, the first rank of $\mathscr{P}$, is the set of all partitions of $\{1,\dots,n\}$ into one pair and $n-2$ singletons). For each $H \leqslant \mathrm{Alt}(p)$, denote by $\sigma(H)$ the element of $\mathscr{P}$ whose parts are the orbit of $H$. If $\sigma = \{\Omega_1,\dots,\Omega_r\} \in \mathscr{P}^*$, then we define $X_\sigma = (\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_r)) \cap \mathrm{Alt}(p)$, the maximal subgroup of $\mathrm{Alt}(p)$ whose orbits are precisely the parts of $\sigma$. As explained in [11],

$$\mu(H, \mathrm{Alt}(p)) = -\sum_{T \in \mathscr{T}(H)} \mu(H,T) + \delta(H)\mu_{\mathscr{P}^*}(\sigma(H), \hat{1})$$

where $\mathscr{T}(H)$ is the set of transitive proper subgroups of $\mathrm{Alt}(p)$ containing $H$, and $\delta(H) = 1$ if $H = X_{\sigma(H)}$, $\delta(H) = 0$ otherwise. We have

$$|\mu_{\mathscr{P}^*}(\sigma(H), \hat{1})| \leqslant |\mathrm{Alt}(p) : H|,$$

since

$$\mu_{\mathscr{P}_*}(\sigma, \hat{1}) = \begin{cases} (-1)^{r-1}(r-1)! & \text{if } \sigma = \{\Omega_1,\dots,\Omega_r\} \neq \hat{0} \\ (-1)^p p!/2 + (-1)^{p-1}(p-1)! & \text{otherwise.} \end{cases}$$

Now let $\mathscr{T}$ be the set of the proper transitive subgroups of $\mathrm{Alt}(p)$. If $T \in \mathscr{T}$, then either $T \leqslant \mathrm{Aff}(1,p)$ or $T$ is almost simple: in the second case, from Guralnick's list of possible socles for primitive almost simple groups of prime power degree [1], one of the following holds: $\mathrm{soc}\, T = \mathrm{PSL}(k,q)$ and $p = (q^k-1)/(q-1)$; $\mathrm{soc}\, T = \mathrm{PSL}(2,11)$ acting on the cosets of $\mathrm{Alt}(5)$; $\mathrm{soc}\, T$ is one of the Mathieu groups $M_{11}$ or $M_{23}$. Since $p \in \Omega$, we can conclude that $T$ is contained in the normalizer of a $p$-cycle, which is metacyclic of order $p(p-1)/2$. Since each of these normalizers contains at most $(p-1)/2$ transitive subgroups, we have $(p-1)!/2 \geqslant |\mathscr{T}|$. If $T \in \mathscr{T}(H)$, then $T$ is a 2-generated solvable group and, by [6, Theorem 1.4] we have

$$|\mu(H,T)| \leqslant |T:H|^2 = (|\mathrm{Alt}(p) : H|/(p-2)!)^2$$

and so

$$\left| \sum_{T \in \mathscr{T}(H)} \mu(H,T) \right| \leqslant \frac{|\mathrm{Alt}(p) : H|^2 (p-1)!}{2((p-2)!)^2}$$

and we conclude $|\mu(H, \mathrm{Alt}\, p)| \leqslant |\mathrm{Alt}(p) : H|^2$. □

**Proposition 12.** *The infinite cartesian product*

$$G = \prod_{p \in \Omega} \mathrm{Alt}(p)^{p!/8}$$

*is not PFG, but* $|\mu(H, G)| \leqslant |G : H|^3$ *for each open subgroup* $H$ *of* $G$.

*Proof.* It is proved in [4] that $G$ is 2-generated but not PFG. Moreover, by Theorem 9 and the previous lemma, $|\mu(H, G)| \leqslant |G : H|^3$ for each open subgroup $H$ of $G$. □

## References

[1] R. Guralnick. Subgroups of prime power index in a simple group. *J. Algebra* **81** (1983), 304–311.
[2] V. C. Harris and M. V. Subbarao. On product partitions of integers. *Canad. Math. Bull.* **34** (1991), 474–479.
[3] A. Jaikin-Zapirain and L. Pyber. Random generation of finite and profinite groups and group enumeration. (In preparation.)
[4] W. Kantor and A. Lubotzky. The probability of generating a finite classical group. *Geom. Dedicata* **36** (1990), 67–87.
[5] A. Lucchini. The $X$-Dirichlet polynomial of a finite group. *J. Group Theory* **8** (2005), 171–188.
[6] A. Lucchini. Subgroups of solvable groups with non-zero Möbius function. *J. Group Theory* **10** (2007), 633–639.
[7] A. Lucchini. Profinite groups with nonabelian crowns of bounded rank and their probabilistic zeta function. *Israel J. Math.*, to appear.
[8] A. Mann. Positively finitely generated groups. *Forum Math.* **8** (1996), 429–459.
[9] A. Mann. A probabilistic zeta function for arithmetic groups. *Internat. J. Algebra Comput.* **15** (2005), 1053–1059.
[10] A. Mann and A. Shalev. Simple groups, maximal subgroups, and probabilistic aspects of profinite groups. *Israel J. Math.* **96** (1996), 449–468.
[11] J. Shareshian. On the Möbius number of the subgroup lattice of the symmetric group. *J. Combin. Theory Ser. A* **78** (1997), 236–267.

Received 19 June, 2009; revised 21 October, 2009

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