J. Group Theory **10** (2007), 633–639
DOI 10.1515/JGT.2007.047

Journal of Group Theory

Subgroups of solvable groups with non-zero Möbius function

Andrea Lucchini

(Communicated by N. Boston)

Abstract. We obtain some results on the subgroups of finite solvable groups with non-zero Möbius function. These are used to prove a conjecture of Mann in the particular case of prosolvable groups: if G is a finitely generated prosolvable group, then the infinite sum $\sum_H \mu_G(H)|G:H|^{-s}$, where H ranges over all open subgroups of G, is absolutely convergent in some right half-plane of the complex plane.

1 Introduction

Let G be a finitely generated profinite group. We can consider G as a probability space, relative to the normalized Haar measure, and denote by $P(G,k)$ the probability that k random elements generate G. The group G is called positively finitely generated (PFG) if $P(G,k) > 0$ for some k. In [3], Mann proposed the following conjecture:

Conjecture 1.1. If G is a PFG group, then the function $P(G,k)$, which is defined and positive for all large integers k, can be continued in a natural way to an analytic function $P(G,s)$, defined for all s in some right half-plane of the complex plane.

The reciprocal of a function with these properties has some right to be called the ζ-function of G. In [3] the existence of this function was proved for finitely generated prosolvable groups (which have been shown to be PFG groups). More recently Mann [4] proved that a function with these properties can also be defined for all arithmetic groups with the congruence subgroup property. In dealing with these groups, Mann proposed a new stronger conjecture. Let us recall some definitions needed to formulate this second conjecture.

The Möbius function $\mu_G(H)$ of a group G is defined for all finite index subgroups H of G by the rules: $\mu_G(G) = 1$, and, for $H < G$, $\sum_{K \geqslant H} \mu_G(K) = 0$. For a finitely generated profinite group G, consider the series

$$P(G,s) = \sum_H \mu_G(H)|G:H|^{-s}, \tag{S}$$

where H ranges over all open subgroups of G, arranged in some order. With a suitable ordering, and with a suitable insertion of parentheses, the series (S) converges, for a positive integer k, to $P(G,k)$. Thus if $P(G,s)$ converges, it is a candidate for the function mentioned in Conjecture 1.1. The conjecture proposed by Mann in [4] is the following:

Conjecture 1.2. Let G be a PFG group. Then the infinite series (S) converges absolutely in some right half plane.

This second conjecture holds when G is an arithmetic group with the congruence subgroup property, but it appears to be much stronger than Conjecture 1.1 and much harder to prove in general. The aim of this paper is to prove Conjecture 1.2 for finitely generated prosolvable groups:

Theorem 1.3. *If G is a finitely generated prosolvable group, then the series* (S) *converges absolutely in some right half-plane.*

This improves the results obtained by Mann in [3, Section 5]. He considered a descending normal subgroup basis $\{N_i\}_{i\in\mathbb{N}}$ for a finitely generated prosolvable group G and proved that the infinite series (S) converges in some half-plane if, for each $i\in\mathbb{N}$, one collects first the summands corresponding to the subgroups H containing N_i. Once we know that (S) converges absolutely, the order of summation of the terms $\mu_G(H)|G:H|^{-s}$ is unimportant and the definition of the ζ-function of G can be given without reference to a descending normal subgroup basis.

Since only subgroups H with $\mu_G(H)\neq 0$ occur in (S), let us denote by $b_n(G)$ the number of such subgroups of index n. We say that $b_n(G)$ grows polynomially if it is bounded above by n^t, for some t independent of n, and we say that $\mu_G(H)$ grows polynomially if $|\mu_G(H)|$ is bounded above by $|G:H|^t$. By [4, Theorem 3], *the series* (S) *converges absolutely in some half-plane if and only if both $\mu_G(H)$ and $b_n(G)$ grow polynomially*. Thus, in order to prove Theorem 1.3, we need to study the behaviour of subgroups of finite solvable groups with non-zero Möbius function. One of the results we will prove is:

Theorem 1.4. *Let G be a finite solvable group and let H be a proper subgroup of G. If G can be generated by d elements, then $|\mu_G(H)|<|G:H|^d$.*

This immediately implies that $|\mu_G(H)|\leqslant|G:H|^d$ for any open subgroup H of a d-generated prosolvable group. There remains the problem of bounding the number of subgroups H with index n and non-zero Möbius function. It is known that if H is proper subgroup of a finite group G with $\mu_G(H)\neq 0$, then H can be expressed as an intersection of maximal subgroups of G; when G is solvable, a stronger result holds:

Theorem 1.5. *Assume that G is a finite solvable group and that H is a proper subgroup of G with $\mu_G(H)\neq 0$. Then there exists a family $M_1,\dots,M_t$ of maximal subgroups of G such that*

(1) $H = M_1 \cap \cdots \cap M_t$;

(2) $|G : H| = |G : M_1| \dots |G : M_t|$.

From the fact that a finitely generated prosolvable group G has polynomial maximal subgroup growth (see [3, Theorem 10]), it follows easily that $b_n(G)$ grows polynomially too.

Note that Theorem 1.5 does not hold without the assumption that G is solvable. For example take $G = \mathrm{Sym}(5)$ and consider the intersection $H \cong \mathrm{Sym}(3)$ of two point stabilizers: we have $\mu_G(H) = 2 \neq 0$ and $|G : H| = 20$; however the maximal subgroups of G containing H are two point stabilizers K_1 and K_2 with index 5 and $K_3 \cong \mathrm{Sym}(2) \times \mathrm{Sym}(3)$ with index 10. It seems more difficult to decide whether Theorem 1.4 remains true for arbitrary finite groups. One can conjecture that there exists a constant α such that $|\mu_G(H)| \leqslant |G : H|^{\alpha d}$ whenever H is a subgroup of a d-generated finite group G. In all examples that we were able to check, this conjecture holds with $\alpha = 1$.

2 The Dirichlet polynomial $P_G(H, s)$

In this section we recall some results from [2], that will be used in our study of subgroups with non-zero Möbius function. To any subgroup H of a finite group G, there corresponds a Dirichlet polynomial $P_G(H, s)$, defined as follows:

$$P_G(H,s) := \sum_{n \in \mathbb{N}} \frac{a_n(G,H)}{n^s} \quad \text{with } a_n(G,H) := \sum_{\substack{|G:K|=n \\ H \leqslant K \leqslant G}} \mu_G(K).$$

Clearly the following is true:

Remark 2.1. If $a_n(G,H) \neq 0$, then $n \leqslant |G : H|$; moreover $\mu_G(H) = a_{|G:H|}(G,H)$.

If N is a normal subgroup of G, then we may consider the Dirichlet polynomial $P_{G/N}(HN/N, s)$. We have that $P_{G/N}(HN/N, s)$ divides $P_G(H, s)$; more precisely:

Proposition 2.2 (see [2, Proposition 16]). *If N is a normal subgroup of a finite group G then*

$$P_G(H,s) = P_{G/N}(HN/N,s) P_{G,N}(H,s)$$

where

$$P_{G,N}(H,s) := \sum_{n \in \mathbb{N}} \frac{b_n(G,H,N)}{n^s} \quad \textit{with } b_n(G,H,N) := \sum_{\substack{|G:K|=n \\ H \leqslant K \leqslant G, KN=G}} \mu_G(H).$$

Remark 2.3. If $b_n(G, H, N) \neq 0$, then there exists K such that $|G : K| = n$, $H \leqslant K$ and $KN = G$; in particular $n = |G : K| = |N : K \cap N| \leqslant |N : H \cap N|$.

By taking a chief series $1 = N_{l+1} < \cdots < N_2 < N_1 = G$ and iterating Proposition 2.2, we obtain an expression of $P_G(H, s)$ as a product indexed by the factors in the series:

$$P_G(H, s) = \prod_{1 \leqslant i \leqslant l} P_{G/N_{i+1}, N_i/N_{i+1}}(HN_{i+1}/N_{i+1}, s). \tag{2.1}$$

When k is a positive integer, $P_G(H, k)$ is the probability that G is generated by k random elements together with the elements of H. But also the polynomials $P_{G/N_{i+1}, N_i/N_{i+1}}(HN_{i+1}/N_{i+1}, s)$ have a probabilistic interpretation. If G can be generated by d elements and $k \geqslant d$, then $P_{G/N_{i+1}, N_i/N_{i+1}}(HN_{i+1}/N_{i+1}, k)$ is the conditional probability that k random elements $g_1, \ldots, g_k$ satisfy the property $G = \langle g_1, \ldots, g_k, HN_{i+1} \rangle$ given that $G = \langle g_1, \ldots, g_k, HN_i \rangle$. In particular:

Remark 2.4. If there exist d elements $\langle g_1, \ldots, g_d \rangle$ of G such that $G = \langle H, g_1, \ldots, g_d \rangle$, then $0 < P_{G/N_{i+1}, N_i/N_{i+1}}(HN_{i+1}/N_{i+1}, d)$ for $1 \leqslant i \leqslant l$.

3 Proof of Theorem 1.3

Lemma 3.1. *Assume that G is a finite group, H is a subgroup of G and N is a normal subgroup of G. If $\mu_G(H) \neq 0$, then the following holds*:

(1) $\mu_G(HN) \neq 0$;

(2) *there exists $K \leqslant G$ such that $H \leqslant K$, $KN = G$ and $H \cap N = K \cap N$.*

Proof. Assume that $\mu_G(H) = a_{|G:H|}(G, H) \neq 0$; by Proposition 2.2, there exist positive integers u, v such that $a_u(G/N, HN/N) \neq 0$, $b_v(G, H, N) \neq 0$ and $uv = |G : H|$. By Remarks 2.1 and 2.3, $u \leqslant |G : HN|$ and $v \leqslant |N : H \cap N|$. Since $|G : H| = |G : HN|\,|N : H \cap N|$, we have $|G : H| = uv$ only if $u = |G : HN|$ and $v = |N : H \cap N|$. By Remark 2.1,

$$a_{|G:HN|}(G/N, HN/N) = \mu_{G/N}(HN/N) = \mu_G(HN) \neq 0.$$

By Remark 2.3, since $b_{|N:H \cap N|}(G, H, N) \neq 0$, there exists K with $H \leqslant K$, $KN = G$ and $|N : K \cap N| = |N : H \cap N|$; clearly we must have $K \cap N = H \cap N$. □

Proof of Theorem 1.5. The proof is by induction on $|G : H|$. Since we have $\mu_G(H) = \mu_{G/\mathrm{Core}_G(H)}(H/\mathrm{Core}_G(H))$, we may assume that $\mathrm{Core}_G(H) = 1$. Let N be a minimal normal subgroup of G. By Lemma 3.1, $\mu_G(HN) \neq 0$ and there exists K such that $H \leqslant K$, $G = KN$ and $K \cap N = H \cap N$. Note that $K \cap N = H \cap N$ is normalized by K and by N which is abelian, and so it is a normal subgroup of $G = KN$. As

$\mathrm{Core}_G(H) = 1$, we conclude that $K \cap N = H \cap N = 1$. In particular, K is a maximal subgroup of G and $|G : K| = |N| = |HN : H|$. If $HN = G$, then $H = K$ is a maximal subgroup of G and we are done. Otherwise, by induction, there exists a family $M_1, \dots, M_u$ of maximal subgroups of G such that

$$HN = \bigcap_{1 \leqslant i \leqslant u} M_i \quad \text{and} \quad |G : HN| = \prod_{1 \leqslant i \leqslant u} |G : M_i|.$$

We have $HN \cap K = H(N \cap K) = H$; hence $H = M_1 \cap \dots \cap M_u \cap K$. Moreover

$$|G : H| = |G : HN|\,|HN : H| = |G : HN|\,|G : K| = |G : M_1| \dots |G : M_u|\,|G : K|.$$

Hence $M_1, \dots, M_u$, K is the required family of maximal subgroups of G. □

Theorem 3.2. *Suppose that G is a finitely generated prosolvable group and denote by $b_n(G)$ the number of subgroups H such that $|G : H| = n$ and $\mu_G(H) \neq 0$. Then there exists a constant β such that $b_n(G) \leqslant n^{\beta}$.*

Proof. Recall that G is PMSG by [3, Theorem 10], which means that there exists α such that, for each $n \in \mathbb{N}$, the number of maximal subgroups of G with index n is bounded by n^{α}. Now, for $n \neq 1$, we want to count the subgroups H with $|G : H| = n$ and $\mu_G(H) \neq 0$. By Theorem 1.5, if H is one of these subgroups, then there exist a factorization $n = n_1 \dots n_t$ and a family $M_1, \dots, M_t$ of maximal subgroups of G with $|G : M_i| = n_i$ for $1 \leqslant i \leqslant t$ and $\bigcap_{1 \leqslant i \leqslant t} M_i = H$. There are at most n choices for the factorization $n = n_1 \dots n_t$ (see [5]) and for any fixed factorization, there are at most n_i^{α} choices for the maximal subgroup M_i, and consequently at most n^{α} choices for the family $M_1, \dots, M_t$. We conclude that $b_n(G) \leqslant n^{\alpha+1}$. □

Proof of Theorem 1.4. If G is a finite solvable group, then the polynomials which appear in (2.1) are very simple; indeed

$$P_{G/N_{i+1}, N_i/N_{i+1}}(HN_{i+1}/N_{i+1}, s) = 1 - \frac{c_i}{m_i^s}$$

where $m_i = |N_i/N_{i+1}|$ and c_i is the number of complements of N_i/N_{i+1} in G/N_{i+1} which contain HN_{i+1}/N_{i+1}. Since G can be generated with d elements, from Remark 2.4, we get

$$c_i < m_i^d. \tag{3.1}$$

Now let $J = \{j \mid 1 \leqslant j \leqslant l \text{ and } c_j \neq 0\}$. We have

$$P_G(H, s) = \prod_{j \in J} \left(1 - \frac{c_j}{m_j^s}\right).$$

By Remark 2.1, either $\mu_G(H) = 0$ or

$$m = \prod_{j \in J} m_j = |G : H| \quad \text{and} \quad \mu_G(H) = a_m(G, H) = (-1)^{|J|} \prod_{j \in J} c_j.$$

In the latter case, by (3.1), we conclude that $|\mu_G(H)| = \prod_{j \in J} c_j < \prod_{j \in J} m_j^d = m^d$. □

4 A final remark

As stated earlier, one can conjecture that there exists a constant α such that $\mu_G(H) \leqslant |G : H|^{\alpha d}$ whenever H is a subgroup of a d-generated finite group. By Theorem 1.4, in the solvable case we can take $\alpha = 1$; one can ask how sharp this choice is. Note that if G is an elementary abelian p-group of rank d, then $\mu_G(1) = (-1)^d p^{d(d+1)/2} = (-1)^d |G|^{(d-1)/2}$ (see for example [1, Corollary 3.5]). This is nearly the worst case, as the following result shows.

Proposition 4.1. *Let G be a finite solvable group and let H be a subgroup of G. If there exist d elements $g_1, \dots, g_d$ such that $G = \langle H, g_1, \dots, g_d \rangle$, then $|\mu_G(H)| < |G : H|^{(d+1)/2}$.*

Proof. We argue as in the proof of Theorem 1.4, but we need more precise information about the numbers c_i. We recall some notation and results from [2]. Let Ω be the set of irreducible G-modules N such that N is G-isomorphic to N_i/N_{i+1} for some $i \leqslant l$. For any $N \in \Omega$, let $J_N = \{j \in J \mid N_j/N_{j+1} \cong_G N\}$. As in the proof of Theorem 1.4, either $\mu_G(H) = 0$ or $m = \prod_{j \in J} m_j = |G : H|$ and $\mu_G(H) = (-1)^{|J|} \prod_{j \in J} c_j$. In the latter case, to prove our statement it suffices to show that for any $N \in \Omega$, we have

$$\prod_{j \in J_N} c_j < \left(\prod_{j \in J_N} m_j \right)^{(d+1)/2} = |N|^{|J_N|(d+1)/2}.$$

Now for a fixed $N \in \Omega$, let $t = |J_N|$, $q = |\mathrm{End}_G(N)|$ and let z be the cardinality of the set of cocycles $\beta \in \mathrm{Z}^1(G/C_G(N), N)$ which satisfy the condition $(hC_G(N))^\beta = 0$ for all $h \in H$. Since G is solvable, $z \leqslant |\mathrm{Z}^1(G/C_G(N), N)| \leqslant |N|$; moreover N is an $\mathrm{End}_G(N)$-vector space, so that $q \leqslant |N|$. As described in [2, Section 3], if $j \in J_N$, then

$$c_j = q^{v_j} z, \quad \text{with } v_j = |\{i \in J_N \mid i < j\}|.$$

By Remark 2.4, if $j^* = \max_{j \in J_N} j$, then $c_{j^*} = q^{t-1} z < |N|^d$. Hence

$$\prod_{j \in J_N} c_j = \prod_{0 \leqslant i \leqslant t-1} q^i z = q^{t(t-1)/2} z^t < |N|^{t(d+1)/2}.$$

This concludes the proof. □

References

[1] T. Hawkes, I. M. Isaacs and M. Özaydin. On the Möbius function of a finite group. *Rocky Mountain J. Math.* **19** (1989), 1003–1034.

[2] A. Lucchini. The X-Dirichlet polynomial of a finite group. *J. Group Theory* **8** (2005), 171–188.

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

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

[5] L. E. Mattics and F. W. Dodd. A bound for the number of multiplicative partitions. *Amer. Math. Monthly* **93** (1986), 125–126.

Received 3 January, 2007

Andrea Lucchini, Università di Brescia, Dipartimento di Matematica, Via Valotti, 25133 Brescia, Italy
E-mail: andrea.lucchini@ing.unibs.it