Andrea Lucchini

Subgroups of soluble groups with non-zero Möbius Function

Profinite and asymptotic group theory
Levico Terme, 16-21 September 2007

Let G be a finitely generated profinite group. We consider G as a probability space, with respect to the normalized Haar measure, and denote by $\boxed{P(G,k)}$ 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.

Conjecture A (Mann 1996) *If G is a PFG group, then the function $P(G,k)$, which is defined and positive for all large integers k, can be interpolated 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 is the *zeta-function of G.* If ζ is the Riemann zeta function, then $P(\hat{\mathbb{Z}},k) = \zeta(k)^{-1}$

Mann proposed two approaches to the problem, suggested by the following results:

$$P(G,k) = \inf_{N \lhd_o G} P(G/N,k)$$

If G is a finite group, then

$$P(G,k) = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^k}$$

If $1 = N_t \lhd \cdots \lhd N_0 = G$ is a normal series of a finite group G, then

$$P(G,k) = \prod_{1 \leq i \leq t} P_{G/N_i, N_{i-1}/N_i}(k) \quad \text{with}$$

$$P_{G/N_i, N_{i-1}/N_i}(k) = \sum_{\substack{N_i \leq H \leq G \\ N_{i-1}H = G}} \frac{\mu_G(H)}{|G:H|^k}$$

The Möbius function $\mu_G(H)$ is defined by:
$\mu_G(G) = 1, \quad \sum_{K \geq H} \mu_G(K) = 0$ if $H < G$.

Let G be a finitely generated profinite group and let $\{N_i\}_{i\in\mathbb{N}}$ be a chain of open normal subgroups with $\bigcap_{i\in\mathbb{N}} N_i = 1$.

The series (S)

$$\boxed{\sum_{H\leq_o G} \frac{\mu_G(H)}{|G:H|^k} \qquad \text{(S)}}$$

$P(G,k) = \lim_{i\to\infty}\left(\sum_{N_i\leq H\leq G} \frac{\mu_G(H)}{|G:H|^k}\right) \Rightarrow$ the series(S), <u>with the above insertion of parentheses</u> and with k replaced by a complex variable s, is a candidate for the conjectural function

Does this series converge in some half plane?

Different choices of the subgroup basis $\{N_i\}_{i\in\mathbb{N}}$ lead to different groupings of the terms in (S), so we have also to know whether two different bases lead to the same function.

It is interesting to know when (S) is convergent as written (without parentheses).

The product (P)

We can associate to G and to the subgroup basis $\{N_i\}_{i\in\mathbb{N}}$, the product

$$\boxed{\prod_{i\in\mathbb{N}} P_{G/N_i,N_{i-1}/N_i}(s) \quad \text{(P)}}$$

The product converges, for $k \in \mathbb{N}$, to the probability $P(G,k)$, so (P) is another candidate for our conjectural function.

(Mann) *Given a descending normal subgroup basis $\{N_i\}_{i\in\mathbb{N}}$, the associated series and product have the same domain of convergence, and in this domain they define the same function.*

The prosoluble case

Consider a descending normal subgroup basis $\{N_i\}_{i\in\mathbb{N}}$ of G with the property that N_{i-1}/N_i is a minimal normal subgroup of G/N_i for each $i \in \mathbb{N}$ (a chief series of G).

If G is prosoluble, then

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

where $m_i = |N_{i-1}/N_i|$ and c_i is the number of complements of N_{i-1}/N_i in G/N_i.

The infinite product $\boxed{\prod_{i\in\mathbb{N}} \left(1 - \frac{c_i}{m_i^s}\right)}$ is absolutely convergent if and only if the series

$$\sum_i c_i/m_i^s = \sum_n m_n(G)/n^s$$

is convergent (where $m_n(G)$ *is the number of maximal subgroups of index* n) and this is true if $|s|$ is large enough, as G has polynomial maximal subgroup growth.

(Mann) *Let G be a finitely generated prosoluble group. For any chief series of G, the associated product converges absolutely in some half plane, and all the functions obtained in this way have the same domain of absolutely convergence and define the same function in this domain.*

These methods does not allow us to conclude that the associated series are absolutely convergent; however a weaker result can be proved: *the series obtained from (S) by collecting together subgroups of the same index converge absolutely in some half plane.*

Conjecture B (Mann 2005) *Let G be a PFG group. Then the infinite series (S) converges absolutely in some right half plane.*

If (S) converges absolutely in some half plane, then (P) also converges absolutely in some half plane, and the two functions are identical in their common domain of convergence.

<u>Definitions</u>:

• $b_n(G) :=$ the number of subgroups H of G with $|G : H| = n$ and $\mu_G(H) \neq 0$

• $b_n(G)$ *grows polynomially* if there exists α such that $b_n(G) \leq n^\alpha \ \forall \alpha \in \mathbb{N}$.

• $\mu_G(H)$ *grows polynomially* if there exists β such that $|\mu_G(H)| \leq |G : H|^\beta \ \forall H \leq_o G$.

Proposition. *The series (S) converges absolutely in some half plane if and only if both* $\mu_G(H)$ *and* $b_n(G)$ *grow polynomially.*

(Mann) The previous criterium is satisfied by the profinite completion of arithmetic groups satisfying the congruence subgroup property.

What about prosoluble groups?

In order to answer this question, we need to study the behaviour of subgroups of finite soluble groups with non-zero Möbius function.

Auxiliary results

To any subgroup H of a finite group G, there corresponds a Dirichlet polynomial

$$P_G(H,s) := \sum_{n\in\mathbb{N}} \frac{\beta_n(G,H)}{n^s} \qquad \text{with}$$

$$\beta_n(G,H) := \sum_{\substack{|G:K|=n,\\ H\leq K\leq G}} \mu_G(K).$$

When k is a positive integer, $P_G(H,k)$ is the probability that k random elements generate G together with the elements of H.

Trivial but crucial remark: $\beta_m(G,H) = 0$ if $m > |G:H|$ and $\mu_G(H) = \beta_{|G:H|}(G,H)$.

If N is a normal subgroup of G, then $P_{G/N}(HN/N, s)$ divides $P_G(H, s)$:

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

$$P_{G,N}(H, s) := \sum_{n \in \mathbb{N}} \frac{\gamma_n(G, H, N)}{n^s} \qquad \text{with}$$

$$\gamma_n(G, H, N) := \sum_{\substack{|G:K|=n \\ H \leq K \leq G,\ KN=G}} \mu_G(K).$$

By taking a chief series $1 = N_t \lhd \ldots \lhd N_0 = G$, we obtain an expression of $P_G(H, s)$ as a product indexed by the factors in the series:

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

Theorem. *Let G be a finite soluble group and let $H < G$. Then $|\mu_G(H)| < |G : H|^{d(G)}$.*

Proof. Let $\boxed{m_i = |N_{i-1}/N_i|}$. There exists $c_i \in \mathbb{N}$ such that

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

$$\boxed{P_{G/N_i, N_{i-1}/N_i}(HN_i/N_i, d(G)) > 0 \Rightarrow c_i < m_i^{d(G)}}$$

Let $J = \{j \mid 1 \leq j \leq l \text{ and } c_j \neq 0\}$; we have

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

Let $\boxed{m = \prod_{j \in J} m_j}$.

$$\mu_G(H) = \begin{cases} 0 & \text{if } m < |G : H| \\ (-1)^{|J|} \prod_{j \in J} c_j & \text{otherwise.} \end{cases}$$

$$\Rightarrow \quad |\mu_G(H)| \leq \prod_{j \in J} c_j < \prod_{j \in J} m_j^{d(G)} = m^{d(G)}.$$

Corollary. *If G is a finitely generated prosoluble group, then $\mu_G(H)$ grows polynomially.*

With a more careful argument, a stronger version of the previous result can be obtained:

Proposition. *Let G be a finite soluble group and let $H < G$. If there exist d elements $g_1, \ldots, g_d$ such that $G = \langle H, g_1, \ldots, g_d \rangle$, then*

$$|\mu_G(H)| < |G : H|^{(d+1)/2}.$$

This result is essentially the best possible:

$$\mu_{C_p^d}(1) = (-1)^d p^{d(d-1)/2}.$$

No result is known in the unsoluble case.

It should be interesting for example to verify whether the following is true:

Conjecture. *There exists a constant γ such that $|\mu_S(1)| \leq |S|^\gamma$, for any nonabelian simple group S.*

We remain with 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 obtained as an intersection of maximal subgroups of G; when G is soluble, a stronger result holds:

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

1. $H = M_1 \cap \cdots \cap M_t$;
2. $|G : H| = |G : M_1| \cdots |G : M_t|$.

Proof. Induction on $|G : H|$, assuming $H_G = 1$.

Let N be a minimal normal subgroup of G. $P_G(H, s) = P_{G/N}(HN/N, s)P_{G,N}(H, s)$ implies:

$\mu_G(HN) \neq 0$ and there exists K such that $H \leq K$, $G = KN$ and $K \cap N = H \cap N$.

$$K \cap N \trianglelefteq G = KN \Rightarrow K \cap N = 1.$$

In particular K is a maximal subgroup of G.

• If $HN = G$, then $H = K$ is a maximal subgroup of G and we are done.

• Otherwise, by induction, there exists a family $M_1, \ldots, M_u$ of maximal subgroups of G s.t.

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

$$\Downarrow$$

$M_1, \ldots, M_u, K$ is the requested family of maximal subgroups of G.

The previous theorem does not hold without assuming that G is soluble.

For example take $G = \mathrm{Sym}(5)$ and consider the intersection $H \cong \mathrm{Sym}(3)$ of two point-stabilizers:

$$\mu_G(H) = 2 \text{ and } |G : H| = 20.$$

However the maximal subgroups of G containing H are:

- the two points stabilizers K_1 and K_2, which have index 5
- $K_3 \cong \mathrm{Sym}(2) \times \mathrm{Sym}(3)$, with index 10.

Corollary. *Suppose that G is a finitely generated prosoluble 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 $b_n(G) \leq n^\beta$.*

Proof. G is PMSG: 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.

For $n \neq 1$, we want to count the subgroups H with $|G : H| = n$ and $\mu_G(H) \neq 0$.

If H is one of these subgroups, then there exist

- a factorization $n = n_1 \cdots n_t$ (there are at most n possible factorizations)
- a family $M_1, \ldots, M_t$ of maximal subgroups of G with $|G : M_i| = n_i$ and $\bigcap_{1 \leq i \leq t} M_i = H$ (there are at most n_i^α possible choices for M_i, and consequently at most n^α possible choices for the family $M_1, \ldots, M_t$).

We conclude $\boxed{b_n(G) \leq n^{\alpha+1}.}$

Putting all together, we reach our conclusion:

Theorem. *If G is a finitely generated prosoluble group, then the series*

$$\sum_{H \leq_o G} \frac{\mu_G(H)}{|G : H|^s}$$

converges absolutely in some right half plane. Moreover if the positive integer k is large enough, then

$$P(G, k) = \sum_{H \leq_o G} \frac{\mu_G(H)}{|G : H|^k}.$$