On profinite groups with polynomially bounded Möbius numbers

Andrea Lucchini

Università di Padova, Italy

ISCHIA GROUP THEORY 2010
April, 14th - 17th

Definitions

Let G be a finitely generated profinite group.

- For each open subgroup H of G we may define

$$\mu(H,G)=\begin{cases}1 & \text{if } H=G\\ -\sum_{H<K\leq G}\mu(K,G) & \text{otherwise.}\end{cases}$$

- For each $n\in\mathbb{N}$, let $b_n(G)$ be the number of open subgroups H of index n in G and satisfying $\mu(H,G)\neq 0$.

Definitions

Let G be a finitely generated profinite group.

- For each open subgroup H of G we may define

$$\mu(H,G) = \begin{cases} 1 & \text{if } H = G \\ -\sum_{H<K\leq G} \mu(K,G) & \text{otherwise.} \end{cases}$$

- For each $n \in \mathbb{N}$, let $b_n(G)$ be the number of open subgroups H of index n in G and satisfying $\mu(H,G) \neq 0$.

We will say that a profinite group G has polynomially bounded Möbius numbers (PBMN) if there exists two constants β_1 and β_2 such that

- $b_n(G) \leq n^{\beta_1} \quad \forall n \in \mathbb{N}$
- $|\mu(H,G)| \leq |G:H|^{\beta_2} \quad \forall H \leq_o G$

Motivation

We consider G as a probability space (with respect to the normalized Haar measure) and denote by $P(G,k)$ the probability that k randomly chosen elements generate G.

Mann's remark

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 half complex plane.

Motivation

We consider G as a probability space (with respect to the normalized Haar measure) and denote by $P(G, k)$ the probability that k randomly chosen elements generate G.

Mann's remark

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 half complex plane.

When this happens, this infinite sum represents in the domain of convergency an analytic function which assumes precisely the value $P(G, k)$ on any positive integer k large enough.

We say that G has polynomial maximal subgroup growth (PMSG) if there exists a number c such that for all $n \in \mathbb{N}$, the number $m_n(G)$ of maximal subgroups of G of index n is at most n^c.

We say that G has polynomial maximal subgroup growth (PMSG) if there exists a number c such that for all $n \in \mathbb{N}$, the number $m_n(G)$ of maximal subgroups of G of index n is at most n^c.

If H is a maximal subgroup of G, then $\mu(H, G) = -1$

$$\Downarrow$$

$$m_n(G) \leq b_n(G)$$

We say that G has polynomial maximal subgroup growth (PMSG) if there exists a number c such that for all $n \in \mathbb{N}$, the number $m_n(G)$ of maximal subgroups of G of index n is at most n^c.

If H is a maximal subgroup of G, then $\mu(H, G) = -1$

$$\Downarrow$$

$$m_n(G) \leq b_n(G)$$

If G has *PBMN*, then G has *PMSG*. Is the converse true?

A profinite group G is called positively finitely generated (PFG) if $P(G,k) > 0\ \exists k \in \mathbb{N}$.

Theorem (Mann - Shalev 1996)

G is PFG if and only if G has PMSG.

Conjecture (Mann 1996)

If G is a PFG group, then the function $P(G,k)$ 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.

Conjecture (Mann 2005)

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

Partial results

The conjecture has been proved:

- for profinite completions of arithmetic groups satisfying the congruence subgroup property (A. Mann 2005);

Partial results

The conjecture has been proved:

- for profinite completions of arithmetic groups satisfying the congruence subgroup property (A. Mann 2005);
- for finitely generated prosoluble groups (AL 2007);

Partial results

The conjecture has been proved:

- for profinite completions of arithmetic groups satisfying the congruence subgroup property (A. Mann 2005);
- for finitely generated prosoluble groups (AL 2007);
- for profinite groups with polynomial subgroup growth (AL 2009);

Partial results

The conjecture has been proved:

- for profinite completions of arithmetic groups satisfying the congruence subgroup property (A. Mann 2005);
- for finitely generated prosoluble groups (AL 2007);
- for profinite groups with polynomial subgroup growth (AL 2009);
- for adelic groups (closed subgroups of $\mathrm{SL}(m, \hat{\mathbb{Z}})$) (AL 2009);

Partial results

The conjecture has been proved:

- for profinite completions of arithmetic groups satisfying the congruence subgroup property (A. Mann 2005);
- for finitely generated prosoluble groups (AL 2007);
- for profinite groups with polynomial subgroup growth (AL 2009);
- for adelic groups (closed subgroups of $SL(m, \hat{\mathbb{Z}})$) (AL 2009);
- for finitely generated profinite groups with the property that all the non abelian composition factors of every finite epimorphic images are of alternating type (V. Colombo AL 2100);

Partial results

The conjecture has been proved:

- for profinite completions of arithmetic groups satisfying the congruence subgroup property (A. Mann 2005);
- for finitely generated prosoluble groups (AL 2007);
- for profinite groups with polynomial subgroup growth (AL 2009);
- for adelic groups (closed subgroups of $\mathrm{SL}(m, \hat{\mathbb{Z}})$) (AL 2009);
- for finitely generated profinite groups with the property that all the non abelian composition factors of every finite epimorphic images are of alternating type (V. Colombo AL 2100);
- for finitely generated profinite groups for which there exists a constant r such that each nonabelian composition factor is either an alternating group or has rank at most r (AL 2010).

Definition

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. $b_n^*(L) \leq n^{\eta_1}$, where $b_n^*(L)$ denotes the number of subgroups K of L with $|L : K| = n$, $\mu(K, L) \neq 0$ and $L = K \operatorname{soc} L$;
2. $|\mu(K, L)| \leq |L : K|^{\eta_2}$ for each $K \leq L$ with $L = K \operatorname{soc} L$.

- If L is a finite monolithic group with nonabelian socle, then $\operatorname{soc} L = S_1 \times \cdots \times S_r$, where the S_i's are isomorphic simple groups.
- Let X_L be the subgroup of $\operatorname{Aut} S_1$ induced by the conjugation action of $N_L(S_1)$ on S_1.
- X_L is a finite almost simple group, uniquely determined by L.

Definition

Let G be a profinite group. We denote by $\Lambda(G)$ the set of finite monolithic groups L such that $\operatorname{soc} L$ is nonabelian and L is an epimorphic image of G.

Theorem (AL 2010)

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

The previous reduction theorem allows us to reformulate Mann's Conjecture as follows:

Conjecture

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

The previous reduction theorem allows us to reformulate Mann's Conjecture as follows:

Conjecture

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

V. Colombo, AL 2009

This conjecture is satisfied by the symmetric and alternating groups.

The reduction theorem follows from two results, proved in different papers and with different methods.

Theorem (A weaker reduction theorem)

A PFG group G has PBMN if there exist η_1 and η_2 such that L is (η_1, η_2)-bounded for each L in $\Lambda(G)$.

Theorem (From monolithic to almost simple groups)

Let L be a finite monolithic group with nonabelian socle. If the associated almost simple group X_L is (c_1, c_2)-bounded, then L is (η_1, η_2)-bounded with $\eta_1 = 11 + c_1 + c_2$ and $\eta_2 = 8 + 2c_2$.

The proof of the "weaker reduction theorem" relies on the following result.

The proof of the "weaker reduction theorem" relies on the following result.

Theorem

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 $\{Y_1,\dots,Y_t\}$ of open subgroups of G with the following properties:

1. $H = Y_1 \cap \cdots \cap Y_t$;
2. $|G : H| = |G : Y_1| \cdots |G : Y_t|$;
3. *for each* $1 \leq i \leq t$, *we have* $\mu(Y_i, G) \neq 0$;
4. *for each* $1 \leq i \leq t$, *either* Y_i *is a maximal subgroup of* G *or there exists an open normal subgroup* K_i *of* G *such that*
   - $K_i \leq Y_i$,
   - G/K_i *is a monolithic group with nonabelian socle, say* N_i/K_i,
   - $Y_i N_i = G$.

The Möbius function in the subgroup lattice of a monolithic group can be studied with the help of the Crapo's Closure Theorem.

A closure on a poset P is a function $x \mapsto \overline{x}$ satisfying:

- $x \leq \overline{x}$ for all $x \in P$
- if $x, y \in P$ with $x \leq y$, then $\overline{x} \leq \overline{y}$
- $\overline{\overline{x}} = \overline{x}$ for all $x \in P$

$\overline{P} = \{x \in P | \overline{x} = x\}$ is a poset with order induced by the order on P.

Theorem (Crapo's Closure Theorem)

Fix $x, y \in P$ such that $y \in \overline{P}$. Then

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

Given a finite monolithic group L with nonabelian socle, we want to study the Möbius function in the poset $\mathcal{P} = \{H \leq L \mid H \operatorname{soc} L = L\}$.

Given a finite monolithic group L with nonabelian socle, we want to study the Möbius function in the poset $\mathcal{P} = \{H \leq L \mid H \operatorname{soc} L = L\}$.

- $\operatorname{soc} L = S_1 \times \ldots \times S_r$ is a product of isomorphic simple groups.
- The conjugation action induces a map $\psi : N_L(S_1) \to \operatorname{Aut} S_1$.
- $X = \psi(N_L(S_1))$ is an almost simple group with $\operatorname{soc} X = \operatorname{Inn} S_1$.

Given a finite monolithic group L with nonabelian socle, we want to study the Möbius function in the poset $\mathcal{P} = \{H \le L \mid H \operatorname{soc} L = L\}$.

- $\operatorname{soc} L = S_1 \times \ldots \times S_r$ is a product of isomorphic simple groups.
- The conjugation action induces a map $\psi : N_L(S_1) \to \operatorname{Aut} S_1$.
- $X = \psi(N_L(S_1))$ is an almost simple group with $\operatorname{soc} X = \operatorname{Inn} S_1$.

For $H \in \mathcal{P}$, let

- $\{t_1, \ldots, t_r\}$ a right transversal of $N_H(S_1)$ in H,
- $Y = \psi(N_H(S_1))$.
- $H_Z := H((Z \cap S_1) \times (Z \cap S_1)^{t_2} \times \cdots \times (Z \cap S_1)^{t_r})$ if $Y \le Z \le X$

We define a closure in $\mathcal{P}$ by setting $\overline{H} := H_Y$.

Given a finite monolithic group L with nonabelian socle, we want to study the Möbius function in the poset $\mathcal{P} = \{H \leq L \mid H \operatorname{soc} L = L\}$.

- $\operatorname{soc} L = S_1 \times \ldots \times S_r$ is a product of isomorphic simple groups.
- The conjugation action induces a map $\psi : N_L(S_1) \to \operatorname{Aut} S_1$.
- $X = \psi(N_L(S_1))$ is an almost simple group with $\operatorname{soc} X = \operatorname{Inn} S_1$.

For $H \in \mathcal{P}$, let

- $\{t_1, \ldots, t_r\}$ a right transversal of $N_H(S_1)$ in H,
- $Y = \psi(N_H(S_1))$.
- $H_Z := H((Z \cap S_1) \times (Z \cap S_1)^{t_2} \times \cdots \times (Z \cap S_1)^{t_r})$ if $Y \leq Z \leq X$

We define a closure in $\mathcal{P}$ by setting $\overline{H} := H_Y$.

$$\mu(H, L) = \sum_{H \leq K \leq L,\ \overline{K} = L} \mu(K, L) \left(\sum_{Y \leq Z \leq X,\ H = H_Z \cap K} \mu(Z, X) \right)$$

An open question

- $\mu(H,G) \neq 0 \Rightarrow H$ is an intersection of maximal subgroups of G.
- The converse is false:

$$G = \langle a, b \mid a^5 = 1, b^4 = 1, a^b = a^2 \rangle \Rightarrow \mathrm{Frat}(G) = 1,\ \mu(1,G) = 0.$$

An open question

- $\mu(H,G) \neq 0 \Rightarrow H$ is an intersection of maximal subgroups of G.
- The converse is false:

$$G = \langle a, b \mid a^5 = 1, b^4 = 1, a^b = a^2 \rangle \Rightarrow \mathrm{Frat}(G) = 1,\ \mu(1, G) = 0.$$

Question

- $b_n(G)$= the numbers of subgroups H of G with index n and with $\mu(H,G) \neq 0$.
- $c_n(G)$= the numbers of subgroups of G with index n that are intersection of maximal subgroups.

$$b_n(G) \leq c_n(G).$$

How faster is the growth of $c_n(G)$ with respect to the growth of $b_n(G)$?

Question

Does there exist a profinite groups in which $b_n(G)$ is polynomially bounded but $c_n(G)$ is not polynomially bounded?

For example, let

$$G = \prod_{n \in \mathbb{N}} \mathrm{Alt}(n).$$

We have proved that $b_n(G)$ is polynomially bounded, but we don't have a good estimation for $c_n(G)$.

If G is a finitely generated prosoluble group, then $\{b_n(G)\}_{n\in\mathbb{N}}$ is polynomially bounded but we don't know what is the behavior of $\{c_n(G)\}_{n\in\mathbb{N}}$

THEOREM (F. MENEGAZZO AL 2010)

If G is a finitely generated prosupersoluble group, then $\{c_n(G)\}_{n\in\mathbb{N}}$ is polynomially bounded.

Let G be a finitely generated prosoluble group. The proof of the fact that $\{b_n(G)\}_{n\in\mathbb{N}}$ is polynomially bounded relies on the following property:

Theorem AL 2008

If G is a finite soluble group and H is a subgroup of G with $\mu(H, G) \neq 0$, then there exists a family $M_1, \dots, M_t$ of maximal subgroups of G such that

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

Question

Let $\mathcal{C}$ be a class of finite soluble groups (closed under subgroups, direct products and epimorphic images). Does there exist a constant γ with the following property?

If $G \in \mathcal{C}$ and $\mu(H, G) \neq 0$, then there exists a family $M_1, \ldots, M_t$ of maximal subgroups of G such that

- $H = M_1 \cap \cdots \cap M_t$;
- $|G : M_1| \cdots |G : M_t| \leq |G : H|^\gamma$

Question

Let $\mathcal{C}$ be a class of finite soluble groups (closed under subgroups, direct products and epimorphic images). Does there exist a constant γ with the following property?

If $G \in \mathcal{C}$ and $\mu(H, G) \neq 0$, then there exists a family $M_1, \dots, M_t$ of maximal subgroups of G such that

- $H = M_1 \cap \cdots \cap M_t$;
- $|G : M_1| \cdots |G : M_t| \leq |G : H|^{\gamma}$

If such a constant exists, then $\{c_n(G)\}_{n \in \mathbb{N}}$ is polynomially bounded whenever G is a finitely generated pro-$\mathcal{C}$-group.

The previous question is strongly related with the following:

Question

Does there exist a constant γ with the following property?

If $G \in \mathcal{C}$, V is an irreducible G-module and $W \subseteq V$, then W contains a subset W^* such that

- $|W^*| \leq \gamma$.
- $C_G(W) = C_G(W^*)$.