Andrea Lucchini

Profinite groups with a rational probabilistic zeta function

Let G be a finitely generated profinite group.

Some relevant sequences of integer numbers can be defined:

$a_n(G) :=$ the number of (open) subgroups of index n in G.

$m_n(G) :=$ the number of (open) maximal subgroups of index n in G.

$$b_n(G) := \sum_{|G:H|=n} \mu_G(H)$$

where μ_G is the Möbius function of the lattice of open subgroups

$\mu_G(G) = 1$, $\mu_G(H) = -\sum_{K>H} \mu_G(K)$ if $H < G$.

Why should one be interested in the study of the sequence $\{b_n(G)\}_{n\in\mathbb{N}}$?

A formal Dirichlet series $P_G(s)$ can be defined by considering the generating function associated with this sequence:

$$P_G(s) := \sum_{n\in\mathbb{N}} \frac{b_n(G)}{n^s}$$

If G is prosolvable (and hopefully in other relevant cases), then the series $P_G(s)$ is convergent in some right half plane of $\mathbb{C}$ and, for $t \in \mathbb{N}$ large enough, $P_G(t)$ gives the probability that t randomly chosen elements in G generate G. Mann proposed the name *probabilistic zeta function* for the multiplicative inverse of $P_G(s)$.

$$P_{\widehat{\mathbb{Z}}}(s) = \sum_n \frac{\mu(n)}{n^s} = \left(\sum_n \frac{1}{n^s}\right)^{-1} = \zeta(s)^{-1}$$

Many important results have been obtained about the asymptotic behavior of the sequences $\{a_n(G)\}_{n\in\mathbb{N}}$ and $\{m_n(G)\}_{n\in\mathbb{N}}$; in particular the connection between the growth type of these sequences and the structure of G has been widely studied.

It is completely unexplored the asymptotic behavior of the sequence $\{b_n(G)\}_{n\in\mathbb{N}}$.

For example it would be interesting to characterize the groups G for which the growth of the sequence $\{b_n(G)\}_{n\in\mathbb{N}}$ is polynomial.

Interesting but hard question!

Let us start with something (hopefully) easier.

Question. What can we say about G, if $b_n(G) = 0$ for almost all $n \in \mathbb{N}$?

Before making a conjecture, let us answer to the same question for the other two sequences.

- $a_n(G) = 0$ for almost all $n \Rightarrow G$ is finite.
- $m_n(G) = 0$ for almost all $n \Rightarrow \frac{G}{\operatorname{Frat} G}$ is finite.

If $\mu_G(H) \neq 0$, then H is an intersection of maximal subgroups of G and $\operatorname{Frat} G \leq H$. Hence

$$b_n(G) = \sum_{|G:H|=n} \mu_G(H) = b_n(G/\operatorname{Frat} G) \; \forall n \in \mathbb{N}.$$

One can expect that $b_n(G) = 0$ for almost all $n \in \mathbb{N}$ would imply that there are only finitely many subgroups of G that are intersection of maximal subgroups. This would lead to conjecture:

Conjecture. If $b_n(G) = 0$ for almost all n, then $G/\operatorname{Frat} G$ is finite.

Technical results that support our conjecture

A finitely generated profinite group G has a family $\{G_n\}_{n\in\mathbb{N}}$ of open normal subgroups such that

- $G_1 = G$,
- $\bigcap_{n\in\mathbb{N}} G_n = 1$,
- $G_{n+1} < G_n$,
- G_n/G_{n+1} is a chief factor of G.

To any chief factor G_n/G_{n+1} a Dirichlet polynomial (i.e. a finite Dirichlet series) $P_n(s)$ is associated:

$$P_n(s) = \sum_{r\in\mathbb{N}} \frac{b_{n,r}}{r^s} \quad \text{with} \quad b_{n,r} = \sum_{\substack{G_{n+1}\leq H\leq G \\ HG_n=G \\ |G:H|=r}} \mu_G(H)$$

The series $P_G(s)$ can be written as a formal infinite product:

$$P_G(s) = \prod_{n \in \mathbb{N}} P_n(s).$$

1. $P_n(s) = 1 \Leftrightarrow G_n/G_{n+1} \leq \mathsf{Frat}(G/G_{n+1})$.

2. $G/\operatorname{Frat} G$ is finite $\Leftrightarrow G_n/G_{n+1}$ is a Frattini factor for all but finitely many $n \in \mathbb{N}$.

3. $b_n(G) = 0$ for almost all $n \in \mathbb{N} \Leftrightarrow P_G(s)$ is finite (i.e. a Dirichlet polynomial).

So, a tempting (but wrong) argument is: if $P_G(s)$ is a finite series, then $P_n(s) = 1$ for all but finitely many $n \in \mathbb{N}$ and $G/\operatorname{Frat} G$ is finite.

We must be more careful: we cannot exclude that a formal product of infinitely many non trivial Dirichlet polynomials could be finite.

A related problem with a surprising solution

Assume that G is a finitely generated prosolvable group, and let p be a fixed prime number.

• If $a_{p^r}(G) = 0$ for almost all $r \in \mathbb{N}$, then G contains an open normal subgroup K which is a pro-p'-group.

• If $m_{p^r}(G) = 0$ for almost all $r \in \mathbb{N}$, then G contains an open normal subgroup K which is pro-p-nilpotent (equivalently, the set Ω_p of $n \in \mathbb{N}$ such that G_n/G_{n+1} is non-Frattini and has p-power order, is finite).

What about the prosolvable groups G with the property that $b_{p^r}(G) = 0$ for almost all $r \in \mathbb{N}$? Do they have the same behaviour as the prosolvable groups in which $m_{p^r}(G) = 0$ for almost all $r \in \mathbb{N}$?

In the prosolvable case, for any $n \in \mathbb{N}$, the finite series $P_n(s)$ associated with the chief factor G_n/G_{n+1} is:

$$P_n(s) = 1 - \frac{c_n}{|G_n/G_{n+1}|^s}$$

where c_n is the number of complements of G_n/G_{n+1} in G/G_{n+1}.

$P_G(s)$ has an *Euler factorization* over the set of prime numbers:

$$P_G(s) = \prod_p P_{G,p}(s)$$

where, for any prime p,

$$P_{G,p}(s) = \sum_r \frac{b_{p^r}(G)}{p^{rs}} = \prod_{n \in \Omega_p} \left(1 - \frac{c_n}{p^{r_n s}}\right), \text{ with}$$

$$\boxed{\Omega_p = \{n \mid |G_n/G_{n+1}| = p^{r_n} \text{ and } c_n \neq 0\}}$$

Question (Mann) Suppose that the p-factor $P_{G,p}(s)$ is a Dirichlet polynomial (equivalently $b_{p^r}(G) = 0$ for almost all $r \in \mathbb{N}$) or, more in general, that $P_{G,p}(s)$ is a rational function of $1/p^s$ (i.e. $P_G(s) = A(s)/B(s)$ with $A(s)$ and $B(s)$ Dirichlet polynomials). Does this imply that G contains a normal open pro-p-nilpotent subgroup?

The answer to the question is negative!

If t_n is the number of irreducible polynomials in $\mathbb{F}_2[x]$ of degree n, then

$$1 - 2x = \prod_n (1 - x^n)^{t_n}$$

So for example

$$1 - \frac{2p}{p^s} = \prod_n \left(1 - \frac{p^n}{p^{ns}}\right)^{t_n}$$

Let H be the free pro-abelian group of rank 2 and fix p an odd prime.

For any $n \in \mathbb{N}$, there is an irreducible action of $\mathbb{Z}_{p^n-1}$ over $(\mathbb{Z}_p)^n$; H contains t_n different open normal subgroups K with $H/K \cong \mathbb{Z}_{p^n-1}$; so we can construct t_n irreducible non isomorphic H-modules of order p^n: $M_{n,1}, \ldots, M_{n,t_n}$.

Consider $\boxed{G := \left(\prod_{n,i} M_{n,i}\right) \rtimes H.}$

G is a 2-generated prosolvable group, with infinitely many non-Frattini chief factors of p-power order: Ω_p is infinite and G does not contain any open normal pro-p-nilpotent subgroup. However

$$\begin{aligned} P_{G,p}(s) &= \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{p}{p^s}\right)\prod_n \left(1 - \frac{p^n}{(p^n)^s}\right)^{t_n} \\ &= \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{p}{p^s}\right)\left(1 - \frac{2p}{p^s}\right) \end{aligned}$$

In particular $b_{p^r}(G) = 0$ if $r \geq 4$.

By repeating the same game with all the prime numbers we can prove:

Theorem. There exists a 2-generated pro-solvable group G such that for each prime p

1. $P_{G,p}(s)$ is a Dirichlet polynomial;
2. G has infinitely many non-Frattini chief factors that are p-groups.

This does not answer our first question: *does* $P_G(s)$ *finite imply* $G/\operatorname{Frat} G$ *finite?* Indeed, the group G we constructed has the property that $P_{G,p}(s)$ is finite for each prime p; however we have also that $P_{G,p}(s) \neq 1$, so $P_G(s) = \prod_p P_{G,p}(s)$ turns out to be infinite.

Our conjecture holds for the prosolvable groups

Theorem (E. Detomi, AL) *Let G be a finitely generated prosolvable group. Then the following are equivalent:*

1. $b_n(G) = 0$ *for almost all* $n \in \mathbb{N}$.
2. $P_G(s)$ *is a Dirichlet polynomial.*
3. $P_G(s)$ *is a rational Dirichlet series.*
4. $G/\operatorname{Frat} G$ *is a finite group.*

The proof relies on the following facts:

A corollary of Skolem-Mahler-Lech Theorem

Let $\{\gamma_n\}_{n\in\mathbb{N}}$, $\{r_n\}_{n\in\mathbb{N}}$ *be two sequences of positive integers and let* $1 \neq \mu \in \mathbb{N}$. *If the infinite product*

$$\prod_{n\in\mathbb{N}} \left(1 - \frac{\gamma_n}{\mu^{r_n s}}\right)$$

is finite (or more in general rational), then for each prime q *there exists* $n \in \mathbb{N}$ *such that* q *divides* r_n.

Some representation theory

Let n *be the degree of an irreducible representation of a finite solvable group* X *over a finite field . If* q *is a prime divisor of* n, *then* $q \leq \max\{\pi(X)\}$.

Sketch of the proof

Let G be a finitely generated prosolvable group and let $\pi(G)$ be the set of prime divisors of the indices of the open subgroups of G.

$P_G(s) = \prod_p P_{G,p}(s)$ rational implies:

1. $\pi(G)$ is finite;

2. $P_{G,p}(s)$ is rational for all $p \in \pi(G)$.

Fix $p \in \pi(G)$ and let

$$P_{G,p}(s) = \prod_{n \in \Omega_p} \left(1 - \frac{c_n}{p^{r_n s}}\right).$$

Assume, by contradiction, $|\Omega_p| = \infty$.

For any prime q there exists $n \in \Omega_p$ such that q divides $r_n = \dim_{\mathbb{F}_p} G_n/G_{n+1}$.

This implies $q \leq \max\{\pi(G)\}$.

What about the general case?

Given an arbitrary finitely generated profinite group G, we can again express the Dirichlet series $P_G(s)$ as an infinite formal product

$$P_G(s) = \prod_n P_n(s)$$

where $P_n(s)$ is the Dirichlet polynomial associated with the chief factor G_n/G_{n+1}.

We would like to prove that if $P_G(s)$ is rational, then $P_n(s) = 1$ for almost all $n \in \mathbb{N}$; this would imply that $G/\operatorname{Frat} G$ is finite.

In the prosolvable case we used the Euler factorization $P_G(s) = \prod_p P_{G,p}(s)$, however $P_G(s)$ *admits an Euler factorization over the set of prime numbers if and only if* G *is prosolvable.*

Anyway, we can get a kind of Euler factorization over the finite simple groups by collecting together, for any simple group S, all the $P_n(s)$ such that the composition factors of G_n/G_{n+1} are isomorphic to S.

$$P_G(s) = \prod_S E_S(s), \text{ with } E_S(s) = \prod_{G_n/G_{n+1} \cong S^{r_n}} P_n(s)$$

In the prosolvable case $P_{G,p}(s) = E_{\mathbb{Z}_p}(s)$.

When we try to work with this generalized Euler factorization, we meet several problems:

♠ In the prosolvable case it is easy to prove that if $P_G(s)$ is rational, then $\pi(G)$ is finite and $P_{G,p}(s) = 1$ for all but finitely many primes. In the general case $\pi(G)$ is finite if and only if $E_S(s) = 1$ for almost all simple groups S; however none of these two equivalent facts can be easily deduced from the rationality of $P_G(s)$.

Let $\tilde{\pi}(G)$ be the set of primes p with the property that there exists $n \in \mathbb{N}$ divisible by p such that $b_n(G) \neq 0$.

If $P_G(s)$ is rational, then $\tilde{\pi}(G)$ is finite; the problem is that $\tilde{\pi}(G)$ could be smaller than $\pi(G)$. Recently it was proved:

Theorem (E. Damian, AL) *If G is finite, then $\pi(G) = \tilde{\pi}(G)$.*

Open problem: can this result be generalized to finitely generated profinite groups?

♠ Even if we know that $P_G(s) = \prod_S E_S(s)$ is the product of finitely many Euler factors $E_S(s)$, we cannot easily deduce, as in the pro-solvable case, that $P_G(s)$ rational implies $E_S(s)$ rational for each S.

♠ Let $\Omega_S = \{n \in \mathbb{N} \mid G_n/G_{n+1} \cong S^{r_n}\}$. Even if we know that $E_S(s) = \prod_{n \in \Omega_S} P_n(s)$ is rational, we cannot apply the same trick (the corollary of Skolem-Mahler-Lech Theorem) we used in the solvable case, because the series $P_n(s)$ are now more complicated and involve many non-trivial terms.

The problem is still open; the best result we were able to prove is:

Theorem (E. Detomi, AL) *Let G be a finitely generated profinite group in which almost every composition factor is cyclic or isomorphic to an alternating group. If $P_G(s)$ is rational, then $G/\operatorname{Frat} G$ is a finite group.*

Remark. The methods employed in the proof could probably be adapted to prove that the same conclusion holds if we assume that almost every composition factor is cyclic or is a group of Lie type over a fixed characteristic p. Roughly speaking, we are in big trouble if infinitely many composition factors belong to uncomparable families of simple groups!

Sketch of the proof

Notation. For any $n \in \mathbb{N}$, let $G_n/G_{n+1} = {S_n}^{r_n}$.

$I := \{i \in \mathbb{N} \mid S_i \cong \mathbb{Z}_{n_i}$ or $S_i \cong \mathsf{Alt}(n_i)\ \exists\ n_i \in \mathbb{N}\}$.

$$P_G(s) \text{ rational}$$
$$\Downarrow$$
$$P(s) = \prod_{i \in I} P_i(s) = \sum_{r \in \mathbb{N}} c_r / r^s \text{ rational}$$

First step. *The set $\pi(G)$ is finite.*

Since $P(s)$ is rational, there exists a prime u such $c_n = 0$ when n is divisible by a prime $q \geq u$.

We prove that $n_i < u$ for any $i \in I$

To deal with the case $S_i \cong \mathsf{Alt}(n_i)$, we need to understand how the properties of maximal subgroups of $\mathsf{Alt}(n_i)$ reflect on the distribution of the coefficients of the polynomial $P_i(s)$.

Second step. Let Ω_S be the set of n such that G_n/G_{n+1} is non-Frattini and isomorphic to a direct product of copies of S. *The set Ω_S is finite for any finite simple group S.*

Assume $\mathcal{T} = \{S \mid |\Omega_S| = \infty\} \neq \emptyset$.
Let $J = \{i \in I \mid S_i \in \mathcal{T}\}, \quad P_j(s) = \sum_l b_{j,l}/l^s$.

There exists $\mu \in \mathbb{N}$ such that:

- $\prod_{j \in J} \left(1 + \frac{b_{j,\mu^{r_j}}}{\mu^{r_j \cdot s}}\right)$ is rational
- $b_{j,\mu^{r_j}} \leq 0 \ \forall j \in J$
- $b_{j,\mu^{r_j}} < 0$ for infinitely many $j \in J$

By Skolem-Mahler-Lech Theorem:

for each prime u there exists $j \in J$ such that u divides the composition length r_j of G_j/G_{j+1}.

Hence for each prime u there exists r such that u divides r and G has either a transitive permutation representation of degree r or a linear irreducible representation of degree r over a finite field; this contradicts $\pi(G)$ finite.

Skolem-Mahler-Lech Theorem

If $\{a_0, a_1, ...\}$ is a recurrence sequence, then the set of all k such that $a_k = 0$ is the union of a finite (possibly empty) set and a finite number (possibly zero) of full arithmetical progressions, where a full arithmetic progression is a set of the form $\{r, r+d, r+2d, ...\}$ with $r \in [0, d)$.

Corollary

Let $c_1, \ldots, c_r, \lambda_1, \ldots, \lambda_r$ be algebraic numbers with the property that

$$\lambda_i/\lambda_j \text{ is a root of unit} \Rightarrow \lambda_i = \lambda_j.$$

Then the exponential polynomial

$$\psi(m) = c_1\lambda_1^m + \cdots + c_r\lambda_r^m$$

vanishes for infinitely many integers m only if $\psi(m)$ is identically zero.