The probabilistic zeta function of finite and profinite groups

Andrea Lucchini

Università di Padova

Intercity number theory seminar
September 3 2010, Leiden

G a finitely generated group

$a_n(G)$ the number of subgroups of index n in G

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

μ is the Möbius function of the subgroup lattice of G :

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

G a finitely generated group

$a_n(G)$ the number of subgroups of index n in G

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

μ is the Möbius function of the subgroup lattice of G :

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

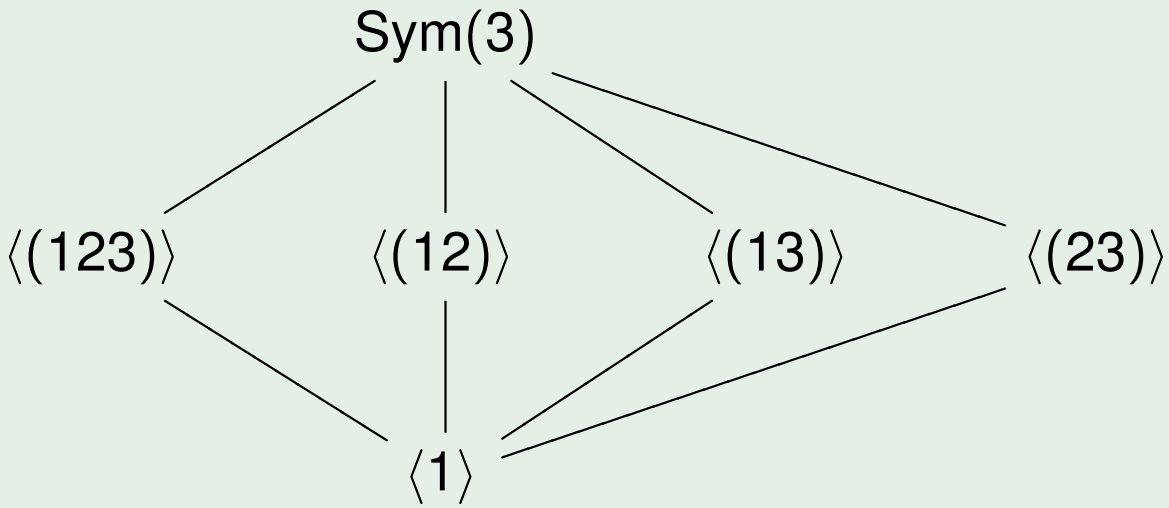
SUBGROUP ZETA FUNCTION

$$Z_G(s) = \sum_{n\in\mathbb{N}} \frac{a_n(G)}{n^s}$$

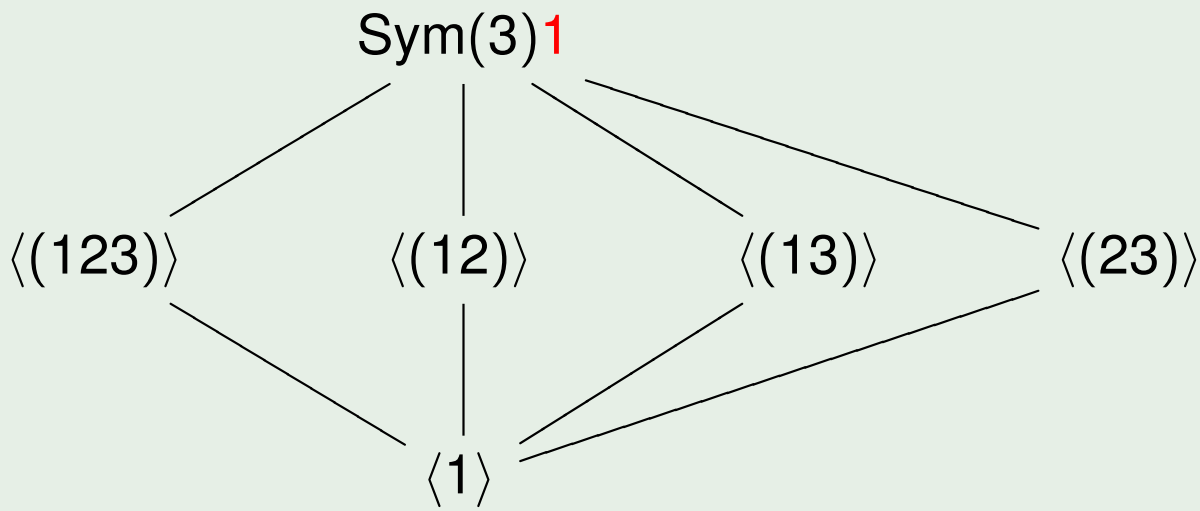
PROBABILISTIC ZETA FUNCTION

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

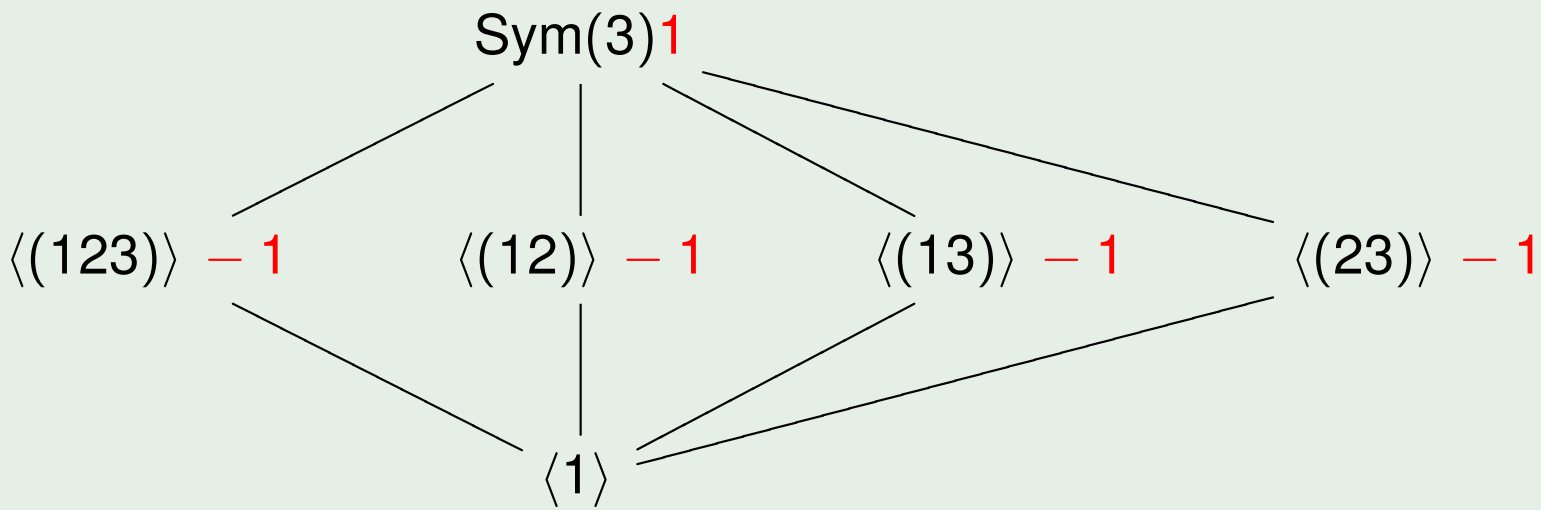
EXAMPLE: $G = \mathrm{Sym}(3)$



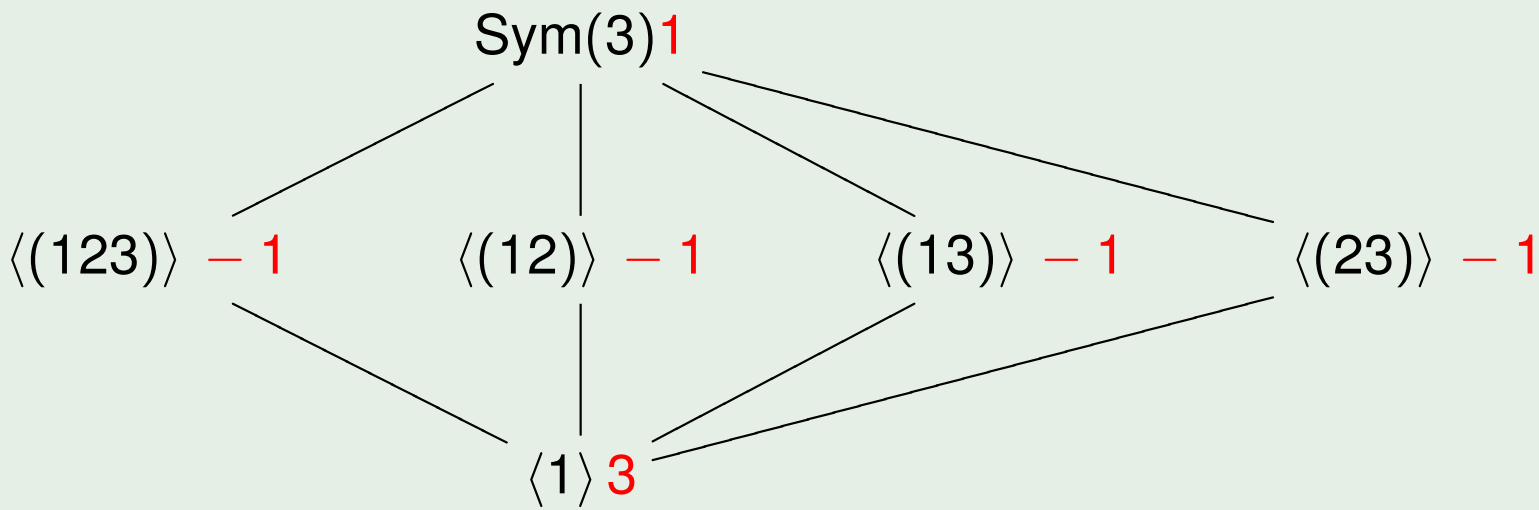
EXAMPLE: $G = \mathrm{Sym}(3)$



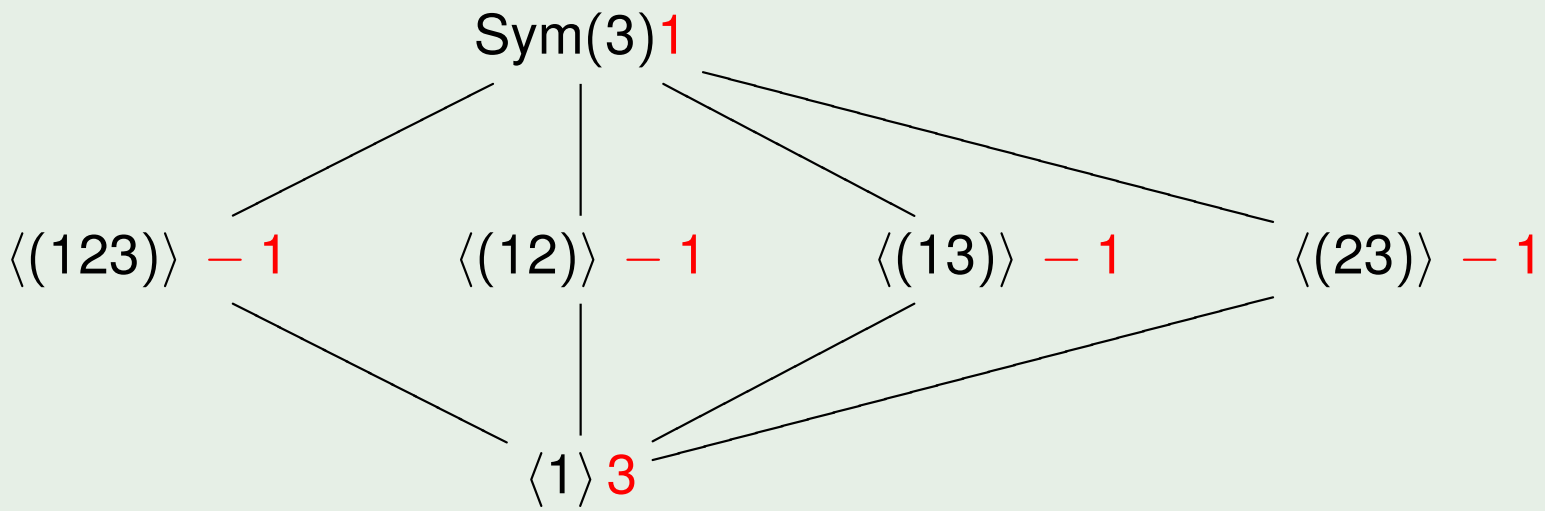
EXAMPLE: $G = \mathrm{Sym}(3)$



EXAMPLE: $G = \mathrm{Sym}(3)$

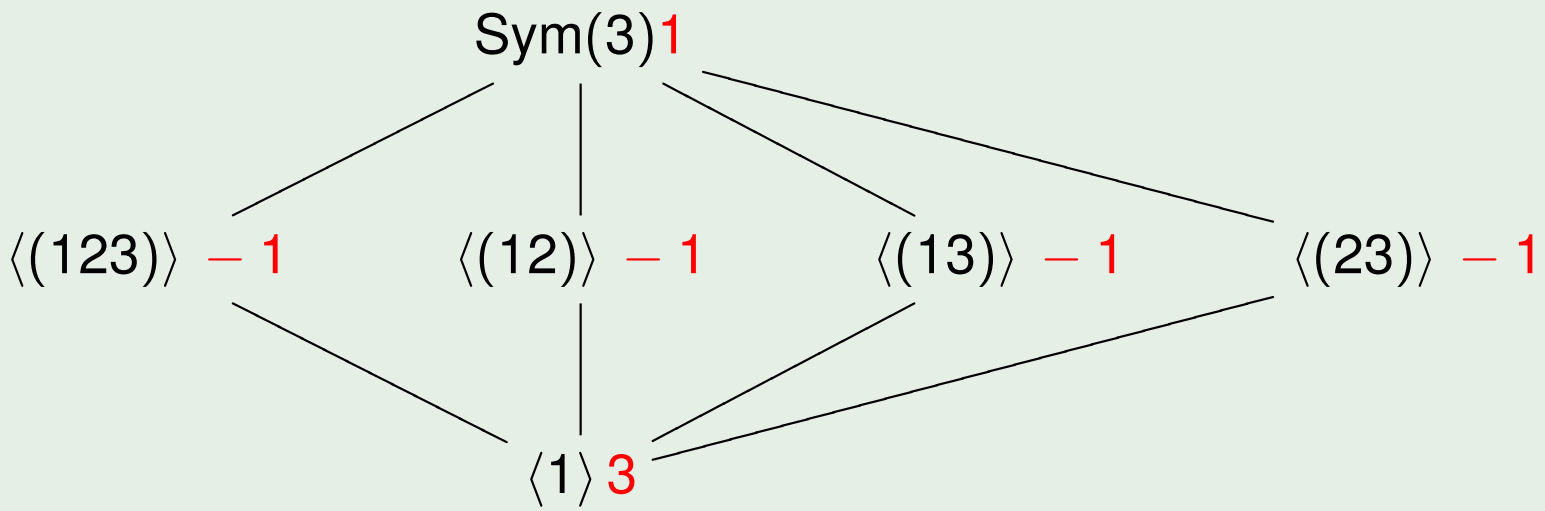


EXAMPLE: $G = \mathrm{Sym}(3)$



- $b_1(G) = \mu_G(G) = 1$
- $b_2(G) = \mu_G(\langle(1,2,3)\rangle) = -1$
- $b_3(G) = \mu_G(\langle(1,2)\rangle) + \mu_G(\langle(1,3)\rangle) + \mu_G(\langle(2,3)\rangle) = -3$
- $b_6(G) = \mu_G(1) = 3$

EXAMPLE: $G = \mathrm{Sym}(3)$



- $b_1(G) = \mu_G(G) = 1$
- $b_2(G) = \mu_G(\langle (1,2,3) \rangle) = -1$
- $b_3(G) = \mu_G(\langle (1,2) \rangle) + \mu_G(\langle (1,3) \rangle) + \mu_G(\langle (2,3) \rangle) = -3$
- $b_6(G) = \mu_G(1) = 3$

$$P_G(s) = 1 - \frac{1}{2^s} - \frac{3}{3^s} + \frac{3}{6^s} \qquad Z_G(s) = 1 + \frac{1}{2^s} + \frac{3}{3^s} + \frac{1}{6^s}$$

EXAMPLE: $G = \mathbb{Z}$

- $|\mathbb{Z} : H| = n \Rightarrow H = n\mathbb{Z}$
- $\mu_{\mathbb{Z}}(n\mathbb{Z}) = \mu(n)$

$$P_{\mathbb{Z}}(s) = \sum_{n \in \mathbb{N}} \frac{\mu(n)}{n^s} = \left(\sum_{n \in \mathbb{N}} \frac{1}{n^s} \right)^{-1} = (\zeta(s))^{-1} = (Z_{\mathbb{Z}}(s))^{-1}$$

EXAMPLE: $G = \mathbb{Z}$

- $|\mathbb{Z} : H| = n \Rightarrow H = n\mathbb{Z}$
- $\mu_{\mathbb{Z}}(n\mathbb{Z}) = \mu(n)$

$$P_{\mathbb{Z}}(s) = \sum_{n \in \mathbb{N}} \frac{\mu(n)}{n^s} = \left(\sum_{n \in \mathbb{N}} \frac{1}{n^s} \right)^{-1} = (\zeta(s))^{-1} = (Z_{\mathbb{Z}}(s))^{-1}$$

EXAMPLE: $G = \mathrm{Alt}(5)$

$$P_{\mathrm{Alt}(5)}(s) = 1 - \frac{5}{5^s} - \frac{6}{6^s} - \frac{10}{10^s} + \frac{20}{20^s} + \frac{60}{30^s} - \frac{60}{60^s}$$

REFERENCES

- N. Boston, A probabilistic generalization of the Riemann zeta function, Analytic number theory, Vol. 1, 155-162, Progr. Math., 138, Birkhäuser Boston, Boston, MA, 1996
- A. Mann, Positively finitely generated groups, Forum Math. 8 (1996), no. 4, 429-459
- K. Brown, The coset poset and probabilistic zeta function of a finite group, J. Algebra 225 (2000), no. 2, 989-1012.

REMARK

$\mu_G(H) \neq 0 \Rightarrow H$ *is an intersection of maximal subgroups of* G.

REMARK

$\mu_G(H) \neq 0 \Rightarrow H$ *is an intersection of maximal subgroups of* G.

The probabilistic zeta function $P_G(s)$ *depends only on the sublattice generated by the maximal subgroups of* G *and not on the complete subgroup lattice.*

REMARK

$\mu_G(H) \neq 0 \Rightarrow H$ is an intersection of maximal subgroups of G.

The probabilistic zeta function $P_G(s)$ depends only on the sublattice generated by the maximal subgroups of G and not on the complete subgroup lattice.

The maximal subgroups of $\mathbb{Z}$ are the subgroups $p\mathbb{Z}$, where p ranges over the set of all the prime numbers.

REMARK

$\mu_G(H) \neq 0 \Rightarrow H$ *is an intersection of maximal subgroups of* G.

The probabilistic zeta function $P_G(s)$ *depends only on the sublattice generated by the maximal subgroups of* G *and not on the complete subgroup lattice.*

The maximal subgroups of $\mathbb{Z}$ are the subgroups $p\mathbb{Z}$, where p ranges over the set of all the prime numbers.

The probabilistic zeta function encodes information about the lattice generated by the maximal subgroups of G, just as the Riemann zeta function encodes information about the primes.

REMARK

If $\widehat{G}$ is the profinite completion of G, then $P_G(s) = P_{\widehat{G}}(s)$

REMARK

If $\widehat{G}$ is the profinite completion of G, then $P_G(s) = P_{\widehat{G}}(s)$

We may restrict the study of the probabilistic zeta function to the case of finitely generated profinite groups.

This allows us:

- to employ properties of profinite groups;
- to find a probabilistic meaning of this object.

REMARK

If $\widehat{G}$ is the profinite completion of G, then $P_G(s) = P_{\widehat{G}}(s)$

We may restrict the study of the probabilistic zeta function to the case of finitely generated profinite groups.

This allows us:

- to employ properties of profinite groups;
- to find a probabilistic meaning of this object.

The Frattini subgroup $\mathrm{Frat}(G)$ of a profinite group G is the intersection of the (closed) maximal subgroups of G.

REMARK

If $\widehat{G}$ is the profinite completion of G, then $P_G(s) = P_{\widehat{G}}(s)$

We may restrict the study of the probabilistic zeta function to the case of finitely generated profinite groups.

This allows us:

- to employ properties of profinite groups;
- to find a probabilistic meaning of this object.

The Frattini subgroup $\mathrm{Frat}(G)$ of a profinite group G is the intersection of the (closed) maximal subgroups of G.

$$\mu_G(H) \neq 0 \Rightarrow \mathrm{Frat}(G) \leq H$$

$$\Downarrow$$

$$P_G(s) = P_{G/\mathrm{Frat}(G)}(s).$$

CONVERGENCE AND PROBABILISTIC MEANING

QUESTION

- What are the groups G for which $P_G(s)$ converges (absolutely) in some half complex plane?
- When $P_G(s)$ converges in a suitable complex plane, which information is given by the corresponding complex function? In particular, what is the meaning of the number $P_G(k)$, if k is a "large" positive integer?

THEOREM (P. HALL 1936)

If G is a finite group and $t \in \mathbb{N}$, then $P_G(t)$ is equal to the probability that a random t-tuple generates G.

THEOREM (P. HALL 1936)

If G is a finite group and $t \in \mathbb{N}$, then $P_G(t)$ is equal to the probability that a random t-tuple generates G.

PROOF.

It follows immediately from the Möbius inversion formula:

$$\sum_{H \leq G} P_H(t)|H|^t = |G|^t \quad \Rightarrow \quad \sum_{H \leq G} \mu_G(H)|H|^t = P_G(t)|G|^t.$$

□

THEOREM (P. HALL 1936)

If G is a finite group and $t \in \mathbb{N}$, then $P_G(t)$ is equal to the probability that a random t-tuple generates G.

EXAMPLE: $G = \mathrm{Alt}(5)$

- $P_G(1) = 0$ since G is not a cyclic group.
- $P_G(2) = \frac{19}{30}$: there are $3600 = 60^2$ ordered pairs $(x, y) \in G^2$ and $2280 = \frac{19 \cdot 3600}{30}$ of these satisfy the condition $\langle x, y \rangle = G$.

THEOREM (P. HALL 1936)

If G is a finite group and $t \in \mathbb{N}$, then $P_G(t)$ is equal to the probability that a random t-tuple generates G.

EXAMPLE: $G = \mathrm{Alt}(5)$

- $P_G(1) = 0$ since G is not a cyclic group.
- $P_G(2) = \frac{19}{30}$: there are $3600 = 60^2$ ordered pairs $(x, y) \in G^2$ and $2280 = \frac{19 \cdot 3600}{30}$ of these satisfy the condition $\langle x, y \rangle = G$.

REMARK

In 1998 Shareshian proved that if G is a finite nonabelian simple group, then $P_G(s)$ has a multiple zero at $s = 1$.

On a profinite group G, a normalized Haar measure ν is defined:

$$\mathrm{Prob}_G(k) = \nu(\{(x_1, \ldots, x_k) \in G^k \mid \langle x_1, \ldots, x_k \rangle = G\})$$

is the probability that k random elements generate G.

On a profinite group G, a normalized Haar measure ν is defined:

$$\mathrm{Prob}_G(k) = \nu(\{(x_1, \ldots, x_k) \in G^k \mid \langle x_1, \ldots, x_k \rangle = G\})$$

On a profinite group G, a normalized Haar measure ν is defined:

$$\mathrm{Prob}_G(k) = \nu(\{(x_1, \ldots, x_k) \in G^k \mid \langle x_1, \ldots, x_k \rangle = G\})$$

WARNING

G can be generated by k-elements $\not\Rightarrow \mathrm{Prob}_G(k) > 0$.

On a profinite group G, a normalized Haar measure ν is defined:

$$\mathrm{Prob}_G(k) = \nu(\{(x_1, \ldots, x_k) \in G^k \mid \langle x_1, \ldots, x_k \rangle = G\})$$

WARNING

G can be generated by k-elements $\not\Rightarrow \mathrm{Prob}_G(k) > 0$.

EXEMPLE (KANTOR,LUBOTZKY 1990)

$G = \prod_{n \geq \bar{n}} \mathrm{Alt}(n)^{n!/8}$ *is 2-generated but* $\mathrm{Prob}_G(k) = 0$ *for all* $k \in \mathbb{N}$.

On a profinite group G, a normalized Haar measure ν is defined:

$$\mathrm{Prob}_G(k) = \nu(\{(x_1, \ldots, x_k) \in G^k \mid \langle x_1, \ldots, x_k \rangle = G\})$$

WARNING

G can be generated by k-elements $\not\Rightarrow \mathrm{Prob}_G(k) > 0$.

EXEMPLE (KANTOR,LUBOTZKY 1990)

$G = \prod_{n \geq \bar{n}} \mathrm{Alt}(n)^{n!/8}$ *is 2-generated but* $\mathrm{Prob}_G(k) = 0$ *for all* $k \in \mathbb{N}$.

DEFINITION

G is Positively Finitely Generated when $\mathrm{Prob}_G(k) > 0$ for some $k \in \mathbb{N}$.

On a profinite group G, a normalized Haar measure ν is defined:

$$\mathrm{Prob}_G(k) = \nu(\{(x_1, \ldots, x_k) \in G^k \mid \langle x_1, \ldots, x_k \rangle = G\})$$

WARNING

G can be generated by k-elements $\not\Rightarrow \mathrm{Prob}_G(k) > 0$.

EXEMPLE (KANTOR,LUBOTZKY 1990)

$G = \prod_{n \geq \bar{n}} \mathrm{Alt}(n)^{n!/8}$ *is 2-generated but* $\mathrm{Prob}_G(k) = 0$ *for all* $k \in \mathbb{N}$.

DEFINITION

G is Positively Finitely Generated when $\mathrm{Prob}_G(k) > 0$ for some $k \in \mathbb{N}$.

THEOREM (MANN, SHALEV 1996)

G is PFG $\Leftrightarrow$ G has Polinomial Maximal Subgroup Growth (the number of maximal subgroups of index n is at most some given power of n).

CONJECTURE A (MANN 1996)

If G is a PFG group, then the function $\mathrm{Prob}_G(k)$ can be interpolated in a natural way to an analytic function defined for all s in some right half-plane of the complex plane.

CONJECTURE B (MANN 2004)

Let G be a PFG group. Then the infinite sum

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

converges absolutely in some right half plane.

CONJECTURE A (MANN 1996)

If G is a PFG group, then the function $\mathrm{Prob}_G(k)$ can be interpolated in a natural way to an analytic function defined for all s in some right half-plane of the complex plane.

CONJECTURE B (MANN 2004)

Let G be a PFG group. Then the infinite sum

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

converges absolutely in some right half plane.

If Conjecture B holds, then $P_G(s)$ is absolutely convergent in a suitable half complex plane and $P_G(k) = \mathrm{Prob}_G(s)$ if $k \in \mathbb{N}$ is large enough.

Conjecture B have been proved in the following particular cases:

- G is a finitely generated prosolvable group (AL 2007);

Conjecture B have been proved in the following particular cases:

- G is a finitely generated prosolvable group (AL 2007);
  for example, if $G = \widehat{\mathbb{Z}}$, then
  - G is procyclic but $P_G(1) = 0$,
  - $P_G(2) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$ is "the probability that two integers are coprime".

Conjecture B have been proved in the following particular cases:

- G is a finitely generated prosolvable group (AL 2007);
- G has polynomial subgroup growth (AL 2009);

Conjecture B have been proved in the following particular cases:

- G is a finitely generated prosolvable group (AL 2007);
- G has polynomial subgroup growth (AL 2009);
- G is an adelic group (a closed subgroup of $\mathrm{SL}(m, \hat{\mathbb{Z}})$) (AL 2009);

Conjecture B have been proved in the following particular cases:

- G is a finitely generated prosolvable group (AL 2007);
- G has polynomial subgroup growth (AL 2009);
- G is an adelic group (a closed subgroup of $\mathrm{SL}(m, \hat{\mathbb{Z}})$) (AL 2009);
- all the nonabelian composition factors of G are alternating groups (V. Colombo AL 2010).

A REDUCTION THEOREM, AL 2010

Conjecture B holds if the following is true:

CONJECTURE

There exists a constant γ such that for each finite almost simple group X ($S \leq X \leq \mathrm{Aut}\, S$ for some finite nonabelian simple group S) we have:

- $|\mu_X(Y)| \leq |X : Y|^\gamma$ *for each* $Y \leq X$.
- *for each* $n \in \mathbb{N}$, X *contains at most* n^γ *subgroups* Y *with index* n *and* $\mu_X(Y) \neq 0$.

A REDUCTION THEOREM, AL 2010

Conjecture B holds if the following is true:

CONJECTURE

There exists a constant γ such that for each finite almost simple group X ($S \leq X \leq \mathrm{Aut}\, S$ for some finite nonabelian simple group S) we have:

- $|\mu_X(Y)| \leq |X : Y|^\gamma$ *for each* $Y \leq X$.
- *for each* $n \in \mathbb{N}$, X *contains at most* n^γ *subgroups* Y *with index* n *and* $\mu_X(Y) \neq 0$.

V.COLOMBO AL 2010

The previous conjecture holds if X is an alternating or symmetric group.

EULER FACTORIZATION ?

- If G is a finite group, then $P_G(s)$ belongs to the rings $\mathcal{R}$ of the finite Dirichlet series (Dirichlet polynomials) with integer coefficients.
- $\mathcal{R}$ is a unique factorization domain and it is interesting to study how $P_G(s)$ factorizes in this ring.
- Let $N \trianglelefteq G$ be a normal subgroup of G. To the factor group G/N the Dirichlet series $P_{G/N}(s)$ is associated. How are the two series $P_G(s)$ and $P_{G/N}(s)$ related ?

EXEMPLE

$G = \mathrm{Sym}(3)$, $N = \langle (1,2,3) \rangle$.

$$P_G(s) = 1 - \frac{1}{2^s} - \frac{3}{3^s} + \frac{3}{6^s} \qquad P_{G/N}(s) = 1 - \frac{1}{2^s}$$

$P_{G/N}(s)$ *divides* $P_G(s)$; *indeed* $P_G(s) = P_{G/N}(s)\left(1 - \frac{3}{3^s}\right)$.

This "good behavior" of the series $P_G(s)$ and $P_{G/N}(s)$ holds for any finite group G and any normal subgroup N:

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

with $P_{G,N}(s) = \sum \frac{b_n(G,N)}{n^s}$ and $b_n(G,N) = \sum_{\substack{|G:H|=n \\ HN=G}} \mu_G(H)$

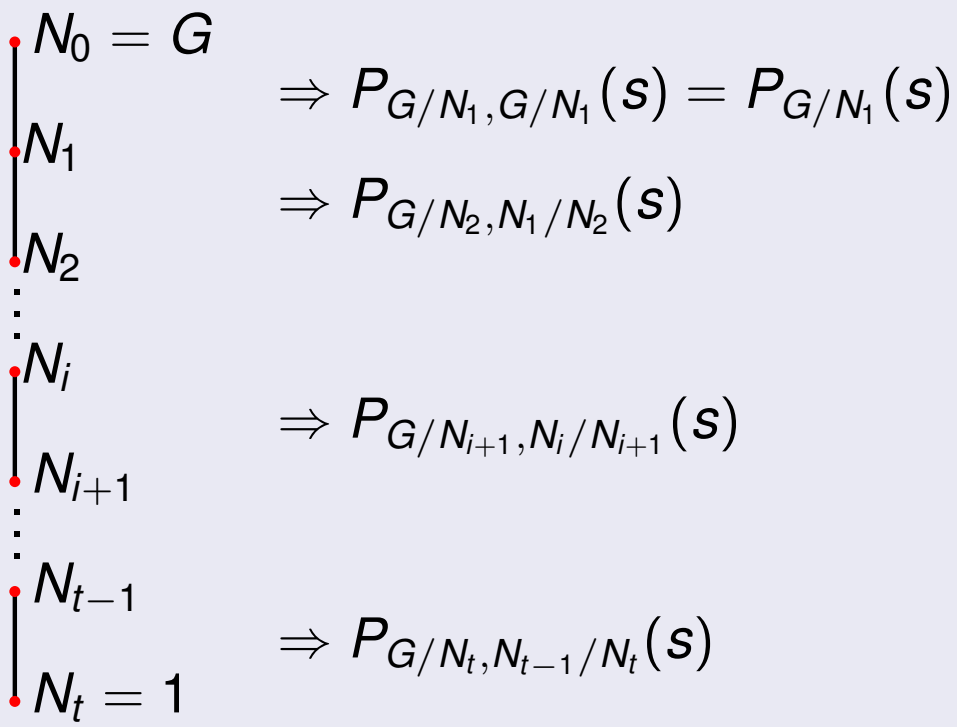
This "good behavior" of the series $P_G(s)$ and $P_{G/N}(s)$ holds for any finite group G and any normal subgroup N:

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

with $P_{G,N}(s) = \sum \frac{b_n(G,N)}{n^s}$ and $b_n(G,N) = \sum_{\substack{|G:H|=n \\ HN=G}} \mu_G(H)$

If G/N can be generated by k elements, then $P_{G,N}(k)$ is the conditional probability that k elements $g_1, \ldots, g_k$ generate G, given that $\langle g_1, \ldots, g_k \rangle N = G$.

Assume that $1 = N_t \trianglelefteq \cdots \trianglelefteq N_0 = G$ is a normal series of G.



$$P_G(s) = \prod_i P_{G/N_{i+1}, N_i/N_{i+1}}(s)$$

CHIEF SERIES

A finitely generated profinite group G possesses a chain of open normal subgroups

$$G = N_0 \trianglerighteq N_1 \trianglerighteq \dots N_i \trianglerighteq \dots$$

such that

- $\bigcap_i N_i = 1$
- N_i/N_{i+1} is a minimal normal subgroup of G/N_{i+1}.

For each i, the Dirichlrt series $P_i(s) = P_{G/N_{i+1},N_i/N_{i+1}}(s)$ is finite and

$$\boxed{P_G(s) = \prod_i P_i(s)}$$

CHIEF SERIES

A finitely generated profinite group G possesses a chain of open normal subgroups

$$G = N_0 \trianglerighteq N_1 \trianglerighteq \dots N_i \trianglerighteq \dots$$

such that

- $\bigcap_i N_i = 1$
- N_i/N_{i+1} is a minimal normal subgroup of G/N_{i+1}.

For each i, the Dirichlrt series $P_i(s) = P_{G/N_{i+1},N_i/N_{i+1}}(s)$ is finite and

$$\boxed{P_G(s) = \prod_i P_i(s)}$$

This infinite formal product can be computed since for each i we have $P_i(s) = 1 + \frac{a_i}{m_i^s} + \dots$ and for each $n > 1$ there exist only finitely many indices i with $m_i \leq n$.

CHIEF SERIES

A finitely generated profinite group G possesses a chain of open normal subgroups

$$G = N_0 \trianglerighteq N_1 \trianglerighteq \dots N_i \trianglerighteq \dots$$

such that

- $\bigcap_i N_i = 1$
- N_i/N_{i+1} is a minimal normal subgroup of G/N_{i+1}.

For each i, the Dirichlrt series $P_i(s) = P_{G/N_{i+1}, N_i/N_{i+1}}(s)$ is finite and

$$\boxed{P_G(s) = \prod_i P_i(s)}$$

THEOREM (E DETOMI, AL 2005)

The family of the Dirichlet polynomials $\{P_i(s)\}_i$ does not depend on the choice of the chief series.

We need some technical details to describe how the Dirichlet series $P_i(s)$ can be computed.

We say that $A = X/Y$ is a chief factor of the profinite group G if $Y \leq X$ are open normal subgroups of G and X/Y is a minimal normal subgroup of G/X.

DEFINITION

Two chief factors A and B of G are G-equivalent ($A \sim_G B$) if either $A \cong_G B$ or there exists an open normal subgroup K of G such that G/K is a primitive permutation group (there exists a maximal subgroup M of G containing K and K is the largest normal subgroup of G contained in M) with two different normal subgroups N_1 and N_2 and $A \cong_G N_1$, $B \cong_G N_2$.

Two abelian chief factors are G-equivalent if and only if they are G-isomorphic, but for nonabelian chief factors G-equivalence is strictly weaker than G-isomorphism. For example the two direct factors of $G = \mathrm{Alt}(5) \times \mathrm{Alt}(5)$ are G-equivalent but not G-isomorphic.

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y, X/Y}(s)$.

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y,X/Y}(s)$.
- We say that A is a Frattini chief factor of G if $X/Y \leq \mathrm{Frat}(G/Y)$. If A is a Frattini chief factor of G, then $Q(s) = 1$.

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y,X/Y}(s)$.
- The monolithic primitive group associated with A is defined as

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y,X/Y}(s)$.
- The monolithic primitive group associated with A is defined as

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

- If A is non-Frattini, then L_A is an epimorphic image of G.

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y,X/Y}(s)$.
- The monolithic primitive group associated with A is defined as

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

- L_A has a unique minimal normal subgroup, say N, and $N \cong A$.

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y,X/Y}(s)$.
- The monolithic primitive group associated with A is defined as

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

- L_A has a unique minimal normal subgroup, say N, and $N \cong A$.

$$\widetilde{P}_{L_A,1}(s) := P_{L_A,N}(s), \quad \widetilde{P}_{L_A,i}(s) := P_{L_A,N}(s) - \frac{(1 + q + \cdots + q^{i-2})\gamma}{|N|^s}$$

with $\gamma = |C_{\mathrm{Aut}\, N}(L_A/N)|$ and $q = \begin{cases} |\mathrm{End}_L N| & \text{if } N \text{ is abelian,} \\ 1 & \text{otherwise.} \end{cases}$

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y,X/Y}(s)$.
- The monolithic primitive group associated with A is defined as

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

- L_A has a unique minimal normal subgroup, say N, and $N \cong A$.

$$\widetilde{P}_{L_A,1}(s) := P_{L_A,N}(s), \quad \widetilde{P}_{L_A,i}(s) := P_{L_A,N}(s) - \frac{(1 + q + \cdots + q^{i-2})\gamma}{|N|^s}$$

with $\gamma = |C_{\mathrm{Aut}\, N}(L_A/N)|$ and $q = \begin{cases} |\mathrm{End}_L N| & \text{if } N \text{ is abelian,} \\ 1 & \text{otherwise.} \end{cases}$

$Q(s) = \widetilde{P}_{L_A,t}(s)$, with t the number of non-Frattini factors G-equivalent to A in a chief series of G/Y.

- Let $A = X/Y$ be a chief factor of G and let $Q(s) := P_{G/Y,X/Y}(s)$.
- The monolithic primitive group associated with A is defined as

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

- L_A has a unique minimal normal subgroup, say N, and $N \cong A$.

$$\widetilde{P}_{L_A,1}(s) := P_{L_A,N}(s), \quad \widetilde{P}_{L_A,i}(s) := P_{L_A,N}(s) - \frac{(1 + q + \cdots + q^{i-2})\gamma}{|N|^s}$$

with $\gamma = |C_{\mathrm{Aut}\, N}(L_A/N)|$ and $q = \begin{cases} |\mathrm{End}_L N| & \text{if } N \text{ is abelian,} \\ 1 & \text{otherwise.} \end{cases}$

$A = X/Y \cong S^r$ with S a finite simple group and $r \in \mathbb{N}$;

- If A is abelian, then $Q(s) = 1 - c/q^s$ where c is the number of complements of X/Y in G/Y.
- If A is non abelian, then there exists K with $S \trianglelefteq K \leq \mathrm{Aut}\, S$ such that $Q(s)$ is "approximated" by $P_{K,S}(rs - r + 1)$.

$G = C_p \times C_p$

Let $N \cong C_p$ be a minimal normal subgroup of G.

- $G/N \cong C_p \Rightarrow P_{G/N}(s) = 1 - 1/p^s$.
- N has complements in $G \Rightarrow P_{G,N}(s) = 1 - p/p^s$.

Hence $P(s) = (1 - 1/p^s)(1 - p/p^s)$.

$G = \mathrm{Alt}(5) \times \mathrm{Alt}(5)$

$$\left(1-\frac{5}{5^s}-\frac{6}{6^s}-\frac{10}{10^s}+\frac{20}{20^s}+\frac{60}{30^s}-\frac{60}{60^s}\right)\left(1-\frac{5}{5^s}-\frac{6}{6^s}-\frac{10}{10^s}+\frac{20}{20^s}+\frac{60}{30^s}-\frac{180}{60^s}\right)$$

$G = \mathrm{Alt}(5) \wr C_2$

The wreath product $G = \mathrm{Alt}(5) \wr C_2$ has a unique minimal normal subgroup $N \cong \mathrm{Alt}(5) \times \mathrm{Alt}(5)$.

$$P_{G,N}(s) = 1 - \frac{25}{25^s} - \frac{36}{36^s} - \frac{120}{60^s} - \frac{100}{100^s} + \frac{600}{300^s} + \frac{720}{360^s} + \frac{400}{400^s} + \frac{1200}{600^s} + \frac{1800}{900^s} - \frac{2400}{1200^s} - \frac{7200}{1800^s} + \frac{3600}{3600^s}$$

can be approximated by

$$P_{\mathrm{Alt}(5)}(2s-1) = 1 - \frac{25}{25^s} - \frac{36}{36^s} - \frac{100}{100^s} + \frac{400}{400^s} + \frac{1800}{900^s} - \frac{3600}{3600^s}$$

Let G be a finitely generated profinite group and let A be a chief factor of G. The number $\delta_G(A)$ of non-Frattini factors in a chief series that are G-equivalent to A is finite and independent on the choice of the chief series.

$$P_G(s) = \prod_A \left(\prod_{1 \leq i \leq \delta_G(A)} \widetilde{P}_{L_A,i}(s) \right)$$

where A runs over a set of representatives of the equivalence classes of non-Frattini chief factors of G.

- Let $\mathcal{A}$ be a set of representatives for the G-equivalence classes of chief factors of G.
- For each simple group T, let $\mathcal{A}_T := \{A \in \mathcal{A} \mid A \cong T^r \ \exists t \in \mathbb{N}\}$.
- Define

$$P_G^T(s) = \prod_{A \in \mathcal{A}_T} \left(\prod_{1 \leq i \leq \delta_G(A)} \widetilde{P}_{L_A,i}(s) \right)$$

We get an Euler factorization indexed over the finite simple groups:

$$\boxed{P_G(s) = \prod_T P_G^T(s)}$$

Assume that G is prosolvable:

- $\mathcal{A}_T \neq \emptyset \Rightarrow T \cong C_p$, a cyclic group of order p, for a suitable p;
- for each prime p we have $P_G^{C_p}(s) = P_{G,p}(S) = \sum_m \frac{b_{p^m}(G)}{p^{ms}}$.

$$\Downarrow$$

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

Assume that G is prosolvable:

- $\mathcal{A}_T \neq \emptyset \Rightarrow T \cong C_p$, a cyclic group of order p, for a suitable p;
- for each prime p we have $P_G^{C_p}(s) = P_{G,p}(S) = \sum_m \frac{b_{p^m}(G)}{p^{ms}}$.

$$\Downarrow$$

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

EXAMPLE: $G = \mathrm{Sym}(4)$

$$1 \trianglelefteq K \cong C_2 \times C_2 \trianglelefteq \mathrm{Alt}(4) \trianglelefteq \mathrm{Sym}(4)$$

$$\begin{aligned} P_G(s) &= \left(1 - \frac{1}{2^s}\right)\left(1 - \frac{3}{3^s}\right)\left(1 - \frac{4}{4^s}\right) \\ &= \left(1 - \frac{1}{2^s} - \frac{4}{4^s} + \frac{4}{8^s}\right)\left(1 - \frac{3}{3^s}\right) \\ &= 1 - \frac{1}{2^s} - \frac{3}{3^s} - \frac{4}{4^s} + \frac{3}{6^s} + \frac{4}{8^s} + \frac{12}{12^s} - \frac{12}{24^s} \end{aligned}$$

Assume that G is prosolvable:

- $\mathcal{A}_T \neq \emptyset \Rightarrow T \cong C_p$, a cyclic group of order p, for a suitable p;
- for each prime p we have $P_G^{C_p}(s) = P_{G,p}(S) = \sum_m \frac{b_{p^m}(G)}{p^{ms}}$.

$$\Downarrow$$

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

THEOREM (DETOMI, AL 2004)

The following are equivalent:

- *G is prosolvable;*
- *$P_G(s) = \prod_p P_{G,p}(s)$;*
- *The sequence $\{b_n(G)\}_{n\in\mathbb{N}}$ is multiplicative.*

ABOUT THE PROOF

Assume that $P_G(s) = \prod_i P_i(s)$ is multiplicative, with $P_i(s)$ the Dirichlet polynomial associated to the chief factor N_i/N_{i+1}.

- If G is finite, then $P_i(s)$ is multiplicative for each $i \in I$. But if N_i/N_{i+1} is non abelian, then $P_i(s)$ cannot be multiplicative (this follows easily by a result proved by Guralnick: $\mathrm{PSL}(2,7)$ is the unique simple group which has subgroups of two different prime power indices).
- If G is infinite, then the infinite product $P_G(s) = \prod_i P_i(s)$ can be multiplicative even if the factors $P_i(s)$ are not multiplicative. For this reason the proof is much more complicate.

APPLICATIONS - GENERATION

QUESTION

How many random elements must be taken in a finite group G to have a "good" probability of generating G with these elements?

THEOREM (DETOMI, AL 2004)

Given a real number $0 < \alpha < 1$, *there exists a constant* c_α *such that for any finite group* G

$$P_G([d(G) + c_\alpha(1 + \log \lambda(G))]) \geq \alpha,$$

where $d(G)$ *is the minimal number of generators for* G *and* $\lambda(G)$ *denotes the number of non-Frattini factors in a chief series of* G.

COROLLARY

If n *is large enough, then* $[n/2]$ *randomly chosen elements of a permutation group* G *of degree* n *almost certainly generate* G.

APPLICATIONS - THE COSET POSET

DEFINITION (S. BOUC - K. BROWN)

The coset poset $\mathcal{C}(G)$ associated to a finite group G is the poset consisting of the proper (right) cosets Hx, with $H < G$ and $x \in G$, ordered by inclusion.

$$Hx \subseteq Ky \iff H \leq K \text{ and } Ky = Kx.$$

We can apply topological concepts to this poset by using the simplicial complex $\Delta = \Delta(\mathcal{C}(G))$ whose simplices are the finite chains $H_1g_1 < H_2g_2 < \ldots < H_ng_n$ of elements of $\mathcal{C}(G)$.

In particular, we can speak of the Euler characteristic of $\mathcal{C}(G)$

$$\chi(\mathcal{C}(G)) := \sum_m (-1)^m \alpha_m$$

where α_m is the number of chains in $\mathcal{C}(G)$ of length m

and we can speak of the reduced Euler characteristic of $\mathcal{C}(G)$

$$\tilde{\chi}(\mathcal{C}(G)) := \chi(\mathcal{C}(G)) - 1.$$

$\tilde{\chi}(\mathcal{C}(G)) \neq 0 \Rightarrow$ the simplicial complex $\Delta(\mathcal{C}(G))$ is not contractible.

BOUC, BROWN 2000

$$\tilde{\chi}(\mathcal{C}(G)) = -P_G(-1).$$

CONJECTURE (BROWN, 2000)

Let G be a finite group. Then $P_G(-1) \neq 0$, hence the simplicial complex associated to the coset poset of G is non-contractible.

BOUC, BROWN 2000

$$\tilde{\chi}(\mathcal{C}(G)) = -P_G(-1).$$

CONJECTURE (BROWN, 2000)

Let G be a finite group. Then $P_G(-1) \neq 0$, hence the simplicial complex associated to the coset poset of G is non-contractible.

EVIDENCES FOR THE CONJECTURE

1. $P_G(-1) \neq 0$ for all the finite groups for which $P_G(-1)$ have been computed by GAP.

BOUC, BROWN 2000

$$\tilde{\chi}(\mathcal{C}(G)) = -P_G(-1).$$

CONJECTURE (BROWN, 2000)

Let G be a finite group. Then $P_G(-1) \neq 0$, hence the simplicial complex associated to the coset poset of G is non-contractible.

EVIDENCES FOR THE CONJECTURE

1. $P_G(-1) \neq 0$ for all the finite groups for which $P_G(-1)$ have been computed by GAP.
2. (K. Brown - 2000) True for solvable groups.

BOUC, BROWN 2000

$$\tilde{\chi}(\mathcal{C}(G)) = -P_G(-1).$$

CONJECTURE (BROWN, 2000)

Let G be a finite group. Then $P_G(-1) \neq 0$, hence the simplicial complex associated to the coset poset of G is non-contractible.

EVIDENCES FOR THE CONJECTURE

1. $P_G(-1) \neq 0$ for all the finite groups for which $P_G(-1)$ have been computed by GAP.
2. (K. Brown - 2000) True for solvable groups.

$$P_G(s) = \prod_i (1 - c_i/q_i^s) \text{ with } c_i \geq 0 \Rightarrow P_G(-1) = \prod_i (1 - c_i q_i) \neq 0.$$

BOUC, BROWN 2000

$$\tilde{\chi}(\mathcal{C}(G)) = -P_G(-1).$$

CONJECTURE (BROWN, 2000)

Let G be a finite group. Then $P_G(-1) \neq 0$, hence the simplicial complex associated to the coset poset of G is non-contractible.

EVIDENCES FOR THE CONJECTURE

1. $P_G(-1) \neq 0$ for all the finite groups for which $P_G(-1)$ have been computed by GAP.
2. (K. Brown - 2000) True for solvable groups.
3. (M. Patassini - 2008) True for $PSL(2, q)$, ${}^2B_2(q)$, ${}^2G_2(q)$.

BOUC, BROWN 2000

$$\tilde{\chi}(\mathcal{C}(G)) = -P_G(-1).$$

CONJECTURE (BROWN, 2000)

Let G be a finite group. Then $P_G(-1) \neq 0$, hence the simplicial complex associated to the coset poset of G is non-contractible.

EVIDENCES FOR THE CONJECTURE

1. $P_G(-1) \neq 0$ for all the finite groups for which $P_G(-1)$ have been computed by GAP.
2. (K. Brown - 2000) True for solvable groups.
3. (M. Patassini - 2008) True for $PSL(2, q)$, ${}^2B_2(q)$, ${}^2G_2(q)$.
4. (M. Patassini - 2009) True for classical groups.

$P_G(s)$ WHEN G IS A FINITE GROUP

Some properties of G can be recognized from $P_G(s)$:

DETOMI - AL G solvable $\Leftrightarrow$ $P_G(s)$ multiplicative
(i.e. $(n, m) = 1 \Rightarrow b_{nm}(G) = b_n(G)b_m(G)$).

$P_G(s)$ WHEN G IS A FINITE GROUP

Some properties of G can be recognized from $P_G(s)$:

DETOMI - AL G solvable $\Leftrightarrow$ $P_G(s)$ multiplicative
(i.e. $(n, m) = 1 \Rightarrow b_{nm}(G) = b_n(G)b_m(G)$).

DAMIAN - AL G p-solvable $\Leftrightarrow$ $P_G(s)$ p-multiplicative
(i.e. $(p, m) = 1 \Rightarrow b_{p^r m}(G) = b_{p^r}(G)b_m(G)$).

$P_G(s)$ WHEN G IS A FINITE GROUP

Some properties of G can be recognized from $P_G(s)$:

DETOMI - AL G solvable $\Leftrightarrow$ $P_G(s)$ multiplicative
(i.e. $(n, m) = 1 \Rightarrow b_{nm}(G) = b_n(G)b_m(G)$).

DAMIAN - AL G p-solvable $\Leftrightarrow$ $P_G(s)$ p-multiplicative
(i.e. $(p, m) = 1 \Rightarrow b_{p^r m}(G) = b_{p^r}(G)b_m(G)$).

DAMIAN - AL The set of the prime divisors of $|G|$ coincides with the set of the primes p such that p divides m for some m with $b_m(G) \neq 0$.

$P_G(s)$ WHEN G IS A FINITE GROUP

Some properties of G can be recognized from $P_G(s)$:

DETOMI - AL G solvable $\Leftrightarrow$ $P_G(s)$ multiplicative
(i.e. $(n, m) = 1 \Rightarrow b_{nm}(G) = b_n(G)b_m(G)$).

DAMIAN - AL G p-solvable $\Leftrightarrow$ $P_G(s)$ p-multiplicative
(i.e. $(p, m) = 1 \Rightarrow b_{p^r m}(G) = b_{p^r}(G)b_m(G)$).

DAMIAN - AL The set of the prime divisors of $|G|$ coincides with the set of the primes p such that p divides m for some m with $b_m(G) \neq 0$.

MASSA - AL G perfect $\Leftrightarrow$ n divides $b_n(G)$ per each $n \in \mathbb{N}$.

$P_G(s)$ WHEN G IS A FINITE GROUP

Some properties of G can be recognized from $P_G(s)$:

DETOMI - AL G solvable $\Leftrightarrow$ $P_G(s)$ multiplicative
(i.e. $(n, m) = 1 \Rightarrow b_{nm}(G) = b_n(G)b_m(G)$).

DAMIAN - AL G p-solvable $\Leftrightarrow$ $P_G(s)$ p-multiplicative
(i.e. $(p, m) = 1 \Rightarrow b_{p^r m}(G) = b_{p^r}(G)b_m(G)$).

DAMIAN - AL The set of the prime divisors of $|G|$ coincides with the set of the primes p such that p divides m for some m with $b_m(G) \neq 0$.

MASSA - AL G perfect $\Leftrightarrow$ n divides $b_n(G)$ per each $n \in \mathbb{N}$.

DAMIAN - MASSA - AL From the series $P_G(s)$, we can deduce whether $G/\operatorname{Frat} G$ is a simple group.

THEOREM

Let G be a finite group and let $m = \min\{n > 1 \mid b_n(G) \neq 0\}$. The factor group $G/\operatorname{Frat} G$ is simple and nonabelian if and only if the following conditions are satisfied:

- *if $b_n(G) \neq 0$, then n divides $m!$;*
- *if $q = p^r$ is a prime power and $b_q(G) \neq 0$, then either $b_q(G) \equiv 0 \bmod p$ and $q = m$ or $(q, m) = (8, 7)$;*
- $\prod_{n \text{ dispari}} n^{\frac{b_n(G)}{n}} \neq 1$.

THEOREM

Let G be a finite group and let $m = \min\{n > 1 \mid b_n(G) \neq 0\}$. The factor group $G/\operatorname{Frat} G$ is simple and nonabelian if and only if the following conditions are satisfied:

- *if $b_n(G) \neq 0$, then n divides $m!$;*
- *if $q = p^r$ is a prime power and $b_q(G) \neq 0$, then either $b_q(G) \equiv 0 \mod p$ and $q = m$ or $(q, m) = (8, 7)$;*
- $\prod_{n \text{ dispari}} n^{\frac{b_n(G)}{n}} \neq 1$.

The third condition is equivalent to say that 1 is a simple zero of the function $\sum_{n \text{ odd}} b_n(G)/n^s$.

THEOREM

Let G be a finite group and let $m = \min\{n > 1 \mid b_n(G) \neq 0\}$. The factor group $G/\operatorname{Frat} G$ is simple and nonabelian if and only if the following conditions are satisfied:

- *if $b_n(G) \neq 0$, then n divides $m!$;*
- *if $q = p^r$ is a prime power and $b_q(G) \neq 0$, then either $b_q(G) \equiv 0 \bmod p$ and $q = m$ or $(q, m) = (8, 7)$;*
- $\prod_{n \text{ dispari}} n^{\frac{b_n(G)}{n}} \neq 1$.

The third condition is equivalent to say that 1 is a simple zero of the function $\sum_{n \text{ odd}} b_n(G)/n^s$.

THEOREM (DAMIAN, PATASSINI, AL)

Let G_1 and G_2 be two finite groups with $P_{G_1}(s) = P_{G_2}(s)$. If G_1 is a simple group, then $G_2/\operatorname{Frat} G_2 \cong G_1$.

IRREDUCIBILITY OF $P_G(s)$

We have seen that for any non-Frattini normal subgroup of G, the Dirichlet polynomial $P_G(s)$ admits a corresponding non trivial factorization.

- Do there exist examples of groups G such that $P_G(s)$ has a non trivial factorization which does not come from normal subgroups?
- In particular is $P_G(s)$ irreducible in $\mathcal{R}$ when G is a simple group?

IRREDUCIBILITY OF $P_G(s)$

We have seen that for any non-Frattini normal subgroup of G, the Dirichlet polynomial $P_G(s)$ admits a corresponding non trivial factorization.

- Do there exist examples of groups G such that $P_G(s)$ has a non trivial factorization which does not come from normal subgroups?
- In particular is $P_G(s)$ irreducible in $\mathcal{R}$ when G is a simple group?

THE SECOND QUESTION HAS A NEGATIVE ANSWER

$$P_{\mathrm{PSL}(2,7)}(s) = 1 - \frac{14}{7^s} - \frac{8}{8^s} + \frac{21}{21^s} + \frac{28}{28^s} + \frac{56}{56^s} - \frac{84}{84^s}$$
$$= \left(1 - \frac{2}{2^s}\right)\left(1 + \frac{2}{2^s} + \frac{4}{4^s} - \frac{14}{7^s} - \frac{28}{14^s} - \frac{28}{28^s} + \frac{21}{21^s} + \frac{42}{42^s}\right)$$

IRREDUCIBILITY OF $P_G(s)$

We have seen that for any non-Frattini normal subgroup of G, the Dirichlet polynomial $P_G(s)$ admits a corresponding non trivial factorization.

- Do there exist examples of groups G such that $P_G(s)$ has a non trivial factorization which does not come from normal subgroups?
- In particular is $P_G(s)$ irreducible in $\mathcal{R}$ when G is a simple group?

THEOREM (PATASSINI 2009)

Let S be a simple group of Lie type. $P_S(s)$ is reducible if and only if $S = \mathrm{PSL}(2, p)$ with $p = 2^n - 1$ a Mersenne prime and $n \equiv 3 \mod 4$.

THEOREM (PATASSINI 2010)

$P_{\mathrm{Alt}(n)}(s)$ is irreducible if n is sufficiently large.

Even if there is not a complete correspondence between the irreducible factors of the Dirichlet series $P_G(s)$ and the factor groups in a chief series of G, factorizing $P_G(s)$ in the ring $\mathcal{R}$ can give useful information on the structure of G.

THEOREM (DAMIAN, AL 2005)

Let G be a finite solvable group. The series $P_G(s)$ can be written in a unique way in the form

$$P_G(s) = \left(1 - \frac{c_1}{q_1^s}\right) \dots \left(1 - \frac{c_t}{q_t^s}\right)$$

where $q_1, .., q_t$ are not necessarily distinct prime powers.

- *A chief series of G contains exactly t non-Frattini factors, with order $q_1, \dots q_t$.*
- *$c_1 + \dots + c_t$ is the number of maximal subgroups of G.*

Let G be a finite group and let $1 = N_t \trianglelefteq N_{t-1} \trianglelefteq \cdots \trianglelefteq N_0 = G$ be a chief series of G. Define:

- $P_i(s) := P_{N_i/N_{i+1}, G/N_{i+1}}(s)$
- $A := \{i \mid N_i/N_{i+1} \text{ is abelian}\}$, $B := \{i \mid N_i/N_{i+1} \text{ is not abelian}\}$
- $P_{G,\mathrm{ab}}(s) := \prod_{i \in A} P_i(s)$, $\quad P_{G,\mathrm{nonab}}(s) := \prod_{i \in B} P_i(s)$

The factorization

$$P_G(s) = P_{G,\mathrm{ab}}(s) P_{G,\mathrm{nonab}}(s)$$

can be determined only from the knowledge of $P_G(s)$.

PATASSINI 2010

- $P_{G,\mathrm{ab}}(s) = \prod_p P_{G,\mathrm{ab},p}(s)$
- p odd $\Longrightarrow P_{G,\mathrm{ab},p}(s) = (P_{G,p}(s), P_G(s))$
- $P_{G,\mathrm{ab},2}(s) = (P_{G,2}(s), P_G(s))/Q(s)$, with $Q(s) \in \mathcal{R}$ uniquely determined from the knowledge of the irreducible factors of $P_G(s)$.

- G a finitely generated profinite group.
- $a_n(G) :=$ the number of open subgroups of index n.
- $m_n(G) :=$ the number of maximal open subgroups of index n.
- μ the Möbius function of the subgroup lattice of G :

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

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

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

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

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.

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 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.

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 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!

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 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 $n \in \mathbb{N}$?

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 $n \Rightarrow G$ has only finitely many maximal subgroups (which is equivalent to say that $|G : \mathrm{Frat}\, G|$ is finite).

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 $n \Rightarrow G$ has only finitely many maximal subgroups (which is equivalent to say that $|G : \operatorname{Frat} G|$ is finite).

The Frattini subgroup $\operatorname{Frat} G$ is the intersection of all maximal subgroups of G

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 $n \Rightarrow G$ has only finitely many maximal subgroups (which is equivalent to say that $|G : \mathrm{Frat}\, G|$ is finite).

- $\mu_G(H) \neq 0 \Rightarrow H$ is an intersection of maximal subgroups.
- One can expect that $b_n(G) = \sum_{|G:H|=n} \mu_G(H) = 0$ for almost all n would imply that there are only finitely many subgroups of G that are intersection of maximal subgroups.

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 $n \Rightarrow G$ has only finitely many maximal subgroups (which is equivalent to say that $|G : \mathrm{Frat}\, G|$ is finite).

- $\mu_G(H) \neq 0 \Rightarrow H$ is an intersection of maximal subgroups.
- One can expect that $b_n(G) = \sum_{|G:H|=n} \mu_G(H) = 0$ for almost all n would imply that there are only finitely many subgroups of G that are intersection of maximal subgroups.

CONJECTURE

If $b_n(G) = 0$ for almost all n, then $G/\mathrm{Frat}\, G$ 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 minimal normal subgroup of G/G_{n+1}.

To any factor G_n/G_{n+1}, a finite Dirichlet series $P_n(s)$ is associated:

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

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

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

G_n/G_{n+1} is a Frattini chief factor if $G_n/G_{n+1} \leq \mathrm{Frat}(G/G_{n+1})$.

- $P_n(s) = 1 \Leftrightarrow G_n/G_{n+1}$ is a Frattini factor.
- $G/\mathrm{Frat}\, G$ is a finite group $\Leftrightarrow G_n/G_{n+1}$ is a Frattini factor for all but finitely many $n \in \mathbb{N}$.
- $b_n(G) = 0$ for almost all $n \in \mathbb{N} \Leftrightarrow P_G(s)$ is finite.

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

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

G_n/G_{n+1} is a Frattini chief factor if $G_n/G_{n+1} \leq \mathrm{Frat}(G/G_{n+1})$.

- $P_n(s) = 1 \Leftrightarrow G_n/G_{n+1}$ is a Frattini factor.
- $G/\mathrm{Frat}\, G$ is a finite group $\Leftrightarrow G_n/G_{n+1}$ is a Frattini factor for all but finitely many $n \in \mathbb{N}$.
- $b_n(G) = 0$ for almost all $n \in \mathbb{N} \Leftrightarrow P_G(s)$ is finite.

A TEMPTING (BUT WRONG) ARGUMENT

If $P_G(s)$ is a finite series, then $P_n(s) = 1$ for all but finitely many $n \in \mathbb{N}$ and $G/\mathrm{Frat}\, G$ is finite.

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

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

G_n/G_{n+1} is a Frattini chief factor if $G_n/G_{n+1} \leq \mathrm{Frat}(G/G_{n+1})$.

- $P_n(s) = 1 \Leftrightarrow G_n/G_{n+1}$ is a Frattini factor.
- $G/\mathrm{Frat}\, G$ is a finite group $\Leftrightarrow G_n/G_{n+1}$ is a Frattini factor for all but finitely many $n \in \mathbb{N}$.
- $b_n(G) = 0$ for almost all $n \in \mathbb{N} \Leftrightarrow P_G(s)$ is finite.

A TEMPTING (BUT WRONG) ARGUMENT

If $P_G(s)$ is a finite series, then $P_n(s) = 1$ for all but finitely many $n \in \mathbb{N}$ and $G/\mathrm{Frat}\, G$ is finite.

WE MUST BE MORE CAREFUL

We cannot exclude that a formal product of infinitely many non trivial finite Dirichlet series could be finite.

A RELATED PROBLEM WITH A SURPRISING SOLUTION

QUESTION

Assume that G is a finitely generated prosolvable group, and let p be a fixed prime number. What can we say about G if $b_{p^r}(G) = 0$ for almost all $r \in \mathbb{N}$? Does G contain only finitely many maximal subgroups of index a p-power?

REMARK

The following are equivalent:

- G contains only finitely many maximal subgroups whose index is a power of p.
- A chief series of G contains only finitely many non-Frattini factors whose order is a p-power.

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:

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

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

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

QUESTION (MANN)

Suppose that the p-factor $P_{G,p}(s)$ is a Dirichlet polynomial or, more in general, that $P_{G,p}(s)$ is a rational function of $1/p^s$. Does this imply that G has only finitely many maximal subgroups of p-power index?

QUESTION (MANN)

Suppose that the p-factor $P_{G,p}(s)$ is a Dirichlet polynomial or, more in general, that $P_{G,p}(s)$ is a rational function of $1/p^s$. Does this imply that G has only finitely many maximal subgroups of p-power index?

The answer to the question is negative!

QUESTION (MANN)

Suppose that the p-factor $P_{G,p}(s)$ is a Dirichlet polynomial or, more in general, that $P_{G,p}(s)$ is a rational function of $1/p^s$. Does this imply that G has only finitely many maximal subgroups of p-power index?

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

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

This implies

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

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 C_{p^n-1} over $(C_p)^n$.
- H contains t_n open normal subgroups K with $H/K \cong C_{p^n-1}$.
- We can construct t_n irreducible non isomorphic H-modules of order p^n, say $M_{n,1}, \ldots, M_{n,t_n}$.

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 C_{p^n-1} over $(C_p)^n$.
- H contains t_n open normal subgroups K with $H/K \cong C_{p^n-1}$.
- We can construct t_n irreducible non isomorphic H-modules of order p^n, say $M_{n,1}, \ldots, M_{n,t_n}$.

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

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 C_{p^n-1} over $(C_p)^n$.
- H contains t_n open normal subgroups K with $H/K \cong C_{p^n-1}$.
- We can construct t_n irreducible non isomorphic H-modules of order p^n, say $M_{n,1}, \ldots, M_{n,t_n}$.

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

G is a 2-generated prosolvable group, with infinitely many non-Frattini chief factors of p-power order: Ω_p is infinite and G contains infinitely many maximal subgroups of p-power index. However

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

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 prosolvable group G such that for each prime p

- *$P_{G,p}(s)$ is a Dirichlet polynomial;*
- *G contains infinitely many maximal subgroups whose index is a p-power.*

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

THEOREM

There exists a 2-generated prosolvable group G such that for each prime p

- *$P_{G,p}(s)$ is a Dirichlet polynomial;*
- *G contains infinitely many maximal subgroups whose index is a p-power.*

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:

- $b_n(G) = 0$ *for almost all* $n \in \mathbb{N}$.
- $P_G(s)$ *is a finite Dirichlet series.*
- $P_G(s)$ *is a rational Dirichlet series.*
- G *contains only finitely many maximal subgroups.*

The proof relies on the following facts:

A COROLLARY OF SKOLEM-MAHLER-LECH THEOREM

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

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

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.

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:

- $\pi(G)$ is finite;
- $P_{G,p}(s)$ is a rational function of $1/p^s$ for all $p \in \pi(G)$.

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:

- $\pi(G)$ is finite;
- $P_{G,p}(s)$ is a rational function of $1/p^s$ for all $p \in \pi(G)$.

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

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

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:

- $\pi(G)$ is finite;
- $P_{G,p}(s)$ is a rational function of $1/p^s$ 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 each prime number 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 $P_G(s)$ as an infinite formal product $P_G(s) = \prod_n P_n(s)$ where $P_n(s)$ is the Dirichlet series associated with the chief factor G_n/G_{n+1}.

WHAT ABOUT THE GENERAL CASE?

Given an arbitrary finitely generated profinite group G, we can again express $P_G(s)$ as an infinite formal product $P_G(s) = \prod_n P_n(s)$ where $P_n(s)$ is the Dirichlet series 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.

WHAT ABOUT THE GENERAL CASE?

Given an arbitrary finitely generated profinite group G, we can again express $P_G(s)$ as an infinite formal product $P_G(s) = \prod_n P_n(s)$ where $P_n(s)$ is the Dirichlet series 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.

WHAT ABOUT THE GENERAL CASE?

Given an arbitrary finitely generated profinite group G, we can again express $P_G(s)$ as an infinite formal product $P_G(s) = \prod_n P_n(s)$ where $P_n(s)$ is the Dirichlet series 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.

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

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

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 $P_G^S(s) = 1$ for almost all simple groups S; however none of these two equivalent facts can be easily deduced from the rationality of $P_G(s)$.

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 $P_G^S(s) = 1$ 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 $\pi(G)$.

THEOREM (E. DAMIAN, AL)

If G is finite, then $\pi(G) = \tilde{\pi}(G)$.

QUESTION

Can this result be generalized to finitely generated profinite groups?

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 $P_G^S(s) = 1$ for almost all simple groups S; however none of these two equivalent facts can be easily deduced from the rationality of $P_G(s)$.

Even if we know that $P_G(s) = \prod_S P_G^S(s)$ is the product of finitely many Euler factors $P_G^S(s)$, we cannot easily deduce, as in the prosolvable case, that $P_G(s)$ rational implies $P_G^S(s)$ rational for each 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 $P_G^S(s) = 1$ for almost all simple groups S; however none of these two equivalent facts can be easily deduced from the rationality of $P_G(s)$.

Even if we know that $P_G(s) = \prod_S P_G^S(s)$ is the product of finitely many Euler factors $P_G^S(s)$, we cannot easily deduce, as in the prosolvable case, that $P_G(s)$ rational implies $P_G^S(s)$ 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 $P_G^S(s) = \prod_{n \in \Omega_S} P_n(s)$ 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:

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.

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 non comparable families of simple groups!

SKETCH OF THE PROOF

NOTATION

- $P_G(s) = \prod_t P_t(s)$ with $P_t(s) = \sum_n b_{t,n}/n^s$ the Dirichlet polynomial corresponding to the chief factor G_t/G_{t+1}.
- $G_t/G_{t+1} = S_t^{r_t}$ with S_t a simple group and $r_t \in \mathbb{N}$.
- $I = \{t \mid S_t \text{ is a cyclic or an alternating group}\}$.

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

SKETCH OF THE PROOF

NOTATION

- $P_G(s) = \prod_t P_t(s)$ with $P_t(s) = \sum_n b_{t,n}/n^s$ the Dirichlet polynomial corresponding to the chief factor G_t/G_{t+1}.
- $G_t/G_{t+1} = S_t^{r_t}$ with S_t a simple group and $r_t \in \mathbb{N}$.
- $I = \{t \mid S_t \text{ is a cyclic or an alternating group}\}$.

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

For each $i \in I$, there exists $n_i \in \mathbb{N}$ such that either S_i is cyclic of order n_i or $S_i \cong \mathrm{Alt}(n_i)$.

Since $P(s)$ is rational, there exists $u \in \mathbb{N}$ such $c_n = 0$ whenever n is divisible by any prime larger than u. We prove: $n_i < u$ for each $i \in I$. This implies in particular that $\pi(G)$ is finite.

Since $P(s)$ is rational, there exists $u \in \mathbb{N}$ such $c_n = 0$ whenever n is divisible by any prime larger than u. We prove: $n_i < u$ for each $i \in I$. This implies in particular that $\pi(G)$ is finite.

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

Since $P(s)$ is rational, there exists $u \in \mathbb{N}$ such $c_n = 0$ whenever n is divisible by any prime larger than u. We prove: $n_i < u$ for each $i \in I$. This implies in particular that $\pi(G)$ is finite.

$$J = \{j \in I \mid n_j = n_i \text{ for infinitely many } i \in I.\}$$

Since $P(s)$ is rational, there exists $u \in \mathbb{N}$ such $c_n = 0$ whenever n is divisible by any prime larger than u. We prove: $n_i < u$ for each $i \in I$. This implies in particular that $\pi(G)$ is finite.

$$J = \{j \in I \mid n_j = n_i \text{ for infinitely many } i \in I.\}$$

$$P(s) = \prod_{i \in I} P_i(s) \text{ rational} \Rightarrow P^*(s) = \prod_{j \in J} P_j(s).$$

Since $P(s)$ is rational, there exists $u \in \mathbb{N}$ such $c_n = 0$ whenever n is divisible by any prime larger than u. We prove: $n_i < u$ for each $i \in I$. This implies in particular that $\pi(G)$ is finite.

$$J = \{j \in I \mid n_j = n_i \text{ for infinitely many } i \in I.\}$$

$$m_0 := \max_{i \in J} n_i, \quad q := \text{largest prime} \leq m_0, \quad p := \text{largest prime} < q.$$

Since $P(s)$ is rational, there exists $u \in \mathbb{N}$ such $c_n = 0$ whenever n is divisible by any prime larger than u. We prove: $n_i < u$ for each $i \in I$. This implies in particular that $\pi(G)$ is finite.

$$J = \{j \in I \mid n_j = n_i \text{ for infinitely many } i \in I.\}$$

$$m_0 := \max_{i \in J} n_i, \quad q := \text{largest prime} \leq m_0, \quad p := \text{largest prime} < q.$$

Consider the set Ω of the positive integers x such that

- q divides x;
- q^2 and p does not divide x;
- $b_{i,x^{r_i}} \neq 0 \; \exists i \in J$.

We prove that $\Omega \neq \emptyset$.

Let w the smallest element of Ω. We prove:

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

Let w the smallest element of Ω. We prove:

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

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.

COMPARING THE PROBABILISTIC ZETA FUNCTION AND THE SUBGROUP ZETA FUNCTION

- The probabilistic zeta function $P_G(s)$ has good combinatorial properties and encodes several information on the group structure. But nothing is known about the analytic properties. Even in the favorable case of finitely generated prosolvable groups nothing is known about the abscissa of convergency and the possibility of a meromorphic continuation.
- On the contrary, for what concern the subgroup zeta function $Z_G(s)$, strong results about the analytic properties have been obtained for some important classes of groups, but not so much is known about the relation with the group structure. It is no more true that $Z_{G/N}(s)$ divides $Z_G(s)$ if $N \trianglelefteq G$.

The subgroup zeta function $Z_G(s) = \sum_n a_n(G)/n^s$ converges in some half complex plane if and only if G has polynomial subgroup growth.

The subgroup zeta function $Z_G(s) = \sum_n a_n(G)/n^s$ converges in some half complex plane if and only if G has polynomial subgroup growth.

THEOREM (A. LUBOTZKY, A. MANN AND D. SEGAL)

Let G be a finitely generated residually finite group. Then G has polynomial subgroup growth if and only if G has a subgroup of finite index which is solvable and of finite rank.

The subgroup zeta function $Z_G(s) = \sum_n a_n(G)/n^s$ converges in some half complex plane if and only if G has polynomial subgroup growth.

If G has polynomial subgroup growth, then also the probabilistic zeta function $P_G(s)$ is absolutely convergent in a suitable half complex plane. However $P_G(s)$ can be absolutely convergent even if the subgroup growth of G is not polynomial: consider for example the free prosolvable group of rank $r > 1$ or the infinite cartesian product $G = \prod_{n\in\mathbb{N}} \mathrm{Alt}(n)$.

The main contributions to the study of the subgroup zeta function are due to D. Segal, G. Smith, F. Grunewald, I. Ilani, M. du Sautoy, C. Voll, L. Woodward. In particular strong results are available if G is a finitely generated torsion-free nilpotent group.

Let G be a finitely generated torsion-free nilpotent group.

- $Z_G(s)$ decomposes as an Euler product $Z_G(s) = \prod_p Z_{G,p}(s)$.
- $Z_{G,p}(s)$ is a rational function in p^{-s}.
- The abscissa of convergency α of $Z_G(s)$ is a rational number.
- There is a $\delta > 0$ such that $Z_G(s)$ can be meromorphically continued to the region $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \alpha - \delta\}$.
- The line $\{s \in \mathbb{C} \mid \mathrm{Re}(s) = \alpha\}$ contains at most one pole of $Z_G(s)$ (at the point $s = \alpha$).

$P_G(s)$ IN THE PRONILPOTENT CASE

The best results in the study of $Z_G(s)$ have been obtained for pronilpotent groups. What can we say about $P_G(s)$ if G is a pronilpotent group?

$P_G(s)$ IN THE PRONILPOTENT CASE

If G is a finitely generated pronilpotent group, then $G = \prod_p G_p$ with G_p the p-Sylow subgroup of G and

$$P_G(s) = \prod_p P_{G_p}(s).$$

$P_G(s)$ IN THE PRONILPOTENT CASE

If G is a finitely generated pronilpotent group, then $G = \prod_p G_p$ with G_p the p-Sylow subgroup of G and

$$P_G(s) = \prod_p P_{G_p}(s).$$

If P is a finitely generated pro-p group and d is the smallest cardinality of a generating set for P, then $P/\operatorname{Frat} P \cong C_p^d$ and

$$P_P(s) = P_{P/\operatorname{Frat} P}(s) = \prod_{0 \leq i \leq d-1} \left(1 - \frac{p^i}{p^s}\right).$$

$Z_G(s)P_G(s) = 1$?

If $G = \hat{\mathbb{Z}}$, then $Z_G(s)P_G(s) = 1$.

PROBLEM

To study the groups G satisfying the condition $Z_G(s)P_G(s) = 1$

DEFINITION

We will say that G is ζ-reversible if $Z_G(s)P_G(s) = 1$.

- If $Z_G(s)$ is convergent in an half complex plane, then $P_G(s)$ is also convergent in an half complex plane and $P_G(t) = \mathrm{Prob}_G(t)$ if $t \in \mathbb{N}$ is large enough.
- If G is ζ-reversible and $P_G(s)$ or $Z_G(s)$ is convergent, then $P_G(s)$, $Z_G(s)$ are both convergent and $(Z_G(t))^{-1} = \mathrm{Prob}_G(t)$ if $t \in \mathbb{N}$ is large enough.

The following identity can help:

$$\sum_{H \leq_o G} \frac{P_H(s)}{|G:H|^s} = 1.$$

$$Z_G(s)P_G(s) = 1 \quad \Leftrightarrow \quad \sum_{H \leq_o G} \frac{P_G(s)}{|G:H|^s} = 1 = \sum_{H \leq_o G} \frac{P_H(s)}{|G:H|^s}$$

$$\Leftrightarrow \quad \sum_{H \leq_o G} \frac{P_G(s) - P_H(s)}{|G:H|^s} = 0$$

COROLLARY

$P_G(s) = P_H(s)$ for each open subgroup H of $G \Rightarrow G$ is ζ-reversible.

EXAMPLES

- If $H \cong G$ for each $H \leq_o G$, then G is ζ-reversible.

EXAMPLES

- If $H \cong G$ for each $H \leq_o G$, then G is ζ-reversible. This occurs if and only if G is abelian and torsion free.

EXAMPLES

- If $H \cong G$ for each $H \leq_o G$, then G is ζ-reversible. This occurs if and only if G is abelian and torsion free.

  For example if $G = \widehat{\mathbb{Z}}^r$ then

$$Z_G(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-(r-1)) = (P_G(s))^{-1}$$

EXAMPLES

- If $H \cong G$ for each $H \leq_o G$, then G is ζ-reversible. This occurs if and only if G is abelian and torsion free.
- Let $d(G)$ be the smallest cardinality of a generating set of G. If G is a pro-p group then

$$P_G(s) = \prod_{0 \leq i \leq d(G)-1} \left(1 - \frac{p^i}{p^s}\right)$$

depends only on $d(G)$. If G is a pro-p group with $d(G) = d(H)$ for each $H \leq_o G$, then G is ζ-reversible.

EXAMPLES

- If $H \cong G$ for each $H \leq_o G$, then G is ζ-reversible. This occurs if and only if G is abelian and torsion free.
- Let $d(G)$ be the smallest cardinality of a generating set of G. If G is a pro-p group then

$$P_G(s) = \prod_{0 \leq i \leq d(G)-1} \left(1 - \frac{p^i}{p^s}\right)$$

depends only on $d(G)$. If G is a pro-p group with $d(G) = d(H)$ for each $H \leq_o G$, then G is ζ-reversible.

Non abelian examples. The pro-p group G with the presentation

$$\langle x_1, \ldots, x_r, y \mid [x_i, x_j] = 1, [x_i, y] = x_i^{p^t} \rangle$$

satisfies $d(H) = r + 1 \ \forall \ H \leq_o G$.

NON PRONILPOTENT EXAMPLES

For any $m \in \mathbb{Z}, m \neq 0$, let G_m be the profinite completion of the Baumslag-Solitar group $B_m = \langle a, b \mid a^{-1}ba = b^m \rangle$.

NON PRONILPOTENT EXAMPLES

For any $m \in \mathbb{Z}, m \neq 0$, let G_m be the profinite completion of the Baumslag-Solitar group $B_m = \langle a, b \mid a^{-1}ba = b^m \rangle$.

- $P_{G_m}(s) = \prod_p \left(1 - \frac{1}{p^s}\right) \prod_{(p,m)=1} \left(1 - \frac{p}{p^s}\right)$
- $H \leq_o G_m \Rightarrow H \cong G_{m^u}$ for some $u \in \mathbb{N} \Rightarrow P_H(s) = P_{G_m}(s)$.

NON PRONILPOTENT EXAMPLES

For any $m \in \mathbb{Z}, m \neq 0$, let G_m be the profinite completion of the Baumslag-Solitar group $B_m = \langle a, b \mid a^{-1}ba = b^m \rangle$.

- $P_{G_m}(s) = \prod_p \left(1 - \frac{1}{p^s}\right) \prod_{(p,m)=1} \left(1 - \frac{p}{p^s}\right)$
- $H \leq_o G_m \Rightarrow H \cong G_{m^u}$ for some $u \in \mathbb{N} \Rightarrow P_H(s) = P_{G_m}(s)$.

$$Z_{G_m}(s) = (P_{G_m}(s))^{-1} = \zeta(s)\zeta(s-1) \prod_{p|m} \left(1 - \frac{p}{p^s}\right)$$

NON PRONILPOTENT EXAMPLES

For any $m \in \mathbb{Z}, m \neq 0$, let G_m be the profinite completion of the Baumslag-Solitar group $B_m = \langle a, b \mid a^{-1}ba = b^m \rangle$.

- $P_{G_m}(s) = \prod_p \left(1 - \frac{1}{p^s}\right) \prod_{(p,m)=1} \left(1 - \frac{p}{p^s}\right)$
- $H \leq_o G_m \Rightarrow H \cong G_{m^u}$ for some $u \in \mathbb{N} \Rightarrow P_H(s) = P_{G_m}(s)$.

$$Z_{G_m}(s) = (P_{G_m}(s))^{-1} = \zeta(s)\zeta(s-1) \prod_{p|m} \left(1 - \frac{p}{p^s}\right)$$

G_m is virtually pronilpotent if and only if $m = \pm 1$.

QUESTION

Do there exist ζ-reversible groups that are not prosolvable?

- G ζ-reversible $\Rightarrow$ the coefficients of $(P_G(s))^{-1}$ are non negative.
- G prosolvable $\Rightarrow$ $P_G(s) = \prod_i (1 - \frac{c_i}{q_i^s}) \Rightarrow$

$$(P_G(s))^{-1} = \prod_i \left(1 + \frac{c_i}{q_i^s} + \frac{c_i^2}{q_i^{2s}} + \dots\right)$$

has non negative coefficients.

QUESTION

Does there exist a finitely generated non prosolvable group G with the property that the coefficients of $(P_G(s))^{-1}$ are non negative?

QUESTION

Do there exist ζ-reversible groups that are not prosolvable?

- G ζ-reversible $\Rightarrow$ the coefficients of $(P_G(s))^{-1}$ are non negative.
- G prosolvable $\Rightarrow$ $P_G(s) = \prod_i (1 - \frac{c_i}{q_i^s}) \Rightarrow$

$$(P_G(s))^{-1} = \prod_i \left(1 + \frac{c_i}{q_i^s} + \frac{c_i^2}{q_i^{2s}} + \dots\right)$$

has non negative coefficients.

QUESTION

Does there exist a finitely generated non prosolvable group G with the property that the coefficients of $(P_G(s))^{-1}$ are non negative?

PROSOLVABLE GROUPS

If G is a prosolvable group then $P_G(s) = \sum_n b_n(G)/n^s$ satisfies the following properties (which are preserved under inversion):

- the sequence $\{b_n(G)\}_n$ has polynomial growth;
- $P_G(s)$ has an Euler factorization over the prime numbers.

PROSOLVABLE GROUPS

If G is a prosolvable group then $P_G(s) = \sum_n b_n(G)/n^s$ satisfies the following properties (which are preserved under inversion):

- the sequence $\{b_n(G)\}_n$ has polynomial growth;
- $P_G(s)$ has an Euler factorization over the prime numbers.

CONSEQUENCES

If G is a ζ-reversible prosolvable group, then

- G has Polynomial Subgroup Growth, hence it has finite rank.
- $Z_G(s)$ has an Euler factorization over the prime numbers.

PROSOLVABLE GROUPS

If G is a prosolvable group then $P_G(s) = \sum_n b_n(G)/n^s$ satisfies the following properties (which are preserved under inversion):

- the sequence $\{b_n(G)\}_n$ has polynomial growth;
- $P_G(s)$ has an Euler factorization over the prime numbers.

CONSEQUENCES

If G is a ζ-reversible prosolvable group, then

- G has Polynomial Subgroup Growth, hence it has finite rank.
- $Z_G(s)$ has an Euler factorization over the prime numbers.

$P_G(s)$ has an Euler factorization over the primes if and only if G is prosolvable. It is still open the problem of characterizing the profinite groups whose subgroup zeta function has an Euler factorization over the primes. If G is pronilpotent, then $Z_G(s)$ has an Euler factorization. However there exist non virtually pronilpotent profinite groups whose subgroup zeta function has an Euler factorization.

PROPOSIZIONE

Let G be a ζ-reversible prosolvable group and let π be the set of the prime divisors of the order of G. For each π-number n, G contains an open subgroup of index n.

PROOF

- It suffices to prove: $a_{p^m}(G) \neq 0 \ \forall p \in \pi, \ \forall \ m \in \mathbb{N}$.

PROPOSIZIONE

Let G be a ζ-reversible prosolvable group and let π be the set of the prime divisors of the order of G. For each π-number n, G contains an open subgroup of index n.

PROOF

- It suffices to prove: $a_{p^m}(G) \neq 0 \ \forall p \in \pi, \ \forall \ m \in \mathbb{N}$. Indeed $(a_1, a_2) = 1, |G : H_1| = a_1, |G : H_2| = a_2 \Rightarrow |G : H_1 \cap H_2| = a_1 a_2$.

PROPOSIZIONE

Let G be a ζ-reversible prosolvable group and let π be the set of the prime divisors of the order of G. For each π-number n, G contains an open subgroup of index n.

PROOF

- It suffices to prove: $a_{p^m}(G) \neq 0 \ \forall p \in \pi, \ \forall \ m \in \mathbb{N}$.
- Fix p: G contains an open subgroup of index pu, with $(u, p) = 1$.

PROPOSIZIONE

Let G be a ζ-reversible prosolvable group and let π be the set of the prime divisors of the order of G. For each π-number n, G contains an open subgroup of index n.

PROOF

- It suffices to prove: $a_{p^m}(G) \neq 0 \ \forall p \in \pi, \ \forall \ m \in \mathbb{N}$.
- Fix p: G contains an open subgroup of index pu, with $(u, p) = 1$.
- $a_{pu}(G) \neq 0$ and $P_G(s)Z_G(s) = 1 \Rightarrow b_{pv}(G) \neq 0 \, \exists \ v$ s.t. $(v, p) = 1$.

PROPOSIZIONE

Let G be a ζ-reversible prosolvable group and let π be the set of the prime divisors of the order of G. For each π-number n, G contains an open subgroup of index n.

PROOF

- It suffices to prove: $a_{p^m}(G) \neq 0 \ \forall p \in \pi, \ \forall \ m \in \mathbb{N}$.
- Fix p: G contains an open subgroup of index pu, with $(u, p) = 1$.
- $a_{pu}(G) \neq 0$ and $P_G(s)Z_G(s) = 1 \Rightarrow b_{pv}(G) \neq 0 \, \exists \ v$ s.t. $(v, p) = 1$.
- $P_G(s) = \prod_i (1 - c_i/q_i^s)$ with $c_i \geq 0$ and q_i prime-powers. Since $b_{pv}(G) \neq 0$ it must be $q_i = p$ for some i.

PROPOSIZIONE

Let G be a ζ-reversible prosolvable group and let π be the set of the prime divisors of the order of G. For each π-number n, G contains an open subgroup of index n.

PROOF

- It suffices to prove: $a_{p^m}(G) \neq 0 \ \forall p \in \pi, \ \forall \ m \in \mathbb{N}$.
- Fix p: G contains an open subgroup of index pu, with $(u, p) = 1$.
- $a_{pu}(G) \neq 0$ and $P_G(s)Z_G(s) = 1 \Rightarrow b_{pv}(G) \neq 0 \, \exists \ v$ s.t. $(v, p) = 1$.
- $P_G(s) = \prod_i (1 - c_i/q_i^s)$ with $c_i \geq 0$ and q_i prime-powers. Since $b_{pv}(G) \neq 0$ it must be $q_i = p$ for some i.
- $$\begin{aligned}(P_G(s))^{-1} &= (1 - c_i/p^s)^{-1}(\textstyle\prod_{j \neq i}(1 - c_j/q_j^s))^{-1} \\ &= (1 + c_i/p^s + c_i^2/p^{2s} + \dots)(\textstyle\sum_m d_m/m^s) \\ &\quad \text{with } d_m \geq 0 \text{ and } d_m = 1.\end{aligned}$$

PROPOSIZIONE

Assume that G is a ζ-reversible prosolvable group of rank 2. Then

- *G is prosupersolvable;*
- *for each prime divisor p of $|G|$, G contains a normal subgroup of index p;*
- *$P_G(s) = P_H(s)$ for each $H \leq_o G$.*

PRO-p-GROUPS

Assume that G is a ζ-reversible pro-p-group (G must be p-adic analytic):

$$\sum_{H \leq_o G} \frac{\prod_{0 \leq i \leq d(G)-1}(1 - \frac{p^i}{p^s}) - \prod_{0 \leq i \leq d(H)-1}(1 - \frac{p^i}{p^s})}{|G : H|^s} = 0.$$

Does this imply $d(G) = d(H)$ for each $H \leq_o G$?

PARTIAL ANSWERS

If $d(H) \neq d(G)$ for some $H \leq_o G$, then

- $d(H) \neq d(G)$ for infinitely many open subgroups H of G.
- If r is minimal with respect to the property that there exists H with $d(H) \neq d(G)$ and $|G : H| = p^r$, then there exist H_1 and H_2 with $|G : H_1| = |G : H_2| = p^r$ and $d(H_1) < d(G) < d(H_2)$.
- G does not contain pro-cyclic open subgroups.
- $d(G) > 2$.

THEOREM (SKOLEM-MAHLER-LECH)

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 no quotient λ_i/λ_j is a non-trivial root of unity. 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.

PROPOSIZIONE

Let $I \subseteq \mathbb{N}$ and let $\{\gamma_i\}_{i\in I}$, $\{n_i\}_{i\in I}$ be positive integers such that

- *for every $n \in \mathbb{N}$, the set $I_n = \{i \in I \mid n_i$ divides $n\}$ is finite;*
- *there exists a prime q such that q does not divide n_i for any $i \in I$.*

If $\prod_{i\in I}(1-\gamma_i x^{n_i})$ is rational in $\mathbb{Z}[[x]]$, then $I = \bigcup_{n\in\mathbb{N}} I_n$ is finite.

SKETCH OF THE PROOF

$$\prod_{i\in I}(1-\gamma_i x^{n_i}) = \frac{(1-\alpha_1 x)\cdots(1-\alpha_s x)}{(1-\beta_1 x)\cdots(1-\beta_r x)}$$

$$\Downarrow$$

$$\psi_n(m) := \sum_{i=1}^{s}(\alpha_i^n)^m - \sum_{i=1}^{r}(\beta_i^n)^m - \sum_{i\in I_n} n_i(\gamma_i^{n/n_i})^m = \sum_{i\in I_{nm}\setminus I_n} n_i\gamma_i^{nm/n_i}.$$

$I_{nq^c} = I_n \forall c \in \mathbb{N}$, hence $\psi_n(m)$ vanishes for infinitely many integers.

$$\psi_n(m) = \sum_{i=1}^{s} (\alpha_i^n)^m - \sum_{i=1}^{r} (\beta_i^n)^m - \sum_{i \in I_n} n_i (\gamma_i^{n/n_i})^m = 0 \text{ for infinitely many } m.$$

To apply the Skolem-Mahler-Lech Theorem we have to choose $n \in \mathbb{N}$ such that no nontrivial root of unit can be expressed as the ratio of two elements in the set $\Lambda_n = \{\alpha_1^n, \ldots, \alpha_s^n, \beta_1^n, \ldots, \beta_r^n, \gamma_i^{n/n_i} \mid i \in I_n\}$.

- Let e be the order of the subgroup of $\mathbb{C}^*$ generated by the set of roots of unit which can be written as x/y with $x, y \in \{\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r\}$.
- As the γ_i's are positive integers, we can choose an integer d such that: $x \in \Lambda_e, (x^d)^m \in \mathbb{N},\ m \in \mathbb{N} \Rightarrow x^d \in \mathbb{N}$.

If we choose $n = ed$, then there is no pair of elements Λ_n whose ratio is a root of unit.

$$\psi_n(m) = \sum_{i=1}^{s}(\alpha_i^n)^m - \sum_{i=1}^{r}(\beta_i^n)^m - \sum_{i\in I_n} n_i(\gamma_i^{n/n_i})^m = 0 \text{ for infinitely many } m.$$

To apply the Skolem-Mahler-Lech Theorem we have to choose $n \in \mathbb{N}$ such that no nontrivial root of unit can be expressed as the ratio of two elements in the set $\Lambda_n = \{\alpha_1^n, \ldots, \alpha_s^n, \beta_1^n, \ldots, \beta_r^n, \gamma_i^{n/n_i} \mid i \in I_n\}$.

- Let e be the order of the subgroup of $\mathbb{C}^*$ generated by the set of roots of unit which can be written as x/y with $x, y \in \{\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r\}$.
- As the γ_i's are positive integers, we can choose an integer d such that: $x \in \Lambda_e, (x^d)^m \in \mathbb{N},\ m \in \mathbb{N} \Rightarrow x^d \in \mathbb{N}$.

If we choose $n = ed$, then there is no pair of elements Λ_n whose ratio is a root of unit.

Conclusion: $\psi_n(m) = 0\ \forall m \in \mathbb{N} \Rightarrow I_{nm} = I_n\ \forall m \in \mathbb{N} \Rightarrow I$ is finite

$$\sum_{H\leq_o G} \frac{P_H(s)}{|G:H|^s} = \sum_{H\leq_o G} \frac{\left(\sum_{K\leq_o H} \frac{\mu_H(K)}{|H:K|^s}\right)}{|G:H|^s}$$

$$= \sum_{K\leq_o H\leq_o G} \frac{\mu_H(K)}{|G:K|^s}$$

$$= \sum_{K\leq_o G} \frac{\sum_{K\leq_o H} \mu_H(K)}{|G:K|^s}$$

$$= \sum_{K\leq_o G} \frac{\delta_{K,G}}{|G:K|^s} = 1.$$

Let G be a nilpotent torsion-free group.

- G may be identified with a subgroup of the upper unitriangular group $\mathrm{Tr}_1(m, \mathbb{Z})$ for some m.
- The set $\mathrm{Tr}_0(m, \mathbb{Q})$ of upper-triangular matrices over $\mathbb{Q}$ with zero diagonal is a Lie algebra with the operation $[a, b] = ab - ba$.
- We may define a map

  $\log : G \to \mathrm{Tr}_0(m, \mathbb{Q}) \qquad g \mapsto \log g = \sum_n \frac{(-1)^{n-1}}{n}(g-1)^n.$

G contains a subgroup G_0 of finite index such that $L = \log G_0$ satisfies the properties:

- L is a Lie subring of $\mathrm{Tr}_0(m, \mathbb{Q})$;
- $(L, +) \cong \mathbb{Z}^r$, for some r;
- For almost all primes p, $a_{p^n}(G)$ coincides with the number of Lie subrings of index p^n in L for all n.

This reduces the study of $Z_G(s)$ to that of the subring zeta function $\zeta_L(s)$ of L.

The p-adic absolute value of $\lambda \in \mathbb{Z}_p$ is written $|\lambda| = p^{-f}$ where $\lambda = p^f u$ and u is a p-adic unit.

Fix a prime p and identify $L \otimes \mathbb{Z}_p$ with $\mathbb{Z}_p^r$ by choosing a $\mathbb{Z}$-basis for L.

$$\zeta_{L,p}(s) = \frac{1}{(1-1/p)^r} \int_{\mathcal{M}} |\lambda_{11}|^{s-1} \cdots |\lambda_{rr}|^{s-r} d\mu$$

where $\mathcal{M}$ is the subset of $\mathrm{Tr}(r, \mathbb{Z}_p)$ defined by a certain collection of bilinear equations, which express the requirement that the linear span of the rows of the matrix (λ_{ij}) be closed under the Lie bracket.

$\zeta_{L,p}(s)$ is given by what Grunewald and du Sautoy call a cone integral.

- $\mathcal{D} = \{f_i, g_i \mid 0 \leq i \leq l\}$ cone integral data: a family of r-variable polynomials over $\mathbb{Q}$;
- $V_p(\mathcal{D}) := \{x \in \mathbb{Z}_p^r \mid v(f_i(x)) \leq v(g_i(x)), 1 \leq i \leq l\}$ where v is the p-adic valuation.
- $Z_{\mathcal{D}}(s,p) := \int_{V_p(\mathcal{D})} |f_0(x)||g_0(x)|^s d\mu$ cone integral defined by $\mathcal{D}$.

THEOREM

There exists $\mathcal{D}$ such that for all primes p

$$\zeta_{L,p}(s) = \frac{1}{a_{p,0}} Z_{\mathcal{D}}(s,p)$$

where $a_{p,0} = Z_{\mathcal{D}}(\infty, p)$ is a non-zero constant.

The proofs uses Denef's method of evaluating p-adic integers by an explicit resolution of singularities.

There exists

- $V_1, \ldots, V_t$ algebraic varieties defined over $\mathbb{Z}$
- $P_1(x, y), \ldots, P_t(x, y) \in \mathbb{Q}(x, y)$ rational functions over $\mathbb{Q}$

such that for almost all primes p

$$Z_{\mathcal{D}}(s, p) = a_{p,0} + \sum_{1 \leq i \leq t} b_i(p) P_i(p^s, p^{-s})$$

with $b_i(p)$ the number of $\mathbb{F}_p$-points on the reduction modulo p of V_i.

This links the group-theoretic zeta function in an explicit way to the Weil zeta function of certain algebraic varieties.