PROFINITE GROUPS IN WHICH THE PROBABILISTIC ZETA FUNCTION HAS NO NEGATIVE COEFFICIENTS

ELOISA DETOMI AND ANDREA LUCCHINI

Abstract. To a finitely generated profinite group G, a formal Dirichlet series $P_G(s) = \sum_{n\in\mathbb{N}} a_n(G)/n^s$ is associated, where $a_n(G) = \sum_{|G:H|=n} \mu(H,G)$ and $\mu(H,G)$ denotes the Möbius function of the lattice of open subgroups of G. Its formal inverse $P_G^{-1}(s)$ is the probabilistic zeta function of G. When G is prosoluble, every coefficient of $(P_G(s))^{-1}$ is nonnegative. In this paper we discuss the general case and we produce a non-prosoluble finitely generated group G with the same property.

1. Introduction

Let G be a finitely generated profinite group, that is a profinite group *topologically* generated by a finite number of elements. For each positive integer n, the number of open subgroups of index n in G is finite. So we can define a formal Dirichlet series $P_G(s)$ as follows:

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

where $\mu(H,G)$ denotes the Möbius function of the lattice of open subgroups of G, defined recursively by $\mu(G,G) = 1$ and $\sum_{H\leq K} \mu(K,G) = 0$ for any proper open subgroup H of G.

The formal inverse of $P_G(s)$ is the probabilistic zeta function which was first introduced by A. Mann [21] for finitely generated groups and by N. Boston [1] in the case of finite groups. Hall [13] showed that for a finite group G and a positive integer t, $P_G(t)$ is equal to the probability that t randomly chosen elements generate G. In [21] A. Mann made a conjecture which implies that $P_G(s)$ has a similar meaning for positively finitely generated (PFG) profinite groups: here we say that a profinite group is PFG if there exists a positive integer t such that $\mu(\Omega(t)) > 0$ where μ is the normalised Haar measure uniquely defined on G^t and $\Omega(t)$ is the set of the generating t-tuples in G (in the topological sense). Namely Mann conjectured that if G is PFG, then the Dirichlet series $P_G(s)$ is absolutely convergent on some complex half-plane of $\mathbb{C}$ and takes the values $\mu(\Omega(t)) > 0$ for (sufficiently large) integers t. This conjecture was proved true for some classes of profinite groups, among which finitely generated prosolvable groups [18] and more generally, any PFG group G with the property that, for each open normal subgroup N of G, all the composition factors of G/N are either abelian or alternating groups [20] (see also [22] and [17] for other classes). But even when the convergence of $P_G(s)$ is not ensured, this Dirichlet series encodes information about the lattice generated

1991 *Mathematics Subject Classification.* 20E07, 11M41, 20P05.
Key words and phrases. Zeta function, Probabilistic zeta function, Profinite groups.

by the open subgroups of G and combinatorial properties of the sequence $\{a_n(G)\}$ reflect on the structure of G. For example, a finitely generated profinite group is prosoluble if and only if the sequence $\{a_n(G)\}$ in multiplicative (see [8] and [9]).

In [6] the authors examine profinite groups in which the probabilistic zeta function coincides with the subgroup zeta function $\zeta_G(s) = \sum_{n\in\mathbb{N}} \frac{\beta_n(G)}{n^s}$ where $\beta_n(G)$ is the number of subgroups of index n in G. If this is the case, the probabilistic zeta function $(P_G(s))^{-1}$ is a Dirichlet series whose coefficients are all nonnegative. For example, if G is a prosoluble group, then $P_G(s)$ can be written as $\prod_{i\in\mathbb{N}}(1 - c_i/q_i^s)$ where q_i is a prime power and $c_i \geq 0$, hence all coefficients of $(P_G(s))^{-1}$ are nonnegative. In [6] the authors ask if there exists non-prosoluble examples of finitely generated groups for which the probabilistic zeta function is a Dirichlet series with nonnegative coefficients.

In this paper we answer in positive to this question.

Theorem 1.1. *There exists a non-prosoluble group G such that G is finitely generated and every coefficient of $(P_G(s))^{-1}$ is nonnegative.*

Note that the group constructed in Theorem 1.1 is a direct product of alternating groups. This group is finitely generated but, possibly, not PFG.

At the present we do not have example of a finite non-soluble group whose probabilistic zeta function has nonnegative coefficients. All the nonabelian finite simple groups that we examined have a negative coefficient in their probabilistic zeta function (see Section 4). For example, for the alternating group of degree 5 we have

$$P_{A_5}(s) = 1 - 5/5^s - 6/6^s - 10/10^s + 20/20^s + 60/30^s - 60/60^s$$

and the probabilistic zeta function $(P_{A_5}(s))^{-1}$ has a negative coefficient for $n = 20$ (namely -20). For any group G, the series $P_G(s)$ can be written as an (infinite formal) product of finite Dirichlet polynomials according to a chief series of G as shown in [7] and in [10]. Using this factorization, it is possible to construct large finite groups in which all first terms of the probabilistic zeta function are positive. For example, in the last section we show that the probabilistic zeta function of $G = C_2^2 \times C_5^2 \times A_5$ has negative coefficients and the first one appears for $n = 50000$. Trying to construct extension of this group by adding abelian chief factors is not a good strategy because the number of generators of the new group might be quite larger (for example, the minimal number of generators of $C_2^2 \times C_5^2 \times G$ is 4). We will show that it is possible to construct an inverse system of groups G_k starting from a (large enough) alternating group and extending it with direct products of alternating groups in such a way that at each step the "first" coefficients $(P_{G_k}(s))^{-1}$ are nonnegative and the minimal number of generators of G_k is bounded. Hence the resulting inverse limit $\varprojlim G_k$ is actually finitely generated and its probabilistic zeta function has no negative coefficients.

2. Preliminaries

In this paper we are mainly interested in finitely generated profinite groups, so, unless stated otherwise, "group" means finitely generated profinite group and "subgroups" means closed subgroups. Moreover, in a profinite group G, open subgroups have finite index in G, and G is (topologically) d-generated if and only if it is the inverse limit of d-generated finite groups.

We define the Möbius function of the lattice of open subgroups of G by $\mu(G,G) = 1$ and

$$\sum_{H \leq K} \mu(K,G) = 0$$

for any proper open subgroup H of G. Then we define formal Dirichlet series

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

as the Dirichlet generating function associated with the sequence

$$a_n(G) = \sum_{|G:H|=n} \mu(H,G).$$

In [10, Theorem 13] the authors show that $P_G(s)$ factorizes through a normal subgroup $N \leq G$, namely $P_G(s) = P_{G/N}(s)P_{G,N}(s)$, where

$$P_{G,N}(s) = \sum_{n \in \mathbb{N}} \frac{a_n(G,N)}{n^s} \qquad \text{with} \qquad a_n(G,N) := \sum_{\substack{|G:H|=n \\ HN=G}} \mu(H,G).$$

Furthermore, by iteration they obtain that given a chief series $\Sigma : G = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq G_\tau = 1$, where $\tau \leq \aleph_0$, the Dirichlet series $P_G(s)$ can be written as a formal product

$$P_G(s) = \prod_{i \geq 0} P_{G/N_{i+1}, N_i/N_{i+1}}(s),$$

and they shows that the factorization is independent of Σ [10, Theorem 17].

To describe the finite Dirichlet series $P_{G/N_{i+1}, N_i/N_{i+1}}(s)$ we need the concept of crowns. This notion was first introduced by Gaschütz in [12] for chief factors of a finite soluble group G, and later generalized to all finite groups (see for example [16] and [27]). In [7] the notion of crown have been applied to study some properties of the probabilistic zeta function of a finite group, and in [10] extended to profinite groups. We refer to [10] for the details, but for short we say that two chief factors of G are G-equivalent (as G-groups) if they are G-isomorphic either between them or to the two minimal normal subgroups of a finite primitive epimorphic image of G (having two minimal normal subgroups). In particular, two G-equivalent factors are equivalent as groups. Given a chief series Σ of G, for any chief factor A we set $\delta_G(A)$ to be the cardinality of the set of the chief factors N_i/N_{i+1} which are not Frattini and are G-equivalent to A; this number does not depend on the chosen chief series and has the remarkable property that G has a section G-isomorphic to $A^{\delta_G(A)}$ (called the A-crown of G). For example, if $G = \prod_i A_{m_i}^{f_i}$ is a direct product of copies of alternating groups, for some integers f_i and $m_i \neq m_j$, then $\delta_G(A_{m_i}) = f_i$.

Let A be a chief factor of G and let $\rho : G \to \mathrm{Aut}(A)$ be defined by $g \mapsto g^\rho$, where $g^\rho : a \mapsto a^g$ for all $a \in A$. The *monolithic primitive group associated with* A is defined as

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

and we identify $\mathrm{soc}(L_A)$ with A. Then we can write $P_G(s)$ as a formal product

$$P_G(s) = \prod_A \left((P_{L_A,A}(s)) \cdots \left(P_{L_A,A}(s) - \frac{(1+q+\cdots+q^{\delta_G(A)-2})\gamma}{|A|^s} \right) \right) \tag{2.1}$$

where A runs over the set of representatives (under the G-equivalence relation) of the non-Frattini chief factors in a given chief series Σ, L_A is the monolithic primitive group associated with A, $\gamma = |C_{\mathrm{Aut}\,A}(L_A/A)|$ and $q = |\operatorname{End}_{L_A} A|$ if A is abelian, $q = 1$ otherwise. Moreover, the factorization of $P_G(s)$ does not depend on the chosen chief series Σ. In particular, if G is a prosoluble group, then

$$P_G(s) = \prod_{q_i} \left(1 - \frac{c_i}{q_i^s}\right)$$

for some positive integer c_i and some prime powers q_i.

In the case where G is a finite group and $G = H \times K$, where H and K have no common isomorphic chief factors, it is possible to prove that the formula 2.1 reduces to the result of Brown [2]

$$P_G(s) = P_H(s)P_K(s) \tag{2.2}$$

and the minimal number of generators $d(G)$ of G is the minimum between the minimal number of generator of H and of K (see [5] for the complete result on $d(G)$). Moreover, if $G = S^f$ for a non-abelian finite simple group S and an integer f, then the formula 2.1 reduces to the result of Boston [1]

$$P_{S^f}(s) = \prod_{i=0}^{f-1} \left(P_S(s) - \frac{i|\operatorname{Aut}(S)|}{|S|^s}\right). \tag{2.3}$$

Let us denote by $c_n(G)$ the coefficients of the probabilistic zeta function of G:

$$(P_G(s))^{-1} = \sum_{n\geq 1} \frac{c_n(G)}{n^s}.$$

Basic properties of the coefficients $a_n(G)$ and $c_n(G)$ are summarised in the following lemmas.

Lemma 2.1. *Given a group G, the following relations hold:*

(1) $c_n(G) = -\sum_{\substack{rs=n\\ r\neq 1}} a_r(G)c_s(G)$;

(2) $|c_n(G)| \leq \sum_{n_1\cdots n_t=n} |a_{n_1}(G)\dots a_{n_t}(G)|$, *where the sum runs over the set of all ordered factorizations of n.*

Lemma 2.2. *If G is a finite perfect group, then n divides $a_n(G)$ and $c_n(G)$ for every n.*

Proof. Let H be a subgroup of G of index n. By [15, Theorem 4.5], the index $|N_G(H) : H|$ divides $\mu(H,G)|G : HG'|$. Since G is perfect, it follows that $n = |G : H|$ divides $\mu(H,G)|G : N_G(H)|$. So, in particular n divides $a_n(G)$. By Lemma 2.1, we deduce that n divides also $c_n(G)$. □

Recall that if H is an open subgroup of G and $\mu(H,G) \neq 0$, then H is an intersection of maximal subgroups of G. We are interested in subgroups that give a nontrivial contributions to $a_n(G)$, so we set

$$b_n(G) = |\{H \leq G \mid \mu(H,G) \neq 0,\ |G : H| = n\}|.$$

The next two results will be the key ingredient to construct our group.

Theorem 2.3. [4, Theorems 1-2] *There exist two absolute constants α and β such that for any $m \in \mathbb{N}$, if G is an alternating or symmetric group, then*

(1) $b_n(G) \leq n^\alpha$, *for every integer n.*

(2) $|\mu(H,G)| \leq |G:H|^{\beta}$ *for every subgroup* H *of* G.

Theorem 2.4. [19, Theorem 9] *Suppose that* G *is a* d*-generated profinite group, and that there exists a constant* a *with the following property: for any epimorphic image* L *of* G *which is monolithic with non-abelian socle and for any* $X \leq L$

$$|\mu(X,L)| \leq |\mu(X\operatorname{soc}(L),L)| \cdot |X\operatorname{soc}(L):X|^{a}.$$

Then

$$|\mu(H,G)| \leq |G:H|^{\tilde{a}}$$

for each open subgroup H *of* G, *where* $\tilde{a} = \max(a+1, d+1)$.

3. Product of alternating groups

Let $c = \alpha + \beta + 11$ where α and β are the constants defined in Theorem 2.3. Assume that f is a function from $\mathbb{N}$ to $\mathbb{N}$ with the property that

$$f(m) \leq (m!)^{c},$$

and let $\{m_i \mid i \in \mathbb{N}\}$ be a strictly increasing sequence of integers.

Consider the product of $f(m_i)$ copies of the alternating groups A_{m_i}, for $i = 1,\dots,k$:

$$G_k = \prod_{i=1}^{k} A_{m_i}^{f(m_i)}.$$

Our first goal is to prove that there exists an integer N such that if $m_1 \geq N$, then G_k is $(c+2)$-generated and $|c_n(G_k)| \leq (n!)^{c}$ for every integer $n > m_k$.

The proof that G_k is boundedly generated, once m_1 is large enough, relies on the following result; throughout, all logarithms are to base 2.

Theorem 3.1. [24] *Let* S *be a nonabelian finite simple group. Let* $h_S(d)$ *be the maximal integer* h *such that* S^h *is* d*-generated. Then*

$$h_S(d) \geq \frac{|S|^{d-1}}{\log|S|},$$

for all $d \geq 2$.

Proposition 3.2. *Assume that* $m_1!/\log(m_1!/2) \geq 2^{c+1}$. *Then* G_k *is* $(c+2)$*-generated.*

Proof. Note that, under the given conditions, $m_1 \geq 5$, hence each A_{m_i} is a non-abelian finite simple group. Since G_k is the direct product of the groups $A_{m_i}^{f(m_i)}$, with $m_i \neq m_j$ for $i \neq j$, it is sufficient to prove that $A_m^{f(m)}$ is $(c+2)$-generated for every $m \geq m_1$.

Theorem 3.1 states that the maximal integer $h = h_{A_m}(c+2)$ such that A_m^h is $(c+2)$-generated satisfies the bound $h \geq (m!/2)^{c+1}/\log(m!/2)$. As $m_1!/\log(m_1!/2) \geq 2^{c+1}$ and $m \geq m_1$, we have that $m!/\log(m!/2) \geq 2^{c+1}$. Hence

$$h \geq \frac{(m!/2)^{c+1}}{\log(m!/2)} \geq (m!)^{c}.$$

Since $f(m) \leq (m!)^{c} \leq h$, we conclude that $A_m^{f(m)}$ is $(c+2)$-generated. □

Corollary 3.3. *Assume that* $m_1!/\log(m_1!/2) \geq 2^{c+1}$. *Then*

$$|\mu(H, G_k)| \leq |G_k : H|^{c+3}$$

for each subgroup H *of* G_k

Proof. By Proposition 3.2 we know that G_k is $(c+2)$-generated. Each monolithic image L of G_k is isomorphic to A_{m_i}, for some i, and $L = \mathrm{soc}(L)$. By Theorem 2.3, for any $X \leq L$

$$|\mu(X, L)| \leq |L : X|^{\beta} = |\mu(X\,\mathrm{soc}(L), L)| \cdot |X\,\mathrm{soc}(L) : X|^{\beta}.$$

We can thus apply Theorem 2.4 to deduce that for each open subgroup H of G_k

$$|\mu(H, G_k)| \leq |G_k : H|^{\tilde{a}},$$

where $\tilde{a} = \max(\beta + 1, (c+2) + 1) = c + 3$, as $c + 2 \geq \beta$. □

Lemma 3.4. *Let* $n > 5$ *be an integer and let* $n_1 \dots n_t = n$ *be a nontrivial (positive) factorization of* n, *that is* $t \neq 1$ *and* $n_i > 1$ *for every* i. *Then*

$$\prod_{i=1}^{t} n_i! \leq \frac{n!}{n^2}.$$

Lemma 3.5. [23, Lemma 8] *For every* $\epsilon > 0$ *there exists an integer* $N = N(\epsilon)$ *such that, if* $\mathrm{soc}(G)$ *is alternating and* $n > N(\epsilon)$, *then* G *has less than* $n^{1+\epsilon}$ *maximal subgroups of index* n.

Lemma 3.6. *There exists an integer* $N \geq 5$ *such that if* $m_1 \geq N$, *then for every integer* n *there are at most*

$$n^3(n!)^c$$

maximal subgroups of index n *in* G_k.

Proof. By Lemma 3.5, applied with $\epsilon = 1/2$, there exists an integer $N(1/2)$ such that if $n \geq N(1/2)$, then an alternating group has less than $n^{1+1/2}$ maximal subgroups of index n. We set N to be the minimal integer greater than $N(1/2)$ and satisfying the condition $N!/\log(N/2) \geq 2^{c+1}$. Note that for $m_1 \geq N$, the index of any subgroup of G_k is always at least N.

Let M be a maximal subgroup of index n in G_k. Since G_k is a direct product of nonabelian finite simple groups (namely A_m, for some $m \geq m_1$), then one of the following holds (see e.g. [21, Lemma 16]):

1) $M = T_i \times K$, where T_i is the product of all minimal normal subgroups of G_k but one, isomorphic to some A_m, and K is a maximal subgroup of A_m,
2) $M = T_{i,j} \times D$, where $T_{i,j}$ is the product of all minimal normal subgroups of G_k but two isomorphic to A_m and D is a "diagonal subgroup" of $A_m \times A_m$, i.e. there exists and an automorphism ϕ of A_m such that $D = \{(x, x^{\phi}) \mid x \in A_m\}$.

In case (1), we have at most $f(m)$ choices for A_m. Moreover, by the definition of N, there are less then $n^{1+1/2}$ choices for the maximal subgroup K of index n in A_m. Thus we have at most

$$\sum_{m \leq n} n^{1+1/2} f(m) \leq \sum_{m \leq n} n^{1+1/2} (m!)^c \leq n^{2+1/2} (n!)^c$$

maximal subgroups M of the first type, since $m \leq n$.

In case (2), we notice that $n = |G_k : M| = |A_m| = m!/2$, hence $m! = 2n$. We have at most $f(m)(f(m)-1)/2$ choices for $T_{i,j}$, and once $T_{i,j}$ is fixed, we have $|\operatorname{Aut}(A_m)| \leq 2m! = 4n$ choices for the automorphism ϕ. Since $f(m) \leq (m!)^c$, we have at most

$$\frac{f(m)(f(m)-1)}{2} \cdot 2m! \leq (2n)^c((2n)^c - 1)2n \leq (2n)^{2c+1}$$

maximal subgroups M of this type. Actually, since $m \geq 5$, we have this type of maximal subgroups only for $n \geq 5!/2$, and thus we have at most

$$(2n)^{2c+1} \leq \frac{(n!)^c}{n}$$

of these subgroups. Adding the two bounds, we conclude that there are at most

$$n^{2+1/2}(n!)^c + \frac{(n!)^c}{n} \leq n^3(n!)^c$$

maximal subgroups of index n in G_k. □

Proposition 3.7. *There exists an integer $N \geq 5$ such that if $m_1 \geq N$, then*

$$|a_n(G_k)| \leq n^c(n!)^c$$

for every integer n. In particular, if $n > m_k$, then

$$|a_n(G_k)| \leq \frac{3}{n}(n!)^c.$$

Proof. Let N be the integer defined in Lemma 3.6 and let Ω be the set of subgroups H of index n in G_k such that $\mu(H, G_k) \neq 0$. If $H \in \Omega$, then, by [19, Theorem 1], there exist a factorization $n = n_1 \cdots n_t$ (with $n_i > 1$) and a family of subgroups $Y_1, \dots, Y_t$ of G_k satisfying the following properties:

(1) $H = Y_1 \cap \cdots \cap Y_t$;
(2) $|G_k : Y_i| = n_i$;
(3) $\mu(Y_i, G_k) \neq 0$ for every i;
(4) either Y_i is a maximal subgroup of G_k or there exists a normal subgroup K_i of G_k such that $K_i \leq Y_i$ and G_k/K_i is simple.

Let Ω_1 be the set of subgroups $H \in \Omega$ such that $t \neq 1$, let Ω_2 be the set of subgroups $H \in \Omega$ such that there exists a normal subgroup K of G_k such that $K \leq H$ and G/K is simple, and let $\Omega_3 = \Omega \setminus (\Omega_1 \cup \Omega_2)$.

Note that if $H \in \Omega_2$, then there exists a normal subgroup K of G_k such that $K \leq H$ and $G/K \cong A_m$ for an integer $m \leq \min(n, m_k)$. For each $m \leq \min(n, m_k)$, we have at most $f(m)$ choices for K and, once K is fixed, by Theorem 2.3, we have at most $b_n(A_m) \leq n^\alpha$ choices for H/K. Moreover, $\mu(H, G_k) = \mu(H/K, G_k/K) \leq n^\beta$. Thus

$$\left| \sum_{H \in \Omega_2} \mu(H, G_k) \right| \leq \sum_{m \leq n} \left(f(m) n^\alpha n^\beta \right) \leq n^{\alpha+\beta+1}(\min(n, m_k)!)^c. \tag{3.1}$$

If $H \in \Omega_3$, then H is a maximal subgroup of G_k, hence $\mu(H, G_k) = -1$. In the proof of Lemma 3.6 we have seen that G_k has at most $(n!)^c/n$ of this kind of maximal subgroups, thus

$$\left| \sum_{H \in \Omega_3} \mu(H, G_k) \right| \leq \frac{(n!)^c}{n}. \tag{3.2}$$

Let now $H \in \Omega_1$. Then there exists a nontrivial factorization $n = n_1 \cdots n_t$ and a family of subgroups $Y_1, \dots, Y_t$ of G_k with $t \neq 1$ satisfying the above properties. There are at most n^2 possible choices for the factorization $n = n_1 \cdots n_t$ (see [14]): fix one of them. By Lemma 3.6 we have at most $n_i^3 (n_i!)^c$ choices of Y_i if Y_i is maximal. If Y_i is not maximal, then Y_i/K_i is a subgroup of $G_k/K_i \cong A_m$, for some $m \leq n_i$, with nontrivial value of the Möbius function. For each $m \leq n_i$, we have at most $f(m) \leq (m!)^c$ choices for K_i and then, by Theorem 2.3, at most $b(n_i) \leq n_i^\alpha$ choices for Y_i/K_i. Therefore we have at most

$$n_i^3 (n_i!)^c + \sum_{m=m_1}^{n_i} n_i^\alpha f(m) \leq n_i^3 (n_i!)^c + n_i \cdot n_i^\alpha (n_i!)^c \leq n_i^{\alpha+5} (n_i!)^c$$

choices for Y_i. Thus, applying Lemma 3.4 we get

$$\begin{aligned} |\Omega_1| &\leq \sum_{\substack{n_1 \cdots n_t = n \\ t \neq 1}} \left(\prod_{i=1}^t n_i^{\alpha+5} (n_i!)^c \right) \\ &\leq n^2 n^{\alpha+5} \left(\frac{n!}{n^2} \right)^c = n^{\alpha+7-2c} (n!)^c. \end{aligned}$$

By Corollary 3.3, $\mu(H, G_k) \leq n^{c+3}$ for every subgroup H of G_k, hence

$$\left| \sum_{H \in \Omega_1} \mu(H, G_k) \right| \leq |\Omega_1| n^{c+3} \leq n^{\alpha+10-c} (n!)^c. \tag{3.3}$$

Combining (3.1), (3.2) and (3.3) and taking into account that $c \geq \alpha + \beta + 11$, we deduce that

$$\begin{aligned} |a_n(G_k)| &\leq n^{\alpha+\beta+1} (\min(n, m_k)!)^c + n^{\alpha+10-c} (n!)^c + \frac{(n!)^c}{n} \\ &\leq n^c (n!)^c. \end{aligned}$$

Whenever $n > m_k$, a sharper bound holds: indeed $\min(n, m_k)! = m_k! \leq (n-1)! = n!/n$ hence from (3.1), (3.2) and (3.3) we conclude that

$$\begin{aligned} |a_n(G_k)| &\leq n^{\alpha+\beta+1} \left(\frac{n!}{n} \right)^c + n^{\alpha+10-c} (n!)^c + \frac{(n!)^c}{n} \\ &= n^{\alpha+\beta+1-c} (n!)^c + n^{\alpha+10-c} (n!)^c + \frac{(n!)^c}{n} \\ &\leq \frac{3}{n} (n!)^c \end{aligned}$$

as claimed. $\square$

Proposition 3.8. *Under the assumption of Proposition 3.7 and for any $n > m_k$*

$$|c_n(G_k)| \leq (n!)^c.$$

Proof. By Lemma 2.1

$$|c_n(G_k)| \leq \sum_{n_1 \cdots n_t = n} |a_{n_1}(G_k) \dots a_{n_t}(G_k)|,$$

where the sum runs over the set of all ordered factorizations $n_1 \dots n_t = n$ with $n_i > 1$. Notice that number $H(n)$ of ways to factor a natural number n into an ordered product of integers, each factor greater than one, is at most $n^{\zeta^{-1}(2)} \leq n^2$

[3]. As $n > m_k$, it follows from Proposition 3.7 that $|a_n(G_k)| \leq \frac{3}{n}(n!)^c$, while the bound $|a_{n_i}(G_k)| \leq n_i^c(n_i!)^c$ suffices for any nontrivial factorization $n_1 \cdots n_t = n$ of n. Indeed, applying Lemma 3.4, we get

$$\begin{aligned}
|c_n(G_k)| &\leq \sum_{\substack{n_1 \cdots n_t = n \\ t \neq 1}} \left(\prod_{i=1}^{t} |a_{n_i}(G_k)| \right) + |a_n(G_k)| \\
&\leq \sum_{\substack{n_1 \cdots n_t = n \\ t \neq 1}} \left(\prod_{i=1}^{t} n_i^c (n_i!)^c \right) + \frac{3}{n}(n!)^c \\
&\leq H(n) \cdot n^c \left(\frac{n!}{n^2} \right)^c + \frac{3}{n}(n!)^c \\
&\leq (n!)^c,
\end{aligned}$$

where the last inequality follows from the fact that $c \geq 3$. □

Now we are ready to prove Theorem 1.1 by constructing a non-prosoluble finitely generated group G such that every coefficient of $(P_G(s))^{-1}$ is nonnegative.

Proof of Theorem 1.1. Let $c = \alpha + \beta + 11$, where α and β are the constants defined in Theorem 2.3, and let N be the constant defined in Proposition 3.7.

We set $m_1 = N$ and we note that, by the definition of N, $m_1/\log(m_1/2) \geq 2^{c+1}$. Then we set $f_1 = 1$ and $G_1 = A_{m_1}$. The probabilistic zeta function of $G_1 = A_{m_1}$ has some negative coefficients (see Section 4): let m_2 the first integer such that $c_{m_2}(G_1) < 0$ and set

$$f_2 = -\frac{c_{m_2}(G_1)}{m_2} \quad \text{and} \quad G_2 = A_{m_1} \times A_{m_2}^{f_2}.$$

Note that, by Proposition 3.8, $f_2 \leq (m_2!)^c$ and, by Lemma 2.2, m_2 divides $c_{m_2}(G_1)$, hence f_2 is actually an integer.

Assume that we have defined two sequences of integers $m_1 < m_2 < \cdots < m_k$ and $f_1, f_2, \ldots, f_k$, such that $f_i \leq (m_i!)^c$ and the coefficients of the probabilistic zeta function of $G_k = \prod_{i=1}^{k} A_{m_i}^{f_i}$ satisfy

$$c_n(G_k) \geq 0, \quad \forall\, n \leq m_k.$$

If all coefficients $c_n(G_k)$ are nonnegative, then we set $G = G_k$, and we are finished. Otherwise, we define m_{k+1} to be the first integer n such that $c_n(G_k) < 0$. By Lemma 2.2, m_{k+1} divides $c_{m_{k+1}}(G_k)$. So, we set $f_{k+1} = -c_{m_{k+1}}(G_k)/m_{k+1}$ and

$$G_{k+1} = G_k \times A_{m_{k+1}}^{f_{k+1}} = \prod_{i=1}^{k+1} A_{m_i}^{f_i}.$$

Note that, since $m_{k+1} > m_k$, from Proposition 3.8 (where f is a function such that $f(m_i) = f_i$) it follows that $f_{k+1} \leq (m_{k+1}!)^c$.

By equation 2.2

$$P_{G_{k+1}}(s) = P_{G_k}(s) \cdot P_{A_{m_{k+1}}^{f_{k+1}}}(s). \tag{3.4}$$

Moreover, by equation 2.3, we can evaluate the first nontrivial terms of $P_{A_{m_{k+1}}^{f_{k+1}}}(s)$

$$\begin{aligned}
P_{A_{m_{k+1}}^{f_{k+1}}}(s) &= \prod_{i=0}^{f_{k+1}-1}\left(P_{A_{m_{k+1}}}(s) - \frac{i|\operatorname{Aut}(A_{m_{k+1}})|}{|A_{m_{k+1}}|^s}\right) \\
&= \prod_{i=0}^{f_{k+1}-1}\left(1 - \frac{m_{k+1}}{{m_{k+1}}^s} + \cdots\right) \\
&= 1 - \frac{f_{k+1}m_{k+1}}{{m_{k+1}}^s} + \cdots,
\end{aligned}$$

hence

$$P_{A_{m_{k+1}}^{f_{k+1}}}(s)^{-1} = 1 + \frac{f_{k+1}m_{k+1}}{{m_{k+1}}^s} + \cdots.$$

Since $f_{k+1}m_{k+1} = -c_{m_{k+1}}(G_k)$, from

$$\begin{aligned}
P_{G_{k+1}}(s)^{-1} &= P_{G_k}(s)^{-1} \cdot P_{A_{m_{k+1}}^{f_{k+1}}}(s)^{-1} \\
&= \left(\sum_n \frac{c_n(G_k)}{n^c}\right) \cdot \left(1 + \frac{f_{k+1}m_{k+1}}{{m_{k+1}}^s} + \cdots\right)
\end{aligned}$$

we deduce that $c_{m_{k+1}}(G_{k+1}) = 0$ and so the coefficients $c_n(G_{k+1})$ are nonnegative for every $n \le m_{k+1}$. This shows that the chosen integers m_{k+1} and f_{k+1} satisfies the above conditions.

Let G be the inverse limit of the finite groups G_k. By Proposition 3.2, each G_k is $(c+2)$-generated. Therefore G is $(c+2)$-generated.

Let $P_G(s)^{-1} = \sum_n c_n(G)/n^s$. Note that $c_n(G) = c_n(G_k)$ whenever $n \le m_k$, since $P_G(s)^{-1} = P_{G_k}^{-1}(s)P_H(s)^{-1}$ for $H = \prod_{j>k} A_{m_j}^{f_j}$ and $c_n(H) = 0$ for every $0 \ne n \le m_{k+1}$. It follows that all the coefficients $c_n(G)$ of the probabilistic zeta function of G are nonnegative. □

4. Simple groups

We know no example of a nonabelian finite simple group G for which the probabilistic zeta function $(P_G(s))^{-1}$ has no negative coefficients. In the case of the small simple groups for which the table of marks is available, the existence of negative coefficients in $(P_G(s))^{-1}$ can be easily detected using GAP.

In the case of alternating groups, we may use the following result: if $G = A_n$, $n \ge 9$ and $|A_n : K| \le n(n-1)$, then K is either a point-stabilizer, or a 2-set stabilizer, or the intersection of two point-stabilizers (see for example [11, Theorem 5.2A]). This implies

$$P_G(s) = 1 - \frac{n}{n^s} - \frac{n(n-1)/2}{(n(n-1)/2)^s} + \frac{n(n-1)}{(n(n-1))^s} + \ldots$$

and consequently

$$(P_G(s))^{-1} = 1 + \frac{n}{n^s} + \frac{n(n-1)/2}{(n(n-1)/2)^s} - \frac{n(n-1)}{(n(n-1))^s} + \ldots$$

has a negative coefficient for $n(n-1)$. For $5 \le n \le 8$, we can use GAP to show the existence of negative coefficients in $(P_G(s))^{-1}$.

When G is a simple group of Lie type defined over a field of characteristic p, one can consider the inverse of the series $P_G^{(p)}(s) = \sum_{(n,p)=1} a_n(G)/n^s$, which can be easily described since it depends only on the parabolic subgroups of G (see [26, Theorem 17]). For example, it is not difficult to see that if $G \neq PSL(2,q)$ is an untwisted group of Lie type, then $(P_G^{(p)}(s))^{-1}$ has at least a negative coefficient. Thus also $(P_G(s))^{-1}$ has a negative coefficient. The case $G = PSL(2,q)$ requires a more detailed case by case analysis, but the probabilistic zeta function in known [25] and it is possible to see again that there is a negative coefficient.

5. The Probabilistic Zeta Function of $C_2^2 \times C_5^2 \times A_5$.

It seems quite challenging to construct a possible example of a finite non-soluble group whose probabilistic zeta function has no negative coefficients. To describe some of the difficulties that arises, in this section we sketch the calculation for the "easy" group $G = C_2^2 \times C_5^2 \times A_5$; here the polynomials involved in the factorization of $P_G(s)$ are all known and easy to handle. We will see that the first negative coefficient of $P_G^{-1}(s)$ occurs for $n = 50000$.

Recall that

$$P_{A_5}(s) = 1 - 5/5^s - 6/6^s - 10/10^s + 20/20^s + 60/30^s - 60/60^s.$$

Thus, the probabilistic zeta function $(P_{A_5}(s))^{-1}$ has a negative coefficient for $n = 20$: $c_{20}(A_5) = -20$.

Let $G = H \times A_5$ where $H = C_2^2 \times C_5^2$. Note that

$$P_G(s) = P_{C_2^2}(s) \cdot P_{C_5^2}(s) \cdot P_{A_5}(s),$$

as the chief factors of G in the sections C_2^2, C_5^2 and A_5 are not G-equivalent.

Moreover

$$P_{C_p^2}(s)^{-1} = \left(\sum_{i=0}^{\infty} \left(\frac{1}{p^s} \right)^i \right) \left(\sum_{j=0}^{\infty} \left(\frac{p}{p^s} \right)^j \right) = \sum_{n=0}^{\infty} \frac{\left(\sum_{j=0}^{n} p^j \right)}{p^{ns}}$$

Thus $P_H(s)^{-1} = \sum_{i=0}^{\infty} c_n(H)/n^s$ where, for any i and k,

$$c_{2^i 5^k}(H) = \left(\sum_{l=0}^{i} 2^l \right) \left(\sum_{t=0}^{k} 5^t \right) = \frac{\left(2^{i+1} - 1\right) \left(5^{k+1} - 1\right)}{4}$$

and $c_n(H) = 0$ if n is not of the form $2^i 5^k$.

As $P_G(s) = P_H(s) \cdot P_{A_5}(s)$ we can evaluate the coefficients $c_n(G)$ of $P_G(s)^{-1}$ by the formula

$$P_G(s)^{-1} \cdot P_{A_5}(s) \quad = \quad P_H^{-1}(s)$$

which gives $c_n(H) = \sum_{\substack{ur=n \\ u \neq 1}} a_u(A_5) c_r(G)$ and thus

$$c_{2^i 5^k}(G) = 5 c_{2^i 5^{k-1}}(G) + 10 c_{2^{i-1} 5^{k-1}}(G) - 20 c_{2^{i-2} 5^{k-1}}(G) + c_{2^i 5^k}(H),$$

for $i, k \geq 1$. A straightforward calculation shows that $c_n(G) < 0$ for $n = 50000$ and this is the first negative coefficient of $P_G(s)^{-1}$.

References

1. N. Boston, *A probabilistic generalization of the Riemann zeta functions.* In *Analytic Number Theory* vol. 1, Allerton Park, IL, 1995, Progr. Math. 138 (1996) 155–162.
2. K. S. Brown, The coset poset and probabilistic zeta function of a finite group. *J. Algebra* **225** (2000), 989–1012.
3. B. Chor, P. Lemke and Z. Mador, On the number of ordered factorizations of natural numbers. *Discrete Math.* **214** (2000), no. 1-3, 123–133.
4. V. Colombo and A. Lucchini, On the subgroups with non-trivial Möbius number in the alternating and symmetric groups. *J. Algebra* **324** (2010), 2464–474.
5. F. Dalla Volta and A. Lucchini, Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc., Ser. A* **64** (1998), 82–91.
6. E. Damian and A. Lucchini, Profinite groups in which the probabilistic zeta function coincides with the subgroup zeta function. *J. Algebra* **402** (2014) 92–119.
7. E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* **265** (2003), no. 2, 651–668.
8. E. Detomi and A. Lucchini, Recognizing soluble groups from their probabilistic zeta functions. *Bull. London Math. Soc.* **35** (2003), no. 5, 659–664.
9. E. Detomi and A. Lucchini, Profinite groups with multiplicative probabilistic zeta function. *J. London Math. Soc. (2)* **70** (2004), no. 1, 165–181.
10. E. Detomi and A. Lucchini, *Crowns in profinite groups and applications.* In *Noncommutative algebra and geometry*, 47–62, Lect. Notes Pure Appl. Math., 243, Chapman & Hall/CRC, Boca Raton, FL, 2006.
11. J. D. Dixon and B. Mortimer, *Permutation groups.* Graduate Texts in Mathematics, Vol. 163 (Springer-Verlag, 1996).
12. W. Gaschütz, Praefrattinigruppen. *Arch. Math.* **13** (1962), 418–426.
13. P. Hall, The Eulerian functions of a group. *Quart. J. Math.* **7** (1936), 134–151.
14. V. C. Harris and M. V. Subbarao, On product partitions of integers. *Canad. Math. Bull.* **34** (1991), 474–479.
15. T. Hawkes M. Isaacs, and M. Özaydin, On the Möbius function of a finite group. *Rocky Mountain J. Math.* **19** (1989), 1003–1034.
16. J. Lafuente, Crowns and centralizers of chief factors of finite groups. *Comm. Algebra* **13** (1985), 657–668.
17. A. Lucchini, The X-Dirichlet polynomial of a finite group. *J. Group Theory* **8** (2005), 171–188.
18. A. Lucchini, Subgroups of solvable groups with non-zero Möbius function. *J. Group Theory* **10** (2007), 633–639.
19. A. Lucchini, On the subgroups with non-trivial Möbius number. *J. Group Theory* **13** (2010), 589–600.
20. A. Lucchini, On profinite groups with polynomially bounded Möbius numbers. *J. Group Theory* **14** (2011), no. 2, 261–271.
21. A. Mann, Positively finitely generated groups. *Forum Math.* **8** No. 4 (1996), 429–459.
22. A. Mann, A probabilistic zeta function for arithmetic groups. *Internat. J. Algebra Comput.* **15** (2005), 1053–1059.
23. A. Mann and A. Shalev, Simple groups, maximal subgroups and probabilistic aspects of profinite groups. *Israel J. Math.* **96** (1996) 449–468.
24. N. E. Menezes, M. Quick and C. M. Roney-Dougal, The probability of generating a finite simple group. *Israel J. Math.* **198:1** (2013), 371–392.
25. M. Patassini, The probabilistic zeta function of $PSL(2,q)$, of the Suzuki groups ${}^2B_2(q)$ and of the Ree groups ${}^2G_2(q)$. *Pacific J. Math.* **240** (2009), no. 1, 185–200.
26. M. Patassini, On the irreducibility of the Dirichlet polynomial of a simple group of Lie type. *Israel J. Math.* **185** (2011), 477–507.
27. P. Jiménez-Seral and J. Lafuente, On complemented nonabelian chief factors of a finite group. *Israel J. Math.* **106** (1998), 177–188.

Eloisa Detomi, Università degli Studi di Padova, Dipartimento di Ingegneria dell'Informazione, email: eloisa.detomi@unipd.it

Andrea Lucchini, Università degli Studi di Padova, Dipartimento di Matematica "Tullio Levi-Civita", email: lucchini@math.unipd.it