NORMALLY ζ-REVERSIBLE PROFINITE GROUPS

LEONE CIMETTA AND ANDREA LUCCHINI

Abstract. We examine (finitely generated) profinite groups in which two formal Dirichlet series, the normal subgroup zeta function and the normal probabilistic zeta function, coincide; we call these groups normally ζ-reversible. We conjecture that these groups are pronilpotent and we prove this conjecture if G is a normally ζ-reversible satisfying one of the following properties: G is prosoluble, G is perfect, all the nonabelian composition factors of G are alternating groups.

Assume that G is a profinite group with the property that for each positive integer n, G contains only finitely many open subgroups of index n. We denote by $\zeta_G(s)$ the Dirichlet generating function associated with the sequence counting the number of open subgroups of index n in G: so

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

where $a_n(G)$ is the number of open subgroups of G of index n and s is a complex variable. Another sequence of nonnegative integers can be associated to G by setting $b_n(G) = \sum_{|G:H|=n,\ H\leq_o G} \mu(H,G)$, where the Möbius function μ of the lattice of open subgroups of G is defined recursively by $\mu(G,G) = 1$ and $\sum_{H\leq K\leq_o G} \mu(K,G) = 0$ for any proper open subgroup $H <_o G$. Again we can consider the corresponding Dirichlet generating function

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

The study of the subgroup sequence $\{a_n(G)\}_n$ and the corresponding zeta function $\zeta_G(s)$ started with [5]; since then there has been an intense research activity aiming at understanding analytical properties of subgroup zeta functions and their local factors for finitely generated nilpotent groups.

The formal inverse of $p_G(s)$ is the probabilistic zeta function which was first introduced and studied by A. Mann in [15] for finitely generated profinite groups and by N. Boston in [1] in the case of finite groups. A central role in the investigation of the properties of the probabilistic zeta function was played by the probabilistic meaning of $p_G(t)$ when G is a finite group and t is a positive integer: Hall in [9] showed that $p_G(t)$ is equal to the probability that t random elements of G generate G. In [15] Mann made a conjecture which implies that $p_G(s)$ has a similar probabilistic meaning for a wide class of profinite groups. More precisely, define $\mathrm{Prob}_G(t) = \mu(\Omega_G(t))$, where μ is the normalised Haar measure uniquely defined on the profinite group G^t and $\Omega_G(t)$ is the set of generating t-tuples in G (in the topological sense). We say that G is positively finitely generated if there exists a

positive integer t such that $\mathrm{Prob}_G(t) > 0$. Mann considered the infinite sum

$$\sum_{H \leq G} \frac{\mu(H,G)}{|G:H|^s}.$$

As it stands, this is not well defined, but he conjectured that this sum is absolutely convergent if G is positively finitely generated. The Dirichlet series $p_G(s)$ can be obtained from this infinite sum, grouping together all terms with the same denominator so in particular Mann's conjecture implies that if G is positively finitely generated, then $p_G(s)$ converges in some right half-plane and $p_G(t) = \mathrm{Prob}_G(t)$, when $t \in \mathbb{N}$ is large enough. The second author proved in [13] that this is true if G is a profinite group with polynomial subgroup growth. But even when the convergence is not ensured, the formal Dirichlet series $p_G(s)$ encodes information about the lattice generated by the maximal subgroups of G and combinatorial properties of the probabilistic sequence $\{b_n(G)\}$ reflect on the structure of G. For example in [6] it is proved that a finitely generated profinite group G is prosoluble if and only if the sequence $\{b_n(G)\}$ is multiplicative.

One can ask whether and how the two formal Dirichlet series $\zeta_G(s)$ and $p_G(s)$ are related. The first example that it is usually presented is when $G = \widehat{\mathbb{Z}}$, the profinite completion of an infinite cyclic group. In this case $\zeta_{\widehat{\mathbb{Z}}}(s) = \sum_n 1/n^s$ is the Riemann zeta function, while $p_{\widehat{\mathbb{Z}}}(s) = \sum_n \mu(n)/n^s$ and an easy application of the Möbius Inversion Formula shows that $p_{\widehat{\mathbb{Z}}}(s)$ and $\zeta_{\widehat{\mathbb{Z}}}(s)$ are one the multiplicative inverse of the other. A natural question is whether this is a particular coincidence or a more general phenomenon. Motivated by this question, in [4] it was introduced the notion of ζ-reversible profinite groups: a profinite group G is said to be ζ-reversible if and only if the formal identity $p_G(s)\zeta_G(s) = 1$ is satisfied. This definition can be introduced and studied independently of the convergence and possible analytic properties of $p_G(s)$ and $\zeta_G(s)$. Hence ζ-reversible only means that $\sum_{rs=n} a_r(G)b_s(G) = 0$ for each $n > 1$ while $a_1(G)b_1(G) = 1$. In [4] it is proved that, even when the convergence of the two series involved is not ensured, the information that G is ζ-reversible can have useful consequences. The results obtained in [4] indicate that ζ-reversibility is a strong property: a ζ-reversible group must have a sort of uniform subgroup structure, in the sense that the open subgroups, even when they are not all isomorphic, must have a comparable structure.

In this paper, our aim is to study a corresponding property, obtained by restricting the attention to the open normal subgroups of a profinite group G. We assume that G is a profinite group with the property that for each positive integer n, G contains only finitely many open normal subgroups of index n (a sufficient, but not necessary, condition for satisfying this property is that G is topologically finitely generated). For any $n \in \mathbb{N}$, let $a_n^{\triangleleft}(G)$ be the number of the open normal subgroups of G and let $b_n^{\triangleleft}(G) = \sum_{|G:H|=n, H \trianglelefteq_o G} \mu^{\triangleleft}(H,G)$, where $\mu^{\triangleleft}$ is the Möbius function in the lattice of the open normal subgroups of G. Again the properties of the sequences $\{a_n^{\triangleleft}(G)\}_{n\in\mathbb{N}}$ and $\{b_n^{\triangleleft}(G)\}_{n\in\mathbb{N}}$ can be encoded by the corresponding Dirichlet generating function

$$\zeta_G^{\triangleleft}(s) = \sum_{n\in\mathbb{N}} \frac{a_n^{\triangleleft}(G)}{n^s} \quad \text{and} \quad p_G^{\triangleleft}(s) = \sum_{n\in\mathbb{N}} \frac{b_n^{\triangleleft}(G)}{n^s}$$

called, respectively, the normal subgroup zeta function and the normal probabilistic zeta function of G. Again $p_G^{\triangleleft}(s)$ has a probabilistic meaning: if G is a finite group

and $t \in \mathbb{N}$, then $p_G^{\triangleleft}(t)$ is the probability that t randomly chosen elements of G generate a subgroup whose normal closure is G (see [7, Section 3]). We will say that a profinite group G is normally ζ-reversible if $\zeta_G^{\triangleleft}(s)p_G^{\triangleleft}(s) = 1$. We conjecture that a normally ζ-reversible profinite group is pronilpotent. An evidence for this conjecture will be given by the following theorem, which implies in particular that a prosoluble normally ζ-reversible profinite group is pronilpotent.

Theorem 1. *Assume that G is a normally ζ-reversible profinite group. If there is no open normal subgroup $N \triangleleft G$ such that G/N is a nonabellian simple group, then G is pronilpotent.*

Our main results are the following:

Theorem 2. *A non trivial normally ζ-reversible profinite group cannot be perfect.*

Theorem 3. *Let G be a normally ζ-reversible profinite group. If G is not pronilpotent, then G has as a composition factor a nonabelian simple group which is not an alternating group.*

The proofs of the previous two theorems rely on the following result (see Theorem 22): suppose that a normally ζ-reversible profinite group G admits a finite nonabelin simple group as an epimorphic image; then there exists a pair (H, T), where H is a finite epimorphic image of G and T is a finite nonabelin simple group, with the following properties:

(1) $|H| = |T|^2$.
(2) H contains a unique minimal normal sugroup N.
(3) Either H/N is nilpotent, or there exists a finite nilpotent group X and a nonabelian simple group S such that $H/N \cong X \times S$. In the latter case $|T| \leq |S|$ and $\pi(S) = \pi(T)$.

With the help of the classification of the finite simple groups, we prove that there are no pairs (H, T) with these properties, under the additional assumption that either H is perfect or all the nonabelian composition factors of H are alternating groups.

1. Notations and general auxiliary results

Given an integer k and a set π of primes, k_π will be the greatest divisors of k whose prime divisors belong to π. In particular, with a little abuse of notation, if p is a prime we will call k_p the greatest power of p dividing k. Moreover we will say that k is a π-number if $k_\pi = k$.

Let $\mathcal{R}$ be the ring of formal Dirichlet series with integer coefficients. For every set π of prime number, we consider the ring endomorphism of $\mathcal{R}$ defined by:

$$F(s) = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s} \mapsto F_\pi(s) = \sum_{n\in\mathbb{N}} \frac{a_n^*}{n^s}$$

where $a_n^* = a_n$ if n is a π-number, $a_n^* = 0$ otherwise.

An element $F(s) = \sum_n a_n/n^s \in \mathcal{R}$ is said to be multiplicative if $a_{rs} = a_r a_s$ whenever $(r, s) = 1$ (equivalently $F(s)$ coincides with the infinite formal product $\prod_p F_p(s)$of its p-local factors). It can be easily proved that if $F(s)$ is multiplicative, then also the formal inverse $F(s)^{-1}$ is multiplicative.

During our proofs we will need information about the "prime gap". For our purpose the following result will suffice.

Lemma 4. *For every integer $n \geq 5$, $n \notin \{6, 10\}$, there exist two primes p, q such that $\frac{n}{2} < p < q \leq n$.*

This lemma is in fact a corollary of a more complete result, proved by Nagura in [14], stating that, if $n \geq 25$, then there is a prime p such that $n \leq p \leq 6n/5$.

We conclude this section by recalling some results concerning the finite non-abelian simple groups.

A crucial role in our proof will be played by the following result:

Theorem 5. [11, Theorem 6.1] *Let S and T be non-isomorphic finite simple groups. If $|S^a| = |T^b|$ for some natural numbers a and b, then $a = b$ and S and T either are $A_2(4)$ and $A_3(2)$ or are $B_n(q)$ and $C_n(q)$ for some $n \geq 3$ and some odd q.*

This result is a consequence of a collection of more general results obtained in [11] and leading to the conclusion that a finite simple group is in general uniquely determined by some partial information on its order encoded by some arithmetical invariants (called Artin invariants). We will make a large use of these results, so we recall here some related definitions.

Definition 6. *Let n be a natural number and r one of its prime divisors. The greatest power of r dividing n is called the contribution of r to n and is denoted by n_r. Moreover, r is called the dominant prime if $n_r > n_q$ for every other prime q. Given a finite group G, we will call the dominant prime of G the dominant prime of its order. We will use the symbol $p(G)$ to denote the dominant prime of G.*

Proposition 7. [11, Theorem 3.3] *The dominant prime of a simple group of Lie type coincides with its characteristic, apart from the following cases:*

(1) $A_1(q)$, where q is a Mersenne prime;
(2) $A_1(q-1)$, where q is a Fermat prime;
(3) $A_1(8)$, ${}^2A_2(3)$, ${}^2A_3(2)$.

Definition 8. *Let G be a finite group and $p = p(G)$ its dominant prime, then*

$$\lambda(G) = \frac{\log(|G|_p)}{\log(|G|)}$$

is called the logarithmic proportion of G.

Proposition 9. [11, Theorems 3.5, 3.6] *Let $x = p^u$ be the contribution of the dominant prime of a finite simple group S of Lie type, then $x^2 < |G| < x^3$, that is*

$$\frac{1}{3} < \lambda(G) < \frac{1}{2}.$$

Definition 10. *Let n be an integer which is not a prime power, let $p = p(n)$ be its dominant prime and p^l its contribution to n, then we define $\omega(n)$ as the largest order of p modulo a prime divisor p_1 of n/p^l. We will call such a p_1 a prominent prime in n.*

Lemma 11. [11, Lemma 4.2] *Given n and $\alpha \in \mathbb{N}$, then $\omega(n^\alpha) = \omega(n)$. Furthermore, if p_1 is prominent in n with contribution $p_1^{l_1}$, then it is also prominent in n^α with contribution $p_1^{l_1\alpha}$.*

Remark 12. *Notice that, if a and b have the same prime divisors and the same dominant prime, then they have also the same prominent prime and $\omega(a) = \omega(b)$.*

Let $S = L(q)$ be a finite simple group of Lie type, defined over a field of cardinality $q = p^r$, where p is a prime (which we will call the characteristic of S). We will factorize the order of a simple group $S = L(q)$ of Lie type in the form

$$|L(q)| = \frac{1}{d} q^h P(q),$$

where d, h and $P(q)$ are given in [11, Table L1]. In particular this order has the *cyclotomic factorization in terms of p*:

$$|L(q)| = \frac{1}{d} p^l \prod_m \Phi_m(p)^{e_m},$$

where $\Phi_m(x)$ is the m-th cyclotomic polynomial. Summing up [11, Proposition 4.5] and [11, Lemma 4.6], we obtain:

Theorem 13. *Let $S = L(q)$ be a simple group of Lie type with characteristic p and $q = p^r$. Then the cyclotomic factorization*

$$|S| = \frac{1}{d} p^{rh} \Phi_{\alpha_1}(p)\Phi_{\alpha_2}(p)\Phi_{\alpha_3}(p)\cdots\Phi_{\alpha_u}(p)$$

satisfies the following properties:

(1) $\alpha_1 > \alpha_2$;
(2) d divides $\Phi_{\alpha_3}(p)\cdots\Phi_{\alpha_u}(p)$ unless $S = A_1(q)$ and $r = 1$;
(3) $\omega(|S|) = \alpha_1$ unless $p = 2$ and $\alpha_1 = 6$.

Definition 14. *Let G be a group with dominant prime p_1, let $p_1^{n_1}$ be its contribution to the order of G. Suppose that p_i is a prime dividing the order of G and that $p_i^{n_i}$ is the contribution to the order. Then p_i is called a good contributor to G if $n_i \log(p_i)\log(3) > n_1 \log(p_1)\log(2)$.*

The good contributors of the finite simple groups are classified in [2].

For later use we need to recall some definitions and results concerning Zsigmondy primes.

Definition 15. *A prime number p is called a* primitive prime divisor *of $a^n - 1$ if it divides $a^n - 1$ but it does not divide $a^e - 1$ for any integer $1 \le e \le n - 1$.*

The following theorem is due to K. Zsigmondy [21]:

Theorem 16 (Zsigmondy's Theorem)**.** *Let a and n be integers greater than 1. There exists a primitive prime divisor of $a^n - 1$ except exactly in the following cases:*

(1) $n = 2$, $a = 2^s - 1$ (i.e. a is a Mersenne prime), where $s \ge 2$.
(2) $n = 6$, $a = 2$.

Primitive prime divisors have a close relation with the cyclotomic factorization described in Theorem 13: if r is a primitive prime divisor of $p^n - 1$, then n is the smallest positive integer with the property that r divides $\Phi_n(p)$.

2. A reduction to a question on finite groups

Assume that G is a profinite group and let $\mathcal{S}$ be the set of the open normal subgroups N of G with the property that $S_N := G/N$ is a nonabelian simple group. Let

$$A_G(s) = P_{G/G'}(s) \quad \text{and} \quad B_G(s) = \prod_{N\in\mathcal{S}} \left(1 - \frac{1}{|S_N|^s}\right).$$

We know from [7, Section 5] that

$$p^{\triangleleft}_G(s) = A_G(s)B_G(s). \tag{2.1}$$

Now consider the two series

$$\Gamma_G(s) := (A_G(s))^{-1} = \sum_n \frac{\gamma_n(G)}{n^s} \text{ and } \Delta_G(s) := (B_G(s))^{-1} = \sum_n \frac{\delta_n(G)}{n^s}. \tag{2.2}$$

Lemma 17. *If G is a normally zeta-reversible profinite group, then*

$$\Gamma_G(s) = \prod_p \Gamma_{G,p}(s) = \prod_p \zeta^{\triangleleft}_{G,p}(s).$$

Proof. Since G is normally ζ-reversible, we have

$$1 = (\zeta^{\triangleleft}_G(s)p^{\triangleleft}_G(s))_p = \zeta^{\triangleleft}_{G,p}(s)p^{\triangleleft}_{G,p}(s) = \zeta^{\triangleleft}_{G,p}(s)A_{G,p}(s)B_{G,p}(s).$$

Since $A_G(s)$ and $\Gamma_G(s)$ are multiplicative series, we deduce

$$\Gamma_G(s) = \prod_p \Gamma_{G,p}(s) = \prod_p A_{G,p}(s)^{-1} = \prod_p \zeta^{\triangleleft}_{G,p}(s)B_{G,p}(s),$$

but there are no nonabelian simple groups whose order is a prime power, thus $B_{G,p}(s) = 1$ for every prime p and we get $\Gamma_G(s) = \prod_p \zeta^{\triangleleft}_{G,p}(s)$. □

Lemma 18. *If G is a normally zeta-reversible profinite group, then for every $n \in \mathbb{N}$, $\gamma_n(G)$ coincides with the number of open normal subgroups N of G with the property that G/N is a nilpotent group of order n.*

Proof. For every $m \in \mathbb{N}$, let $\mathcal{N}_m$ be the set of the open normal subgroups N of G with the property that G/N is nilpotent of order m. Let $n \in \mathbb{N}$ and write $n = q_1 \cdots q_r$ as a product of powers of different primes. If $N_i \in \mathcal{N}_{q_i}$ for every $1 \le i \le r$, then $N = N_1 \cap \cdots \cap N_r \in \mathcal{N}_n$. Conversely every $N \in \mathcal{N}_n$ can be uniquely expressed in the form $N = N_1 \cap \cdots \cap N_r$, with $N_i \in \mathcal{N}_{q_i}$ for every $1 \le i \le r$. This implies that $|\mathcal{N}| = |\mathcal{N}_{q_1}| \cdots |\mathcal{N}_{q_r}|$. On the other hand if q is a prime power and N is an open normal subgroup of G of index q, then G/N, being a p-group, is nilpotent, hence $|\mathcal{N}_q| = a^{\triangleleft}_q(G)$; moreover $a^{\triangleleft}_q(G) = \gamma_q(G)$ by Lemma 17. Hence

$$\gamma_n(G) = \gamma_{q_1}(G) \cdots \gamma_{q_r}(G) = a^{\triangleleft}_{q_1}(G) \cdots a^{\triangleleft}_{q_r}(G) = |\mathcal{N}_{q_1}| \cdots |\mathcal{N}_{q_r}| = |\mathcal{N}|. \quad \square$$

Proof of Theorem 1. If there is no open normal subgroup N of G such that G/N is a nonabelian simple group, then $B_G(s) = 1$, hence, by (2.1), we have $\Gamma_G(s) = A_G(s)^{-1} = p^{\triangleleft}_G(s)^{-1} = \zeta^{\triangleleft}_G(s)$, i.e. $\gamma_n(G) = a^{\triangleleft}_n(G)$ for every $n \in \mathbb{N}$. We conclude from Lemma 18 that G/N is nilpotent for every open normal subgroup N of G. □

Conjecture 1. *If G is a normally ζ-reversible profinite group, then there is no open normal subgroup $N \triangleleft G$ such that G/N is a nonabelian simple group (and consequently G is pronilpotent).*

For the remaining part of this section we will assume that G is a counterexample to the previous conjecture. We will denote with Σ_G the set of the finite nonabelian simple groups which are continuous epimorphic images of G. Take $T \in \Sigma_G$ with the property that the set $\pi = \pi(T)$ of the prime divisors of $|T|$ is minimal and let $M = O^\pi(G)$ be the intersection of the open normal subgroups N of G with the property that G/N is a π-group. It can be easily checked that G/M is a pro-π-group. Moreover $\zeta^{\triangleleft}_{G/M}(s) = \zeta^{\triangleleft}_{G,\pi}(s)$ and $p^{\triangleleft}_{G/M}(s) = p^{\triangleleft}_{G,\pi}(s)$. But then $\zeta^{\triangleleft}_{G/M}(s)p^{\triangleleft}_{G/M}(s) = \zeta^{\triangleleft}_{G,\pi}(s)p^{\triangleleft}_{G,\pi}(s) = (\zeta^{\triangleleft}_G(s)p^{\triangleleft}_G(s))_\pi = 1$, hence G/M is still a normally ζ-reversible profinite group and represents a counterexample to Conjecture 1. So we may assume that $M = 1$. With this assumption, if $S \in \Sigma_G$, then S is a π-group and, by the minimality property of T, $\pi \leq \pi(S)$. Hence $\pi(S) = \pi$ for every $S \in \Sigma_G$. There are only finitely many nonabelian simple groups S with $\pi(S) = \pi$, hence Σ_G is finite. Let $m = |T| = m_1 < m_2 < \cdots < m_u$ be the orders of the nonabelian simple in Σ_G and for $i \in \{1, \ldots, u\}$ let t_i (with $t = t_1$) be the cardinality of the set of the open normal subgroups N of G such that G/N is a nonabelian simple group of order m_i. We must have:

$$\Delta_G(s) = \left(\prod_i \left(1 - \frac{1}{m_i^s}\right)^{t_i}\right)^{-1} = \prod_i \left(\sum_{j=0}^{\infty} \frac{1}{m_i^{s\cdot j}}\right)^{t_i}$$

and

$$\zeta^{\triangleleft}_G(s) = \Gamma_G(s)\Delta_G(s) = \Gamma_G(s) \prod_i \left(1 + \frac{1}{m_i^s} + \frac{1}{m_i^{2s}} + \cdots\right)^{t_i}.$$

We now want to collect information about the open normal subgroups N of G with $|G/N| \leq m^2$. Consider the series

$$\sum_n \frac{a^*_n}{n^s} := \Gamma_G(s) \left(1 + \frac{1}{m^s} + \frac{1}{m^{2s}}\right)^t \prod_{i=2}^{u} \left(1 + \frac{1}{m_i^s}\right)^{t_i}.$$

If $n \leq m^2$, then, as $n < m_i^2$ for $i \neq 1$, we have $a^{\triangleleft}_n(G) = a^*_n$.

Lemma 19. *Let N be an open normal subgroup of G. If $|G/N| < m^2$ then either G/N is nilpotent or $G/N \cong X_1 \times X_2$ where X_1 is nilpotent and X_2 is a nonabelian simple group.*

Proof. If $n < m^2$, then

$$a^{\triangleleft}_n(G) = a^*_n = \gamma_n(G) + \sum_{m_i r = n} t_i \gamma_r(G). \tag{2.3}$$

Let $\mathcal{N}_r$ be the set of the open normal subgroups N of G with the property that G/N is nilpotent of order r and let $\mathcal{S}_i$ be be the set of the open normal subgroups M of G with the property that G/M is a nonabelian simple group of order m_i. Suppose $m_i r = n$. If $N \in \mathcal{N}_r$ and $M \in \mathcal{S}_i$, then $G/(N \cap M) \cong G/N \times G/M$ (since the nilpotent group G/N and the simple group G/M have no common composition factor) and this is the unique way to obtain $N \cap M$ as intersection of two subgroups in $\mathcal{N}_{r^*}$ and $\mathcal{S}_{i^*}$, for some $r^* \leq n$ and $i^* \leq u$. Hence there are at least a^*_n open normal subgroups N of G of index n and with the property that G/N is either nilpotent or is the direct product of a nilpotent subgroup with a finite nonabelian simple group. Since, by (2.3), $a^{\triangleleft}_n(G) = a^*_n$ all the open normal subgroups of G of index n have this property. □

Let us consider now the set of open normal subgroups of index m^2 in G: in this case we have

$$a^{\triangleleft}_{m^2}(G) = a^*_{m^2} = \gamma_{m^2}(G) + \sum_{m_i r = m^2} t_i \gamma_r(G) + \binom{t}{2} + t. \tag{2.4}$$

With the same arguments used in the proof of the previous lemma, it can be easily noticed that:

Lemma 20. *The first three summands in the previous expression of $a^{\triangleleft}_{m^2}(G) = a^*_{m^2}$ have the following meaning:*

1. *$\gamma_{m^2}(G)$ is the number of the open normal subgroups N of index m^2 such that G/N is nilpotent;*
2. *$\sum_{m_i r = m^2} t_i \gamma_r$ is the number of the open normal subgroups N of index m^2 such that G/N is a direct product of a nilpotent group and a nonabelian simple group.*
3. *$\binom{t}{2}$ is the number of the open normal subgroups N of index m^2 such that G/N is the direct product of two nonabelian simple groups of order m.*

Notice that the last summand in equation (2.4) consists of t open normal subgroups of index m^2 that does not fill in any of the three classes described in Lemma 20: let M be one of these normal subgroups and let $H = G/M$.

Lemma 21. *H has a unique minimal normal subgroup.*

Proof. Suppose by contradiction that H has two different minimal normal subgroups N_1, N_2. By Lemma 19, there exists two finite nilpotent groups X_1, X_2 and two finite groups Y_1 and Y_2 that are either trivial or nonabelian and simple such that $G/N_1 \cong X_1 \times Y_1$ and $G/N_2 \cong X_2 \cap Y_2$. Since $N_1 \cap N_2 = 1$, H is a subdirect product of $X_1 \times X_2 \times Y_1 \times Y_2$, However this implies that H is nilpotent, or it is the direct product of two nonabelian simple groups of order m, or it is the direct product of a simple nonabelian group with a nilpotent group; but then M fills in one of the three family of open normal subgroups described in Lemma 20, a contradiction. □

We may summarize the conclusions of this section in the following statement.

Theorem 22. *If Conjecture 1 is false, then there exists a finite nonabelian simple group T and a finite group H with the following properties:*

1. *$|H| = |T|^2$.*
2. *H contains a unique minimal normal sugroup N.*
3. *Either H/N is nilpotent, or there exists a finite nilpotent group X and a nonabelian simple group S such that $H/N \cong X \times S$. In the latter case $|T| \leq |S|$ and $\pi(S) = \pi(T)$.*

3. Perfect profinite groups

In this section we concentrate our attention on the case of perfect profinite groups. Our aim is to prove that a perfect profinite group cannot be normally ζ-reversible.

It follows immediately from Theorem 22 that:

Proposition 23. *If there exists a perfect normally ζ-reversible profinite group, then exist there a finite nonabelian simple group T and a finite group H with the following properties:*

(1) $|H| = |T|^2$.
(2) H *contains a unique minimal normal sugroup* N.
(3) There exists a finite a nonabelian simple group S *such that* $H/N \cong S$. *Moreover* $|T| \leq |S|$ *and* $\pi(S) = \pi(T)$.

Lemma 24. *If H is a finite group satisfying the statement of Proposition 23, then $N = \operatorname{soc} H$ is abelian.*

Proof. Suppose by contradition that N is nonabelian: there exist a nonabelian simple group L and a positive integer u such that $N = L_1 \times \cdots \times L_u$, with $L_i \cong L$ for all i. It must be $u \neq 1$ (otherwise, by the Schreier conjecture, H/N would be soluble). The conjugation action on $\{L_1, \cdots, L_u\}$ induces a homomorphism $\psi : H \to \mathrm{Sym}(u)$ and $\psi(H)$ is a transitive subgroup of $\mathrm{Sym}(u)$. The kernel of this action coincides with N so $S \cong H/N \cong \psi(H)$. In particolar S contains a subgroup of index u. We have two cases:

(1) $S \cong \mathrm{Alt}(n)$ for some n. We must have $n \leq u$. Moreover, by Lemma 4, there exists a prime number r such that $n/2 < r \leq n$, in particular r divides $|S|$ with multiplicity 1. On the other hand $|H| = |T|^2 = |S||N| = |S||L|^u$, hence $r \,|\, |L|$. Since finite nonabelian simple groups have even order, we deduce that $2r$ divides $|L|$ and $(2r)^u$ divides $|N|$, thus
$$\frac{|T|^2}{|S|} = |N| \geq (2r)^u \geq n^u \geq n^n > \frac{n!}{2} = \left|\frac{H}{N}\right| = |S|,$$
but then $|T| > |S|$, against Proposition 23.
(2) S is not an alternating group and has a (faithful) transitive action of degree u. In particular S has a primitive action of degree $v \leq u$, hence, by [16], $|S| \leq 4^v \leq 4^u$. By Proposition 23, $|T| \leq |S|$, hence
$$|L|^u = |N| = \frac{|T|^2}{|S|} \leq |S| \leq 4^u,$$
but then $|L| \leq 4$, contradiction. □

Corollary 25. *If there exists a perfect normally ζ-reversible profinite group, then there exists a triples (S, T, V) with the following properties:*

(1) T and S are finite nonabelian simple groups;
(2) V is an irreducible S-module of dimension a over the field with p elements;
(3) $|T|^2 = |S|\,|V| = |S|p^a$;
(4) $|V| < |T| < |S|$;
(5) $p \in \pi(T) = \pi(S)$;
(6) if $a = 1$, then p divides the order of the Schur multiplier $M(S)$ of S and divides $|S|$ with multiplicity at least 3.

Proof. The first five statements follow immediately from Proposition 23, taking $V = \mathrm{soc}(H)$ (we cannot have $|S| = |T|$, since this would implies $|T| = p^a$). We have only to prove (6). A faithful irreducible representation of a nonabelian simple group cannot have degree 1; thus, if $a = 1$, then V is a central S-module: in particular $H = V.S$ is a central perfect extension of S and, consequently, $|V| =$

p divides $|M(S)|$. Moreover, if $a = 1$ then, by (3), p must divide $|S|$ with odd multiplicity. Now suppose that $a = 1$ and p divides $|S|$ with multiplicity 1: then a Sylow p subgroup of H, having order p^2, is abelian. We apply [10, Proposition 5.6] stating that, if a group J has an abelian Sylow p-subgroup, then p does not divide $|J' \cap Z(J)|$: since $H' = H$ and $Z(H) = \operatorname{soc} H \cong V$, we would have that p does not divide $|V| = p$, a contradiction. □

In the remaining part of this section, we will prove that there is no triple (S, T, V) satisfying the properties listed in the previous corollary. Suppose by contradiction that such a triple (S, T, V) exists.

Remark 26. *Since $|S|p^a = |T|^2$, every prime divisor of $|S|$ different from p divides $|S|$ with even multiplicity.*

Proposition 27. *S is a simple group of Lie type.*

Proof. By Remark 26, it suffices to prove that, if S is alternating or sporadic, then there are at least two primes dividing $|S|$ with odd multiplicity. This can be directly verified for the sporadic groups and for the alternating groups $\mathrm{Alt}(n)$ when $n \leq 10$. For the remaining alternating groups, we deduce from Lemma 4 that there are at least two primes p, q dividing $\mathrm{Alt}(n) = n!/2$ with multiplicity exactly one. □

Proposition 28. *If $a \neq 1$, then p is the characteristic of S.*

Proof. If $a \neq 1$, then a is the degree of a faithful irreducible representation of S over the field of order p. Assume, by contradiction, that p does not coincide with the characteristic of S. We must have $a \geq \delta(S)$, denoting by $\delta(S)$ the smallest degree of a nontrivial irreducible representation of S in cross characteristic. Lower bounds for the degree of irreducible representations of finite groups of Lie type in cross characteristic were found by Landazuri and Seitz [12] and improved later by Seitz and Zalesskii [17] and Tiep [18]. It turns out that $\delta(S)$ is quite large, and, apart from finitely many exceptions, we have $p^{\delta(S)} > |S|$, in contradiction with $|S| > p^a \geq p^{\delta(S)}$. The few exceptions can be easily excluded, proving directly that, for these particular choices of S, there are no T and V with $|T^2| = |S||V|$. For example, if $S = A_n(q)$ with $n \geq 2$, then $|S| < q^{n^2+2n}$ and, except in the exceptional cases $(n, q) = (2, 2), (2, 4), (3, 2), (3, 3)$, we have $\delta(S) \geq \frac{q^{n+1}-q}{q-1} - 1$ [18, Table II], which implies that either $p^\delta(S) > |S|$ or $(n, q) = (2, 3)$. On the other hand, if $(n, q) = (2, 2), (2, 3), (2, 4), (3, 2), (3, 3)$, then there are at least two primes dividing $|S| = |A_n(q)|$ with odd multiplicites, so these cases must be excluded by Remark 26. The other families of finite simple groups of Lie type can be discussed with similar arguments. □

Proposition 29. *The dominant prime of S coincides with the characteristic of S.*

Proof. By Proposition 7, if the dominant prime of S does not coincide with the characteristic of S, then one of the following three cases occurs.

(1) $S = A_1(q)$, with $q = 2^t - 1$ a Mersenne prime. We must have that t is an odd prime but then 2 and q divide $|S| = (q-1) \cdot q \cdot (q+1)/2$ with odd multiplicity, against Remark 26.
(2) $S = A_1(q-1)$ with $q = 2^{2^k} + 1$ a Fermat prime. Since

$$|T|^2 = (q-2) \cdot (q-1) \cdot q \cdot p^a$$

we have that $p = q$, a is odd and $|T|^2 = \left(2^{2^k}+1\right)^{a+1} 2^{2^k}\left(2^{2^k}-1\right)$: this would imply that $2^{2^k}-1$ is a square too, which is impossible.

(3) $S \in \{A_1(8), {}^2A_2(3), {}^2A_3(2)\}$. The orders $|A_1(8)|$ and $|{}^2A_2(3)|$ are divisible by at least two different primes with odd multiplicity, so these two cases must be excluded. If $S = {}^2A_3(2)$, then $|T|^2 = |S|p^a = 2^6 \cdot 3^4 \cdot 5 \cdot p^a$, hence $p = 5$, a is odd and the condition $|T| < |S|$ implies $a = 1, 3, 5$; however it cannot be $a = 1$ since 5 does not divide the order of the Schur multiplies of ${}^2A_3(2)$, and it cannot be $a = 3, 5$ since there exists no simple group of order $2^3 \cdot 3^2 \cdot 5^2$ or $2^3 \cdot 3^2 \cdot 5^3$. □

Corollary 30. *If $a \neq 1$, then p is the dominant prime of S and T.*

Proof. Suppose $a \neq 1$. By Propositions 28 and 29, p is the characteristic and the dominant prime of S. Since $|T|^2 = |S|p^a$, p is also the dominant prime of T. □

Proposition 31. *T is not an alternating group.*

Proof. Let $T = \mathrm{Alt}(m)$, $m \geq 5$. First assume $m \leq 9$. We use [3, p. 239–242] to check that if $|S|$ is a finite simple group with $\pi(S) = \pi(T)$ and $|T|^2 = |S|p^a$ for some prime power p^a, then $m = 6$, $p = 5$, $a = 1$ and $S = {}^2A_3(2)$; however we must exclude this possibility, since 5 does not divide the order of the Schur multiplier of ${}^2A_3(2)$.

So from now on we will assume $m \geq 10$. This implies that 2 is the dominant prime of T [11, Table L.4]. We will prove that the dominant prime of S is 2 too. Suppose, by contradiction, that the dominant prime q of S is not 2. Then, being $|T|^2 = |S|p^a$, we must have $p = 2$ and, by Corollary 30, $a = 1$, so

$$|T|^2 = 2\,|S|\,. \tag{3.1}$$

Let $|T|_2 = 2^t$, $|T|_q = q^h$, then $2^t > q^h$ (as 2 is the dominant prime of T) and, by (3.1), $q^{2h} > 2^{2t-1}$ (as q is the dominant prime of S). Joining these inequalities we get $q^h < 2^t < q^{h+1/2}$, whence $h\log(q) < t\log(2) < \left(h + \frac{1}{2}\right)\log(q)$, and so

$$1 < \frac{t\log(2)}{h\log(q)} < 1 + \frac{1}{2h} \leq \frac{3}{2} < \frac{\log(3)}{\log(2)}. \tag{3.2}$$

By Equation (3.2), q is a good contributor to T, but [2, Theorem 3.8] enlists all good contributors to alternating groups, and for $m \geq 10$, it must be

$$\begin{cases} q = 3 & \text{or} \\ q = 5 & \text{and } m \in \{10, 11, 15, 25, 26, 30\}. \end{cases}$$

Moreover [2, 3.2] gives some useful lower and upper bounds for t, h as linear functions on m. Using these bounds and some direction computations for the small values of m, it can be easily proved that the only case in which we really have $q^{2h} > 2^{2t-1}$ is when $q = 3$ and $m = 15$; however, we can again use [3, p. 239–242] to see that there is no simple group S with $2|S| = |\,\mathrm{Alt}(15)|^2$, against (3.1).

Now we claim that $p \neq 2$. Indeed, assume by contradiction, $p = 2$. By Corollary 30, it must be $a = 1$. If $m = 10$, then we would have $\lambda(S) < 1/3$, in contradiction

with Proposition 9. For $m \geq 11$ we have $\lambda(\mathrm{Alt}(m)) < 1/3$ (see [11, Table L.4]), hence

$$\frac{1}{3} > \frac{\log(|T|_2^2)}{\log(|T|^2)} = \frac{\log(|S|_2) + \log(2)}{\log(|S|) + \log(2)} > \frac{\log(|S|_2)}{\log(|S|)}$$

contradicting again Proposition 9.

Thus S and T both have dominant prime 2 and p is odd. By Proposition 9

$$\left(\frac{m}{e}\right)^m < \frac{m!}{2} = |T| < |S| \leq |S|_2^3 \leq |T|_2^6 . \tag{3.3}$$

Let $|T|_2 = 2^l$, then we can extimate l by

$$l = \sum_{i=1}^{\infty} \left[\frac{m}{2^i}\right] - 1 < \sum_{i=1}^{\infty} \frac{m}{2^i} - 1 = m - 1.$$

This result, joined with (3.3), gives $m < e \cdot 2^{6-12/m}$; in particular $m \leq 165$.

Since $p \neq 2$, we have $|S|_2 = |T|_2^2$ and, by Proposition 9,

$$\frac{1}{3} \leq \frac{\log(|S|_2)}{\log(|S|)} = \frac{\log(|T|_2^2)}{\log(|T|)^2 - a\log(p)}. \tag{3.4}$$

Moreover 3 is dominant prime of $|\mathrm{Alt}(m)|_{2'}$ for every $m \geq 10$ (see [2, Theorem 3.7 (b)]), so

$$p^a \leq \frac{|T|_3^2}{3}. \tag{3.5}$$

From Equations (3.4) and (3.5) we finally get

$$\frac{1}{3} \leq \frac{\log(|T|_2^2)}{\log(|T|)^2 - \log(|T|_3^2) + \log(3)} = \frac{\log(|T|_2)}{\log(|T|_{3'}) + \log(3)/2} \tag{3.6}$$

and it is easy to verify that, in the given range $10 \leq m \leq 165$, (3.6) is true only for $10 \leq m \leq 14$ or $16 \leq m \leq 21$ or $m = 24$. In all these cases, S should be a simple group of Lie type of characteristic 2 with the property that $|S| = |\mathrm{Alt}(m)|^2 p^a$ for some odd prime prime $p \leq m$ and some positive integer a. A boring but elementary check shows that there is no simple group S with these properties. □

Proposition 32. *T is not a sporadic simple group.*

Proof. At first, we will prove that S and T have the same dominant prime. Suppose by contradiction that the dominant primes do not coincide: then, since $|T|^2 = |S|p^a$, p coincides with the dominant prime of T and, by Corollary 30, $a = 1$. So we have

$$|T|^2 = p\,|S|\,. \tag{3.7}$$

Let q be the dominant prime of $|T|_{p'}$, necessarily it is the dominant prime of S. Let $|T|_p = p^t$, $|T|_q = q^h$, then $p^t > q^h$ and, by (3.7), $q^{2h} > p^{2t-1}$, so we get

$$q^h < p^t < q^{ht/(t-1/2)}.$$

By Corollary 25 (6), it must be $t > 1$ so

$$1 < \frac{t\log(p)}{h\log(q)} < \frac{t}{t-1/2} < \frac{\log(3)}{\log(2)}. \tag{3.8}$$

This implies that q is a good contributor to T. The good contributors to sporadic simple groups are listed in [2, Theorem 1]: it is easy to verify that these good

contributors does not satisfy (3.8), apart from the cases $T = F_5$ and $T = J_1$. However

$$\begin{cases} T = F_5 \Rightarrow |S| = |F_5|^2/2 \Rightarrow \lambda(S) < 1/3 \\ T = J_1 \Rightarrow |S| = |J_1|^2/19 \Rightarrow \lambda(S) < 1/3. \end{cases}$$

contradicting Proposition 9.

Thus, we know that S and T have the same dominant prime $p(S)$

Now suppose $a \neq 1$. Then $p = p(S)$ by Corollary 30 and $\lambda(S) > 1/3$ by Proposition 9, so

$$\frac{1}{3} < \frac{2\log(|T|_p) - a\log(p)}{2\log(|T|) - a\log(p)}$$

whence

$$2 \leq a \leq \left[\frac{3\log(|T|_p) - \log(|T|)}{\log(p)}\right] = a_*(T). \tag{3.9}$$

It can be easily checked that Equation (3.9) is satisfied only if

$$T \in \{B, Fi_{22}, Co_2, Ru, M_{24}, M_{22}, {}^2F_4(2)'\}.$$

All these groups have dominant prime 2, so $p = p(S) = p(T) = 2$ and S should be a simple group of Lie type of characteristic 2 with $|T|^2 = |S| \cdot 2^a$ and $2 \leq a \leq a_*(T)$. It can be checked that no simple group S satisfies these conditions.

Thus, $a = 1$. In particular, $|S| = |T|^2/p$. A direct computation shows that that, for every possible choice of a sporadic simple group T and every prime divisor p of its order, there is no simple group of Lie type satisfying this condition (many possibilities can be excluded since they are not compatible with the condition $\lambda(S) > 1/3$). □

So from now on we may assume that both S and T are simple groups of Lie type.

Lemma 33. *If p is the dominant prime of S, then p coincides with the characteristic of T.*

Proof. Suppose that p is the dominant prime of S. Since $|T|^2 = |S|p^a$, p is also the dominant prime of T. By Proposition 7, if p does not coincide with the characteristic of T, then one of the following cases occurs.

(1) $T = A_1(q)$, where $q = 2^k - 1$ is a Mersenne prime (so in particular k is prime). The dominant prime of T is 2. So $p = 2$ and, by Proposition 29, it also coincides with the characteristic of S. The order of $|S|$ has a cyclotomic factorization in term of 2 as it is described in the statement of Theorem 13. We have

$$|S| = \frac{|T|^2}{2^a} = 2^{2k-a} \cdot (2^k - 1)^2 \cdot (2^{k-1} - 1)^2 = \frac{2^b \cdot \Phi_{\alpha_1}(2) \cdots \Phi_{\alpha_u}(2)}{d}.$$

We must have $\alpha_1 = k$. Moreover $\Phi_k(2) = 2^k - 1 = q$, as k is a prime, and the multiplicity of $\Phi_k(2)$ in the factorization of $|S|$ is 2, so $\alpha_2 = \alpha_1$, contradicting Theorem 13 (1).

(2) $T = A_1(q-1)$, where $q = 2^{2^k} + 1$ is a Fermat prime. Then q is the dominant prime of T, whence $q = p$ and $(q \cdot (q-1) \cdot (q-2))^2 = |S| \cdot q^a$, in particular

$q^2 = q^a \cdot |S|_q$. As $|S|$ and $|T|$ have the same prime divisors, q must divide $|S|$, so $a = 1$, but then $|S| = q \cdot (q-1)^2 \cdot (q-2)^2$ and

$$|S|_2 = (q-1)^2 = 2^{2^{k+1}} > 2^{2^k} + 1 = q = |S|_q,$$

thus q cannot be the dominant prime for S, a contradiction.

(3) $T = A_1(8)$. Then $|T| = 2^3 \cdot 3^2 \cdot 7$, $p = 3$ and $2^6 \cdot 3^4 \cdot 7^2 = |S| \cdot 3^a$ for $a \geq 1$, whence $|S|_3 \leq 3^3 < 2^6 = |S|_2$, a contradiction.

(4) $T = {}^2A_2(3)$. Then $|T| = 2^5 \cdot 3^3 \cdot 7$, $p = 2$ and $2^{10} \cdot 3^6 \cdot 7^2 = |S| \cdot 2^a$ for $a \geq 1$, whence $|S|_2 \leq 2^9 < 3^6 = |S|_3$, a contradiction.

(5) $T = {}^2A_3(2)$. Then $|T| = 2^6 \cdot 3^4 \cdot 5$, $p = 3$ and $2^{12} \cdot 3^8 \cdot 5^2 = |S| \cdot 3^a$ for $a \geq 1$, whence $|S|_3 \leq 3^7 < 2^{12} = |S|_2$, a contradiction. □

From Lemma 33, Proposition 28 and Proposition 29, it follows:

Corollary 34. *If $a \neq 1$, then p coincides with the characteristic and dominant primes of S and T.*

Lemma 35. *Let $\alpha_1(T), \alpha_1(S)$ be the greatest indexes in the cyclotomic decompositions of $|T|$ and $|S|$ described in Theorem 13. Then $\alpha_1(T), \alpha_1(S) \geq 2$ and, denoting by p_T and p_S the characteristics of S and T, we have $(p_T, \alpha_1(T)), (p_S, \alpha_1(S)) \notin \{(2,6), (2^k - 1, 2) | k \in \mathbb{N}\}$.*

Proof. First notice that $\alpha_1(T), \alpha_1(S) \geq 2$ from Theorem 13.

If R is a simple group of Lie type with $p_R = 2^k - 1$ and $\alpha_1(R) = 2$, then $R = A_1(2^k - 1)$. We can exclude $(p_S, \alpha_1(S)) = (2^k - 1, 2)$ by Proposition 29 and $(p_T, \alpha_1(T)) = (2^k - 1, 2)$ by Lemma 33. Suppose now $(p_S, \alpha_1(S)) = (2, 6)$. Then $S \in \Sigma = \{A_5(2), A_2(2^2), A_1(2^3), B_3(2), D_4(2)\}$, but in these cases $|S|$ is divisible with odd multiplicity by at least two primes, contradicting Remark 26. Finally assume $(p_T, \alpha_1(T)) = (2, 6)$. Then $T \in \Sigma$. We may exclude $T = A_1(2^3)$, since there is no simple group S with $|S|p^a = |T|^2$ for some prime power p^a. In the remaining cases, 2 is the dominant prime of $|T|$ and also of $|T|/2$ and this implies that 2 is also the dominant prime of S (if $a \neq 1$ this follows from Corollary 30, while if $a = 1$ it suffices to recall that $|S| = |T|^2/p$). Hence the characteristic of S is 2 too, moreover $\alpha_1(S) \leq 6$, as $|S|$ cannot have primitive prime divisors not dividing $|T|$. We have already proved that $\alpha_1(S) \neq 6$. It is easy to verify that if S is a simple group of Lie type with characteristic 2 and satisfying $\alpha_1(S) \leq 5$ then the condition $|T|^2 = |S|p^a$ cannot be verified. □

Lemma 36. *The characteristic p_S of S does not coincide with the prime p.*

Proof. Suppose $p = p_S$. By Propostion 29, p coincides with the dominant prime of S, and consequently, since $|S| = |T|^2 p^a$, with the dominant prime of T; but then, by Lemma 33, p coincides also with the characteristic of T. By Lemma 35 and Theorem 13 (3), we get that $\alpha_1(T) = \omega(|T|)$ and $\alpha_1(S) = \omega(|S|)$. By Remark 12, $\omega(|S|) = \omega(|T|)$, so we conclude that $\alpha_1(T) = \alpha_1(S)$. Again by Lemma 35, we can use Zsigmondy's Theorem to find a primitive prime divisor t of $p^{\alpha_1(T)} - 1$. The multiplicity of t in $|T|$ coincides with the multiplicity of t in $\Phi_{\alpha_T}(p_T) = \Phi_{\alpha_S}(p_S)$, which is equal to the multiplicity of t in $|S|$, thus contradicting $|T|^2 = |S|p^a$. □

Proposition 37. $a = 1$.

Proof. Suppose $a \neq 1$: then, by Corollary 34, p is the characteristic and dominant prime of both S and T, contradicting Lemma 36. □

We remain with the possibility that $a = 1$ and consequently $|T|^2 = |S|\, p$ where p divides the order of the Schur multiplier $M(S)$. Moreover, the Schur multiplier can be decomposed as $M(S) = R \times P$, where P is a p_S-group and R a p_S'-group whose order coincides with the denominator d_S of the cyclotomic factorization of the order of S (see [8, Table 4.1]). By Lemma 36, $p \neq p_S$, thus p divides d_S.

Lemma 38. *If S, T have the same dominant prime u and $u \neq p$, then u coincides with the characteristic of T.*

Proof. By Proposition 7, if u does not coincide with the characteristic of T, then one of the following cases occurs.

(1) $T = A_1(q)$, where $q = 2^k - 1$ is a Mersenne prime. Then $u = 2$ and
$$((2^k - 1) \cdot 2^k \cdot (2^{k-1} - 1))^2 = |S| \cdot p.$$
By Proposition 29, the characteristic of S coincides with $u = 2$, hence, considering the cyclotomic factorization of $|S|$ described in Theorem 13, we have $\alpha_1(S) = k$ and $\Phi_k(2) = 2^k - 1 = q$. By Theorem 13 (1), $\Phi_k(2)$ divides $|S|$ with multiplicity 1, so necessarily $p = q$ by Remark 26. On the other hand, p divides d_S and, by Theorem 13 (2), d_S divides $\Phi_{\alpha_3}(2) \cdots \Phi_{\alpha_u}(2) = (2^{k-1} - 1)^2 / \Phi_{\alpha_2}(2)$, thus p divides $(2^{k-1} - 1)$, whence $p \leq 2^{k-1} - 1 < 2^k - 1 = q = p$, a contradiction.

(2) $T = A_1(q - 1)$, where $q = 2^{2^k} + 1$ is a Fermat prime. Then $u = q$ and
$$q^2 \cdot (q - 1)^2 \cdot (q - 2)^2 = |S| \cdot p.$$
By Proposition 29, the characteristic of S coincides with $u = q$, in particular the characteristic of S divides $|S|$ with multiplicity 2 and it is easy to check that the only group satisfying this condition is $S = A_1(q^2)$, but then $d_S = 2$ whence $p = 2$. Hence
$$q^2 \cdot (q - 1)^2 \cdot (q - 2)^2 = |A_1(q^2)| \cdot 2 = q^2 \cdot (q^2 - 1) \cdot (q^2 + 1),$$
whence $(q - 1) \cdot (q - 2)^2 = (q + 1) \cdot (q^2 + 1)$, but this is false.

(3) $T = A_1(2^3)$. Then $|T| = 2^3 \cdot 3^2 \cdot 7$, $u = 3$, $p = 2$ and $|S| = 2^5 \cdot 3^4 \cdot 7^2$, however there is no simple group of Lie type S with this order.

(4) $T = {}^2A_2(3)$. Then $|T| = 2^5 \cdot 3^3 \cdot 7$, $u = 2$, $p = 3$ and $|S| = 2^{10} \cdot 3^5 \cdot 7^2$, however there is no simple group of Lie type S with this order.

(5) $T = {}^2A_3(2)$. Then $|T| = 2^6 \cdot 3^4 \cdot 5$, $u = 3$, $p = 2$ and $|S| = 2^{11} \cdot 3^8 \cdot 5^2$, however there is no simple group of Lie type S with this order. □

Lemma 39. *S and T have different dominant primes.*

Proof. Suppose that r is the dominant prime of S and T. Then, by Lemma 36, $r \neq p$ and therefore $|T|_r^2 = |S|_r$ and, by Remark 12, $\omega(S) = \omega(T)$. Moreover, by Lemma 35 and Theorem 13 (3), $\alpha_1(S) = \omega(S)$ and $\alpha_1(T) = \omega(T)$, whence $\alpha_1(S) = \alpha_1(T) = \alpha$. By Proposition 29 and Lemma 38, r is also the characteristic of both S and T. Again by Lemma 35, we can apply Zsigmondy's Theorem and consider a primitive prime divisor u dividing of $r^\alpha - 1$. This prime u divides $|S|$ and $|T|$ with the same multiplicity (coinciding with the multiplicity of u in $\Phi_\alpha(r)$). On the other hand $|S| \cdot p = |T|^2$, so we must have that $r = p$ and that p divides $|S|$ with multiplicity 1, in contradiction with Corollary 25 (6). □

Now we are ready to conclude our proof. We have reduced to the case $|T|^2 = p \cdot |S|$, where the dominant prime of T and S (which coincide with their characteristic) are different, and consequently p is the dominant prime of T. Let r be the dominant prime of S and let p^t, r^h be the contributions of p and r to $|S|$. We have

$$p^t < r^h < p^{t+1}, \tag{3.10}$$

and consequently, since $t > 1$ by Corollary 25 (6),

$$1 < \frac{h\log(r)}{t\log(p)} < 1 + \frac{1}{t} < \frac{\log(3)}{\log(2)}.$$

thus p is a good contributor of S. By [2, Theorem 4.1] S is one of following groups:

(1) $A_3(3), {}^2A_3(3), {}^2A_3(7), {}^2A_4(3), B_2(3), B_2(5), B_2(7), B_2(9), B_3(3), C_3(3), D_4(3), G_2(3)$ (and $p = 2$);
(2) ${}^2A_3(2), {}^2A_4(2), {}^2A_5(2), B_3(2), D_4(2)$ (and $p = 3$);
(3) $A_1(r), A_2(r), {}^2A_2(r)$.

The possibilities listed in (1) and (2) can be immediately excluded noticing that either p does not divide $|M(S)|$, or there exists a prime different from p dividing $|S|$ with odd multiplicity, or $|S|p$ is not a square.

The only cases that remain to be discussed are thus $A_1(r)$, $A_2(r)$, ${}^2A_2(r)$: we have $|S| = r^\epsilon \cdot u$ where ϵ is odd and $(u, r) = 1$, so, by Remark 26, $r = v^2$ for some integer v. If $S = {}^2A_2(v^2)$, then $M(S) = (3, v^2 + 1) = 1$, a contradiction. Suppose $S = A_1(v^2)$. We have already excluded the possibilities $S \cong A_1(4) \cong \mathrm{Alt}(5)$ and $S \cong A_1(9) \cong \mathrm{Alt}(6)$, so we have $M(S) = (2, v^2 - 1)$ and consequently $p = 2$ and v is odd. In particular

$$|S|_2 = \frac{(v^4 - 1)_2}{2} = \frac{(v^2 - 1)_2(v^2 + 1)_2}{2} = (v^2 - 1)_2$$

and from (3.10) we deduce $(v^2 - 1)_2 < v^2 < 2(v^2 - 1)_2$: the only possibility is $v = 3$, but we have already excluded this case. Finally, suppose $S = A_2(v^2)$. We may exclude $S = A_2(4)$ since in this case 5 and 7 divide $|S|$ with multiplicity 1. In the remaining case $M(S) = (3, v^2 - 1)$, so it must $v^2 - 1 = 0 \mod 3$ and $p = 3$. But then $v^4 + v^2 + 1 = (v^2 - 1)^2 + 3v^2 \cong 3v^2 \cong 3 \mod 9$, thus

$$|S|_3 = \frac{(v^2 + 1)_3(v^2 - 1)_3^2(v^4 + v^2 + 1)_3}{3} = (v^2 - 1)_3^2$$

and by (3.10) we have $(v^2 - 1)_3^2 < v^6 < 3(v^2 - 1)_3^2$, whence $v^6 < 3(v^2 - 1)^2$, a contradiction.

4. Proof of Theorem 3

It follows immediately from Theorem 22 that:

Proposition 40. *If there exists a non-pronilpotent normally ζ-reversible profinite group all of whose composition factors are of alternating type, then there exist a positive integer m and a finite group H with the following properties:*

(1) $|H| = |\mathrm{Alt}(m)|^2$.
(2) H contains a unique minimal normal sugroup N.
(3) Either H/N is nilpotent or there exist a nilpotent group X and a positive integer $n \geq m$ such that $H/N \cong X \times \mathrm{Alt}(n)$; in the latter case $\pi(m!) = \pi(n!)$ i.e. there is no prime p with $m < q \leq n$.
(4) Either N is abelian or $N \cong \mathrm{Alt}(u)^t$ for some u and $t \in \mathbb{N}$.

In this section we will prove that there is no pair (m, H) satisfying the condition requested by the previous proposition. We will assume, by contradiction, that (m, H) is one of these pairs and we will prove a series of restrictions that will lead to a finale contradiction.

Lemma 41. *H is not soluble.*

Proof. If H is soluble, then H is a finite soluble group which is not nilpotent but all of whose proper quotients are nilpotent. This implies that $H = N \rtimes A$, where N is an elementary abelian p-group and A is a nilpotent p'-subgroup of $\operatorname{Aut} N$. By [20, Theorem 1.6], $|A| \leq |N|^{\beta}/2$ with $\beta = \log(32)/\log(9)$ so

$$\frac{\log(|H|)}{\log(|N|)} < \frac{\log(288)}{\log(9)}. \tag{4.1}$$

On the other hand, since $|H| = |\operatorname{Alt}(m)|^2$, we have

$$\log(|H|)/\log(|N|) \geq \big(\lambda(\operatorname{Alt}(m))\big)^{-1}.$$

The values of the logarithmic proportion of alternating groups are listed in [11, Tables $L.3$ and $L.4$] and it can be easily seen that

$$\frac{\log(|H|)}{\log(|N|)} \geq \big(\lambda(\operatorname{Alt}(m))\big)^{-1} > \frac{\log(288)}{\log(9)} \quad \text{for} \quad m \notin \{5, 8\}$$

contradicting (4.1). Direct computations shows that (4.1) is false also when $m \in \{5, 8\}$. □

Lemma 42. *$N = \operatorname{soc} H$ is abelian.*

Proof. Suppose by contradiction that N is nonabelian: then there exist positive integers $u \geq 5$ and t such that $N = L_1 \times \cdots \times L_t$, with $L_i \cong L = \operatorname{Alt}(u)$ for all i. In particular

$$L^t \cong N \trianglelefteq H \leq \operatorname{Aut}(N) \cong \operatorname{Aut}(L) \wr \operatorname{Sym}(t).$$

If $t = 1$, then $|\operatorname{Alt}(m)|^2 = |H| = 2^j \cdot u!$ for some $j \in \mathbb{Z}$, however by Lemma 4 there exists an odd prime dividing $u!$ with multiplicity 1, a contradiction. If $t = 2$, then from $|\operatorname{Alt}(m)|^2 = H$, we would deduce $(m!)^2 = (u!)^2 2^j$ for some positive integer $j \in \{1, 2, 3, 4, 5\}$, but this is impossible. So we can assume $t \geq 3$. By Proposition 40 we can write $H/N = X_1/N \times X_2/N$, where X_1/N is nilpotent and either $X_2/N = 1$ or $X_2/N \cong \operatorname{Alt}(n)$ for some $n \geq m$. First suppose that either $X_2/N = 1$ and $m \notin \{6, 10\}$, or $X_2/N \cong \operatorname{Alt}(n)$ with $n \notin \{6, 10\}$. Then, by Lemma 4, we can find two primes p, q as follows:

$$\begin{cases} \frac{n}{2} < p < q \leq n & \text{if } X_2/N \cong \operatorname{Alt}(n), \\ \frac{m}{2} < p < q \leq m & \text{if } X_2/N = 1. \end{cases}$$

We claim that p, q both divide the order of $\operatorname{Alt}(m)$ with multiplicity 1: this is clear if X_2/N is trivial, while if $X_2/N \cong \operatorname{Alt}(n)$ it follows from the fact that $m/2 \leq n/2 < p < q \leq m$. So p and q divide $|H| = (m!/2)^2$ with multiplicity exactly 2: as $L^t \leq H$ and $l > 2$, they cannot divide $|L|$, so they divide $|H/N| = |X_1/N||X_2/N|$ with multiplicity 2. On the other hand, by the way in which they have been defined, they divide $|X_2/N|$ with multiplicity at most 1, so $p \cdot q$ must divide order of the nilpotent group X_1/N. This implies that the transitive permutation group induce

by the conjugacy action of H on the t direct factors $L_1, \dots, L_t$ contains a central element of order $p \cdot q$. In particular $t \geq p \cdot q$ and consequently,

$$60^{\frac{m^2}{4}} \leq 60^{p \cdot q} \leq |L|^t \leq |H| = (m!)^2 \leq m^{2m}$$

but this is false for all $m \geq 5$. We have still to consider the two cases $X_2/N = 1$ and $m \in \{6, 10\}$ or $X_2 \cong \mathrm{Alt}(n)$ with $n \in \{6, 10\}$. If $m = 6$ or $n = 6$ (and consequently $m \leq 6$), then $|\mathrm{Alt}(u)|^3$ divides $|\mathrm{Alt}(6)|^2$, hence 5^3 divides $(6!)^2$, a contradiction. If $m = 10$ or $n = 10$, then 7 divides $|H|$ with multiplicity at most 2; as a consequence $|H/N|$ is divisible by 7 and $t \geq 7$; but then

$$7 \cdot 60^7 \leq |H/N| \cdot |N| = |H| \leq (10!)^2$$

which leads again to a contradiction. □

Combining Proposition 40 with Lemma 41 and Lemma 42, we can conclude that there exists two subgroups X_1 and X_2 of H such that

(1) $H/N = X_1/N \times X_2/N$;
(2) X_1/N is nilpotent;
(3) $X_2/N \cong \mathrm{Alt}(n)$.
(4) N is an elementary abelian p-group.

Lemma 43. *N is not central in X_2.*

Proof. Assume, by contradiction, $N \leq Z(X_2)$. Notice that $\mathrm{Frat}(X_2)$ is a nilpotent normal subgroup of H, so either $\mathrm{Frat}(X_2) = 1$ or $\mathrm{Frat}(X_2) = N$. In the first case, we would have $X_2 = N \times S$, with $S \cong \mathrm{Alt}(n)$. But then S would be normal in H, against the fact that N is the unique minimal normal subgroup of G. If $\mathrm{Frat}(X_2) = N$, then X_2 is a perfect central extension of N, so in particular $|N|$ divides the order of the Schur multiplier of $\mathrm{Alt}(n)$, hence $|N| \in \{2, 3\}$. This implies that X_1 is a $\{2, 3\}$-group (if a prime $q > 3$ would divide $|X_1|$, then a Sylow q-subgroup of X_1 would coincide with $O^q(C_{X_1}(N))$ and would be normal in H). From $|H| = |X_1/N| \cdot |X_2|$, we deduce

$$(m!)^2 = n! \cdot 2^\alpha \cdot 3^\beta$$

for some positive integers α, β, in contradiction with the fact that, by Lemma 4, there exists a prime dividing $n!$ with multiplicity 1. □

The previous result, combined with Clifford's theory, implies that N contains a nontrivial irreducible $\mathrm{Alt}(n)$-modulo, say M.

Lemma 44. $n \leq 8$.

Proof. Suppose $n \geq 9$. By [19, Theorem 1.1], the dimension of a nontrivial irreducible $\mathrm{Alt}(n)$-module is at least $n - 2$, so $|N| \geq |M| \geq p^{n-2}$. But then, from $|\mathrm{Alt}(m)|^2 = |H| \geq |N| \cdot |\mathrm{Alt}(n)|$, we get

$$((m!/2))_p^2 \geq p^{n-2} \cdot (n!/2)_p.$$

Let now $a = m - n \geq 0$ and $\eta_p = 0$ is p is odd, $\eta_2 = 1$ if $p = 2$; since $(m!)_p < p^{m/(p-1)}$, we have

$$p^{m/(p-1)-\eta_p} > (m!/2)_p \geq (m+1)_p \cdots (m+a)_p \cdot p^{m+a-2} \geq p^{m+a-2}.$$

This implies

$$p = 2, \quad n = m, \quad |N| = |M| = 2^{n-2} = (n!/2)_2.$$

Since

$$|H| = \left(\frac{n!}{2}\right)^2 = \frac{|X_1||X_2|}{|N|} = \frac{n!|X_1|}{2} \quad \text{and} \quad 2^{n-2} = (n!/2)_2,$$

we must have that $X_1 = N \rtimes K$, where N is an elementary abelian 2-group and K is a nilpotent group of odd order; more precisely $|K| = (n!)_{2'}$. Moreover, the fact that N is the unique minimal normal subgroup of H implies $C_K(N) = 1$, hence K is a completely reducible subgroup of $\operatorname{Aut} N$. In particular

$$|K| \leq \frac{|N|^\beta}{2} = 2^{\beta(n-2)-1} \text{ with } \beta = \frac{\log(32)}{\log(9)}$$

whence

$$n! = (n!)_{2'} \cdot (n!)_2 = |K| \cdot (n!)_2 \leq 2^{\beta(n-2)-1} \cdot 2^{n-1} = 2^{n(\beta+1)-2\beta-2}$$

which is false for $n \geq 9$. □

We remain with the the cases $5 \leq m \leq n \leq 8$. Recall that $\pi(n!) = \pi(m!)$ and that $|N| \cdot |\operatorname{Alt}(n)|$ divides $|H| = \left(\frac{m!}{2}\right)^2$ (i.e. $2|N|n!$ divides $(m!)^2$). This means that N is a completely reducible $\operatorname{Alt}(n)$-module of relatively small order. Looking to the irreducible representations of small degree of $\operatorname{Alt}(n)$ over the field with p elements when $5 \leq n \leq 8$ and $p \leq n$, we easily conclude that the only possibilities are: $m = n = 8$ and N is an irreducible $\operatorname{Alt}(8)$-module with $|N| \in \{2^4, 2^6\}$. In both these cases, a $2'$-Hall subgroup K of X_1 would be nilpotent and of order $3^2 \cdot 5 \cdot 7$. Moreover $C_K(N) = 1$ (otherwise we would have $N \neq \operatorname{soc} H$) and $\operatorname{Aut}(N)$ would contain an element of order $3^2 \cdot 5 \cdot 7$, which is false.

References

1. N. Boston, A probabilistic generalization of the Riemann zeta function, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995) **138** (1996), 155–162.
2. F. Buekenhout, Good contributors to the order of the finite simple groups, Arch. Math. (Basel) 44 (1985), no. 4, 289–296.
3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985.
4. E. Damian and A. Lucchini, Profinite groups in which the probabilistic zeta function coincides with the subgroup zeta function, J. Algebra 402, 92-119 (2014).
5. F. Grunewald, D. Segal and G.C. Smith, Subgroups of finite index in nilpotent groups, Invent. Math. 93 (1988), no. 1, 185–223.
6. E. Detomi and A. Lucchini, Profinite groups with multiplicative probabilistic zeta function, J. London Math. Soc. (2) 70 (2004), no. 1, 165–181.
7. E. Detomi and A. Lucchini, Some generalizations of the probabilistic zeta function, Ischia group theory 2006, 56–72, World Sci. Publ., Hackensack, NJ, 2007.
8. D. Gorenstein, Finite simple groups. An introduction to their classification. University Series in Mathematics. Plenum Publishing Corp., New York, 1982.
9. P. Hall, The eulerian functions of a group, Quart. J. Math. (1936), no. 7, 134–151.
10. I. M. Isaacs, Character theory of finite groups. Pure and Applied Mathematics, No. 69. Academic Press, New York-London, 1976.
11. W. Kimmerle, R. Lyons, R. Sandling and D. N. Teague, Composition factors from the group ring and Artin's theorem on orders of simple groups, Proc. London Math. Soc. (3) 60 (1990), no. 1, 89–122.
12. V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra 32 (1974), 418–443.
13. A. Lucchini, Profinite groups with nonabelian crowns of bounded rank and their probabilistic zeta function, Israel J. Math. 181 (2011), 53–64.

14. J. Nagura, On the interval containing at least one prime number, Proc. Japan Acad. 28, (1952). 177–181.
15. A. Mann, Positively finitely generated groups, Forum Math. 8 (1996), no. 4, 429–459.
16. C. E. Praeger and J. Saxl, On the orders of primitive permutation groups, Bull. London Math. Soc. 12 (1980), no. 4, 303–307.
17. G. Seitz and A. Zalesskii, On the minimal degrees of projective representations of the finite Chevalley groups II, J. Algebra 158 (1993), no. 1, 233–243.
18. P. H. Tiep, Low dimensional representations of finite quasisimple groups, Groups, combinatorics and geometry (Durham, 2001), 277–294, World Sci. Publ., River Edge, NJ, 2003.
19. A. Wagner, The faithful linear representation of least degree of S_n and A_n over a field of characteristic 2. Math. Z. 151 (1976), no. 2, 127–137.
20. T. R. Wolf, Solvable and nilpotent subgroups of $GL(n, q^m)$. Canad. J. Math. 34 (1982), no. 5, 1097–1111.
21. K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys. 3 (1892), no. 1, 265–284.

Dipartimento di Matematica, Università di Padova, Via Trieste 63, 35121 Padova, Italy

E-mail address: leone.cimetta@gmail.com

Dipartimento di Matematica, Università di Padova, Via Trieste 63, 35121 Padova, Italy

E-mail address: lucchini@math.unipd.it